ANTI MONEY LAUNDERING POLICY & PROCEDURE

Prevention of Money Laundering Act, 2002

Updated As On July 11, 2024

Introduction:

According to Prevention of Money Laundering Act, 2002 and Rules framed thereunder, Dhani Stocks Limited (DSL) has developed and implemented the Anti-Money Laundering program designated to achieve and monitor the compliance with the requirement. For the purpose of compliance with requirements and provisions of the Act, DSL is maintaining a record of such transactions the nature and value of which has been prescribed in the Rules under the PMLA. Such transactions include:

- All cash transactions valued at more than Rs.10 lacs or its equivalent in foreign currency.
- All series of cash transactions integrally connected to each other which have been individually valued below Rs 10 lakhs 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 Rs. 10 Lakh or its equivalent in foreign currency.
- 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;
- 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.

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

"**Suspicious transactions**" means a transaction whether or not made in cash which to a person acting in good faith –

1. Gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime** or
2. Appears to be made in circumstances of unusual or unjustified complexity or
3. Appears to have no economic rationale or bonafide purpose or
4. Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

** **Note:** "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.

DSL has existing policies and procedures for its various business functions form the basis for its overall money laundering prevention program. This assures that anti-money laundering compliance reach all aspects of our company's business.

Money laundering is the process of transforming the proceeds of crime into ostensibly legitimate

money or other assets. If undertaken successfully, money laundering allows criminals to legitimize "dirty" money by mingling it with "clean" money, ultimately providing a legitimate cover for the source of their income. Section 3 of the PMLA, described the offence under Money Laundering. Section 3 reads as under:

"Whosoever directly or indirectly attempts to indulge or knowingly assists or knowingly is a party or is actually involved in any process or activity connected with the proceeds of crime and projecting it as untainted property shall be guilty of offence of money-laundering."

There are three different steps in money laundering described by three terms as follows:

- **Placement:** Dirty Money, generally in the form of Cash is inserted into a legitimate financial institution.
- **Layering:** Layering involves sending the money through various financial transactions to change its form and make it difficult to follow. Layering may consist of several bank-to- bank transfers, wire transfers between different accounts in different names in different countries, changing the money's currency, and purchasing high-value items to change the form of the money
- **Integration:** At the integration stage, the money re-enters the mainstream economy in legitimate-looking form. This may involve a final bank transfer into the account of a local business in which the launderer is "investing" in exchange for a cut of the profits. At this point, the criminal can use the money without getting caught.

Anti-money laundering procedures set out by DSL are reviewed regularly and updated as necessary, based on any legal/regulatory or business/operational changes, such as additions or amendments to existing anti-money laundering rules & regulations or business expansion.

Appointment of a Designated Director and his Duties

DSL has appointed a Designated Director in terms of Rule 2 (ba) of the PML Rules to ensure overall compliance with the obligations imposed under chapter IV of the Act and the Rules.

Appointment of Principal Officer and his/her Duties

DSL has appointed Principal Officer to discourage and identify any money laundering or terrorist financing activities as required under the Prevention of Money Laundering Act.

Further DSL has appointed Money Laundering Control Officer who is responsible for all Anti-Money Laundering related activities in absence of the Principal Officer.

The designated Principal Officer is the central point of contact for communicating with regarding issues related to the company's anti-money laundering program.

The basic functions that are carried out by the Principal Officer to curb money laundering are enumerated as follows:

a. Communication of group policies relating to prevention of money laundering and terrorist financing to all management and relevant staff that handle account information, securities transactions, money and customer records etc. whether in branches, departments or subsidiaries;
b. Define customer acceptance policy and customer 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 Carrying on internal audits or compliance functions to ensure compliance with policies, procedures, and controls relating to prevention of money laundering and terrorist financing, 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.

DSL has adopted certain procedures to implement the Anti-Money Laundering provisions as envisaged under the Anti-Money Laundering Act, 2002. Such procedures inter alia includes, but not limited to, 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

Client Due Diligence (CDD)

The CDD measures comprise the following:

i. Obtaining sufficient information in order to identify persons who beneficially own or control the securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party shall be identified using reliable and independent client identification and verification procedures. The beneficial owner is the natural person or persons who ultimately own, control or influence a client and/or persons on whose behalf a transaction is being conducted. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.
ii. Identify the clients, verify their identity using reliable and independent sources of identification, obtain information on the purpose and intended nature of business relationship, where applicable;
iii. Verify the client's identity using reliable, independent source documents, data or

information. Where the client purports to act on behalf of juridical person or individual or trust then verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person;

However, in case of a Trust, the trustees need to disclose their status at the time of opening their trading / demat account with DSL.

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

a. **Where the client is company,** the beneficial owner is the natural person, 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: Controlling ownership interest means ownership of / or entitlement to:

(i) more than 10% of shares or capital or profits of the company;

However, incase of company, the term "Control" shall include the right to appoint majority of the directors or to control the management or policy decisions including by virtue of their shareholding or management rights or shareholders' agreements or voting agreements

b. **Where the client is a partnership firm,** the beneficial owner(s) is a nature person (s) who , whether acting alone or together, or through one or more judicial person, has ownership of /or entitlement to more than 10% of capital or profits of the partnership or who exercises control through other means;

Explanation: For the purpose of this clause:-

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

c. **Where the client is an unincorporated association or body of individuals,** the beneficial owner is the natural person(s), who, whether acting alone or together, or through one or more juridical person, has ownership of or entitlement to more than 15% of the property or capital or profits of such association or body of individuals;

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

e. **For client which is a trust:** Where the client is a trust, the identification of the beneficial owner shall include identification of the author of the trust, the trustee, the protector, the settlor, the beneficiaries with 10% 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.

f. **Where the client or the owner of the controlling interest is an entity listed on a stock exchange in India or it is an entity resident in jurisdictions notified by the Central Government and listed on stock exchanges in such jurisdictions notified by the Central Government, or it is a, subsidiary of such listed entities,** it is not necessary to identify and verify the identity of any shareholder or beneficial owner of such entities.

g. **Applicability for foreign investors:** DSL is dealing with foreign investors' as 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.

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

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

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

viii. Review the due diligence measures including re-verifying the identity of the client(s) 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

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

x. DSL shall register the details of the client, in case of the client being a Non-Profit Organization, 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 with client has ended or the account has been closed, whichever is later.

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

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

Policy for acceptance of clients

DSL has further developed customer acceptance policies and procedures that aim to identify the types of customers that are likely to pose a higher than the average risk of money laundering or terrorist financing. By establishing such policies and procedures, we will be in a better position to apply customer due diligence on a risk sensitive basis depending on the type of customer business relationship or transaction. In a nutshell, the following safeguards are followed while accepting the clients:

a. DSL shall not allow opening of or keep any anonymous account or account in fictitious names or account on behalf of other persons whose identity has not been disclosed or cannot be verified.

b. Factors of risk perception (in terms of monitoring suspicious transactions) of the client are clearly defined having regard to client's location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover etc.

and manner of making payment for transactions undertaken. The parameters enable classification of clients into low, medium and high risk. Clients of special category (as given below) may, if necessary, be classified even higher. Such clients require higher degree of due diligence and regular update of KYC profile.

c. DSL shall undertake enhanced due diligence measures as applicable for Clients of Special Category (CSC).

CSC shall include:

- Non-Resident Clients
- High Net-worth Clients
- Trust, Charities, Non - Governmental Organization (NGOs) and organizations receiving donations
- Companies having close family shareholdings or beneficial ownership
- Politically Exposed Persons (PEPs) shall have the same meaning as given in clause (db) sub-rule (1) of rule 2 of the PML Rules. PEP are individuals who are or have been entrusted with prominent public functions by a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials. The additional norms applicable to PEP's shall also be applied to the accounts of the family members or close relatives / associates of PEPs.
- Clients in high risk countries – While dealing with clients from or situated in high risk countries or geographic areas or when providing delivery of services to clients through high risk countries or geographic areas i.e. places where existence or effectiveness of action against money laundering or terror financing is suspected, apart from being guided by the FATF recommendations (published by the FATF on its website (www.fatf-gafi.org)), DSL shall also independently access and consider other publicly available information along with any other information which we may have access to. However, this shall not preclude DSL from entering into legitimate transactions with clients from or situate in such high risk countries and geographic areas or delivery of services through such high risk countries or geographic areas. Additionally, DSL will apply enhanced due diligence (EDD) measures, proportionate to the risk, to business relationships and transactions with natural and legal persons (including financial institutions) from countries as highlighted by FATF from time to time.
- Non face to face clients- (i.e. clients who open account without visiting DSL's branch/office premises or meeting its officials). **Note:** Video based customer identification process is treated as face-to-face onboarding of clients.
- Clients with dubious reputation as per public information available etc.

d. Documentation requirement and other information are collected in respect of different classes of clients depending on perceived risk and having regard to the requirement to the Rule 9 of PML

Rules, Directives and Circulars issued by SEBI from time to time.

e. Ensure that an account is not opened where we are unable to apply appropriate clients due diligence measures / KYC policies. This may be applicable in cases where it is not possible to ascertain the identity of the client or information provided to DSL is suspected to be non-genuine, or there is perceived non-cooperation of the client in providing full and complete information. It is ensured that we do not continue business with such a person and is also ensure that DSL files a suspicious activity report. Further, prior to closing/freezing the trading/demat account, DSL shall also thoroughly evaluate if any transaction / trade undertaken seems to be suspicious in nature. DSL shall ensure that it does not return securities or money that may be from suspicious trades. However, DSL shall consult the relevant authorities in determining what action it shall take when it suspects suspicious trading.

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

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

h. Necessary checks shall be conducted before opening a new account so as to ensure that the identity of the customer does not match with any person with banned entities such as individual terrorists or terrorist organizations etc. For conducting such reviews, DSL shall check the lists provided by SEBI /Exchanges/internally maintained lists, it shall rely primarily on the United Nations list which is available at http://www.un.org/sc/committees/1267/consolist.shtml and http://www.un.org/sc/committees/1988/list.shtml. The list of FATF countries is also updated on an ongoing basis, in our system/software, to ensure that clients part of /covered under the high risk countries, as per the FATF list, are not allowed to open accounts with DSL. The compliance team shall be responsible to ensure that the said lists are updated on a daily basis through various sources.

i. If a customer attempts to open account with DSL via forged KYC documents, and the same is revealed at any point of time, then the attempt of the customer shall be construed as fiduciary/suspicious. Actions are initiated as per the prescribed guidelines.

j. The CDD process shall necessarily be revisited, if required, when there are suspicions of money laundering or financing of terrorism (ML/FT).

Risk Management/ Risk Based Approach

DSL applies a risk based approach for mitigation and management of the identified risk. It is generally recognized that certain customers may be of a higher or lower risk category depending on circumstances

such as the customer's background, type of business relationship or transaction etc. At the time of opening of account, customer are classified as High Risk if declared income range per annum is above Rs. 25 lakhs, Medium Risk if declared income range per annum is Rs. 10 – 25 Lakhs and Low risk if declared income per annum is less than Rs 10 Lakhs. Thereafter every month clients are classified based on following parameters,

High Risk

- Collateral > = 2 Crore
- Average daily turnover > = 5 Crore
- Client of special category

Medium Risk

- 50 lacs < = Collateral < 2 Crore
- 1 crore < = Average daily turnover < 5 Crore

Low Risk

- Collateral < 50 lacs
- Average daily turnover < 1 Crore

DSL follows stringent customer due diligence measures on all risk categories of clients. Further, it also carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to its clients, countries and geographical areas, nature and volume of transaction, payment method used by clients, etc. The risk assessment 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 individual and entities who are subjected to sanction measures as required under the various United Nations Security Council Resolutions.

Risk Assessment:

1. DSL carries out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to its clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients etc.
2. The risk assessment carried out by DSL considers all the relevant risk factors before determining the level of overall risk, the appropriate level and type of mitigation to be applied. The risk assessment is updated on regular basis and is presented/submitted to relevant competent authorities on demand basis.
3. DSL shall identify and assess the risks involved in regards to development of new products/new business practices/new or developing technology for both new and existing products.
4. DSL shall ensure that ML/TF risk assessments are always done prior to the launch or use of new products, practices, services, technologies etc.

In addition to the above, DSL has also adopted a risk based approach to mitigate and manage the risk as

detailed below.

i. DSL does not accept cash from the clients.
ii. Receipts from clients to be accepted in the form of crossed cheque in favor of Dhani Stocks Limited and drawn on the bank account of the particular client as updated in our records, or through demand drafts made from the client's own funds or by means of fund transfers from the account of the particular client as updated in our records.
iii. Similarly payments due to a client to be made by means of crossed cheque in favor of the respective client. Third party cheques should not be accepted on behalf of any client.
iv. Pay in / Pay out to be received from/made to the Demat account of the particular client as updated in our records and no to/fro movement to be accepted from any third party account in/from our pool account.

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

Client of special category (CSC):

Clients of Special Category (CSC) are classified as "High Risk" clients. Such clients include the following:

- Non-resident clients
- High Net worth clients
- Trust, Charities, Non – Governmental Organization (NGOs) and organizations receiving donations,
- Companies having close family shareholdings or beneficial ownership,
- Politically Exposed Persons (PEPs) shall have the same meaning as given in clause (db) sub-rule (1) of rule 2 of the PML Rules. PEP are individuals who are or have been entrusted with prominent public functions by a foreign country, e.g., Heads of States or of Governments, senior politicians, senior government/judicial/military officers, senior executives of state-owned corporations, important political party officials. The additional norms applicable to PEP's shall also be applied to the accounts of the family members or close relatives / associates of PEPs.

  Clients in high risk countries – While dealing with clients from or situated in high risk countries or geographic areas or when providing delivery of services to clients through high risk countries or geographic areas i.e. places where existence or effectiveness of action against money laundering or terror financing is suspected, apart from being guided by the FATF recommendations (published by the FATF on its website (www.fatf-gafi.org)), DSL shall also independently access and consider other publicly available information along with any other information which we may have access to. However, this shall not preclude DSL from entering into legitimate transactions with clients from or situate in such high risk countries and geographic areas or delivery of services through such high risk countries or geographic areas. Additionally, DSL will apply enhanced due diligence (EDD) measures, proportionate to the risk, to business relationships and transactions with natural and legal persons (including financial institutions) from countries as highlighted by FATF from time

to time.

- Non-face to face clients - (i.e. clients who open account without visiting DSL's branch/office premises or meeting its officials). Note: Video based customer identification process is treated as face-to-face onboarding of clients
- Clients with dubious reputation as per public information available etc.

We do recognize that the above mentioned list is only illustrative and we shall be exercising independent judgment to ascertain whether any other set of clients should be classified as CSC or not.

Procedure for Client Identification

The "Know your Client" (KYC) procedures clearly spells out the client identification process that is carried out at different stages i.e. while establishing client relationship i.e. client onboarding, while carrying out transactions for the client or when DSL has doubt/suspicion about the veracity or the adequacy of previously obtained client identification data. DSL has framed its own internal guidelines and legal requirements as per the established practices detailing the list of documents required during account opening process. The underlying principle is to follow the principles enshrined in the PML Act, 2002 as well as the SEBI Act, 1992.

a. DSL has proactively put in place Risk Management Systems to determine whether their client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPs.
b. Senior management approval for establishing business relationships with PEPs is obtained. Where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP, Dhani Stocks Ltd shall obtain senior management approval to continue the business relationship.
c. DSL has also taken reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP".
d. Verify customer's identity using reliable, independent source documents, data or information;
e. Each original document is seen prior to acceptance of a copy.
f. Failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the higher authority within DSL.
g. Conduct in-person verification (IPV) by personally visiting the client's premises and confirming various details. All supporting documents to be verified with the originals by the branch personnel i.e. Relationship Manager (RM) / Authorized Partner (AP). RM/AP to identify client through discreet enquiry about the client's background, financial status, and location etc. Do not open accounts of clients who are not approachable or who do not produce the necessary documents/clarification in support of the details provided by the client. No account should be opened without a valid PAN number, which is verified with IT Dept. website.

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

DSL may rely on a third party for the purpose of identification and verification of the identity of a client and determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner provided such third party shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under the PML Act. Such reliance shall be subject to the conditions that are specified in Rule 9 (2) of the PML Rules and shall be in accordance with the regulations and circulars/ guidelines issued by SEBI from time to time.

In terms of Rule 9(2) of PML Rules, DSL shall:

a. Obtain necessary information of client due diligence carried out by third party, if any.
b. Take adequate steps to satisfy itself that copy(ies) of client identification data and other relevant documentation relating to client due diligence requirements will be made available from the third party upon request without delay
c. Satisfy itself that the 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 PMLA Act.
d. Take necessary measures to ensure that the third party is not based in a country or jurisdiction assessed as high risk
e. Be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable

Monitoring of Transactions

Regular monitoring of transactions is vital for ensuring effectiveness of the Anti-Money Laundering procedures. Following internal processes to be followed while monitoring the transactions:

a) Pay special attention to all complex, unusually large transactions / patterns which appear to have no economic purpose.
b) Monitor trading transactions of Dormant clients
c) Monitor transactions of clients with Fund In/Out >= 50 lacs through single entry in a day
d) All alerts received from Depositories (NSDL / CDSL) as well as generated from system as per the internal policy, to be duly investigated to ensure genuineness in terms of capacity of client to execute such transactions & source of meeting the obligations of those transactions. In broader sense to reassure on the following aspects:
    a. Verify client's KYC document along with PAN re-verification.
    b. Verify genuineness of transactions & Call confirmation records.
    c. Verify Bank transactions whether funds received from / paid in linked account only.
    d. Check whether the off-market transfer is done in his/her own A/c or not.
    e. In case the transaction is not from his /her own account then review the purpose of transaction for off-market transactions i.e. Loan, Corporate Action, Margin or else.
    f. In case of high transaction volume, check if client belongs to promoter group of the scrip

in question. Same to be verified from the independent source of information (like NSE/BSE web site about the promoters).

g. Sudden activity in dormant accounts which may raise doubt over the genuineness of transactions.
h. Unusual activity compared to past transactions.
i. Check if the client receives shares through off market & sells in market (either in small quantity or in single transaction), simultaneously made withdrawal after selling shares in market.
j. Check if the client's shares are sold in market irrespective of market price – non- profit motive or no economic rationale.
k. Check if the transactions appear to be the case of insider trading or transactions reflect likelihood of market manipulations.
l. Check if the executed transaction is of value just under reporting threshold amount which can be termed as an apparent attempt to avoid reporting.
m. Check if the payment pattern of client is inconsistent to his/her normal behavior.
n. Check if the block deal which is not at market price or prices appear to be artificially inflated / deflated.
o. Check abnormal trading activity like dealing in large quantities in penny stocks

e) Alerts received from the NSE/BSE are analyzed. Explanation and documentary evidences sought from the client. In case Client's response does not appear to be satisfactory then same is reported to Exchange for their further action. If facts of the matter warrant then STR are also filed with the FIU-India.
f) Records of transactions are preserved and maintained in terms of section 12 of the PMLA 2002 and that transaction of suspicious nature or any other transaction notified under section 12 of the act are reported to the Director – FIU-IND . Suspicious transactions also need to be reported to the relevant authority of DSL as well.
g) Compliance cell of DSL 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.
h) DSL also undertakes client due diligence measures for existing clients on the basis of materiality and risk as appropriate. The extent of such monitoring is in accordance with the risk category of the client.

Suspicious Transaction Monitoring and Reporting:

The Suspicious Transaction Report (STR) shall be furnished 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 once a suspicious transaction report is received from a branch or any other office. Such report shall be made available to the competent authorities on request. Further, the Principal Officer shall on being satisfied that the transaction is suspicious, furnish the information promptly in writing by fax or by electronic mail to the Director, FIU-IND.

DSL shall not put any restriction on operations in the accounts where an STR has been made. DSL and their directors, officers and employees (permanent and temporary) shall be prohibited from disclosing ("tipping off") the fact that a STR or related information is being reported or provided to the FIU-IND. This prohibition on tipping off extends not only to the filing of the STR and/or related information but even before, during and after the submission of an STR. Thus, it shall be ensured that there is no tipping off to the client at any level. In exceptional circumstances, consent may not be given to continue to operate the account and transactions may be suspended.

DSL, irrespective of the amount of transaction and/or the threshold limit envisaged for predicate offences specified in part B of Schedule of PMLA, 2002, shall file STR if they have reasonable grounds to believe that the transactions involve proceeds of crime.

Suspicious activity can occur either at the outset of the client relationship or long after the relationship has been initiated. Transactions are viewed in the context of other account activity and a determination of whether the transaction is actually suspicious would necessarily depend on the customer and the particular transaction, compared with the customer's normal business activity. Unusual or questionable transactions may include transactions that appear to lack a reasonable economic basis or recognizable strategy based upon what the firm knows about the particular customer. Examples of activity that may be indicative of unusual or potentially suspicious activity are provided to all appropriate firm personnel through standard distribution channels and are being incorporated into the firm's anti-money laundering policies and procedures, as well as its anti-money laundering training materials.

Any transactions that are related to unlawful activities such as fraud and market manipulation is equivalent to a suspicion that they are related to money laundering, and must be strictly reported.

Principal Officer ensures to take appropriate steps to enable suspicious transactions to be recognized and have appropriate procedures for reporting suspicious transactions. A list of circumstances which are 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 appears not to cooperate;
b. Asset management services for clients where the source of the funds is not clear or not keeping up with clients apparent standing /business activity;
c. Clients in high-risk jurisdictions or clients introduced by banks or affiliates or other clients based in high risk jurisdictions;
d. Substantial increases in business without apparent cause;
e. Unusually large transactions made by an individual or business;
f. Attempted/Transfer of investment proceeds to apparently unrelated third parties.
g. Unusual transaction by CSCs and businesses undertaken by offshore banks/financial services

In case transactions are abandoned or aborted by clients on being asked to give some details or to provide

documents then DSL shall report all such attempted transactions in STRs, even if not completed by clients, irrespective of the amount of the transaction.

Record and report STR of all suspicious transactions post assessment as per the prescribed format.

In addition to the above, DSL 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

DSL shall also send a copy of the communication mentioned above to the UAPA Nodal Officer of the State/UT where the account is held and to SEBI and FIU-IND, without delay.

DSL shall also intimate SEBI through email (sebi_uapa@sebi.gov.in) and also via post to -

The UAPA nodal officer of SEBI,
Deputy General Manager,
Division of FATF,
Market Intermediaries Regulation and Supervision Department,
Securities and Exchange Board of India,
SEBI Bhavan II, Plot No. C7, "G" Block,
Bandra Kurla Complex, Bandra (E), Mumbai 400 051

Reporting to Financial Intelligence Unit-India

In terms of the PML Rules, DSL shall report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) in respect of transactions referred to in Rule 3 at the following address:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Tower – 2, Jeevan Bharti Building
Connaught Place, New Delhi-110001.
Website: http://fiuindia.gov.in

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

Note: Cash Transaction Report (CTR), wherever applicable for a given month, shall be submitted to FIU-IND by 15th of the succeeding month.

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

DSL has put in place the system to ensure the implementation of the order issued by the Central Government/SEBI/FIU-India.

DSL shall ensure that in terms of Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) and amendments thereto, it does not have any accounts opened 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).

Procedure for implementation of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005

In accordance with the provisions of Section 12A of the Weapons of Mass Destruction (WMD) and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005 ("WMD Act"), the central government is empowered to –

1. Freeze, seize or attach funds or other financial assets or economicresources—
    a. owned or controlled, wholly or jointly, directly or indirectly, by suchperson; or
    b. held by or on behalf of, or at the direction of, such person; or
    c. derived or generated from the funds or other assets owned orcontrolled, directly or indirectly, by such person;
2. 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.

DSL, to comply with the order dated January 30, 2023 vide F. No. P-12011/14/2022-ES Cell-DOR ("the Order") issued by The Government of India, Ministry of Finance 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") has ensured the following –

1. List of individuals/entities ("Designated List") is maintained and updated at regular intervals.

2. 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, DSL shall not carry out such transaction and shall immediately, without delay, inform the transaction details with full particulars of the funds, financial assets or economic resources involved to the Central Nodal Officer ("CNO"), whose details are as under –

   The Director, FIU- India
   Tel.: 011-23314458
   Fax: 011-23314459
   Email: dir@fiuindia.gov.in

3. Run a check, on the given parameters, at the time of establishing a relation with a client and on a periodic basis to verify whether individuals and entities in the Designated List are holding any funds, financial assets or economic resources or related services, in the form of bank accounts, stocks, insurance policies etc. In case, the clients' particulars match with the particulars of Designated List, DSL 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.

4. Details of the concerned personnel forming a part of the Designated list are informed to the SEBI Nodal Officer, via email and post.
   a. Email: sebi_uapa@sebi.gov.in
   b. Address:
      SEBI Nodal Officer/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

5. Prevent the concerned individual/entity from conducting financial transactions, in case it is suspected that the funds / assets held by the concerned shall form a part of the Weapons of Mass Destruction (WMD) Act (Section 12A (2)(a) or Section 12A(2)(b)).
6. File a Suspicious Transaction Report (STR) with the FIU-IND covering all transactions in the accounts of individuals/entities ("Designated List")
7. DSL shall also comply with the provisions regarding exemptions from the above orders of the CNO and inadvertent freezing of accounts, as may be applicable.

List of designated Individuals/Entities:

The Ministry of Home Affairs, in pursuance of Section 35(1) of UAPA 1967, declares the list of individuals/entities, from time to time, who are designated as 'Terrorists'. DSL 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 by DSL.

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 .

1. 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.
2. 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.

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

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

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

Employees' Hiring/Employee's Training/ Investor Education

Hiring Policy

DSL is having adequate screening procedures in place to ensure high standards when hiring employees. The key position is identified having regard to the risk of Money Laundering and Terrorist Financing. DSL further ensures that the employees taking up such key positions are suitable and competent to perform their duties.

Employees' Training

DSL will have adequate procedure to provide ongoing employee training program so that the members of the staff are adequately trained in AML and CFT procedures. While sales people having direct contact with clients are in the best position to identify some forms of suspicious activity, other business units

or areas also benefits from training, including treasury, operations, margin, credit, corporate security, audit and legal and compliance.

Investors Education

Implementation of KYC procedures requires DSL to demand certain information from customer which may be of personal nature or which has hitherto never been called for. This sometimes leads to a lot of questioning by the customer as to the motive and purpose of collecting such information. The Relationship Managers of DSL shall be trained to explain to the customers the regulatory requirements and benefits of adhering to the KYC guidelines and seek co-operation of the customer.

Record Management:

DSL maintains and preserves the following information in respect of transactions referred to in Rule 3 of PML Rules:

a. Nature of the transactions;
b. Amount of the transaction and the currency in which it is denominated;
c. Date on which the transaction was conducted; and
d. Parties to the transaction.

Record Keeping

Principal Officer ensures that we are in compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made there-under, PML Act, 2002 as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars. It is ensured to maintain and preserve the records evidencing the identity of its clients and beneficial owners as well as account files and business correspondence for a period of five years after the business relationship between a client and intermediary has ended or the account has been closed, whichever is later.

The Principal Officer ensures that all customer transaction records and information are available on a timely basis to the competent investigating authorities. Further ensured to maintain and preserve the record of information related to transactions, whether attempted or executed, which are reported to the Director, FIU-IND, as required under Rules 7 & 8 of PML Rules, for a period of five years from the date of transaction between the client and the intermediary.

As per SEBI circular no. SEBI/HO/MRD2/DDAP/CIR/P/2020/153 dated August 18, 2020, regarding corrigendum to Master Circular for Depositories dated October 25, 2019 on preservation of records, which reads as “Depositories and Depository Participants are required to preserve the records and documents for a minimum period of 8 years”.

In case of any suspected laundered money or terrorist property, the competent investigating authority(ies) would need to trace through the audit trail for reconstructing a financial profile of the

suspect account. To enable this reconstruction, DSL 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
c. For selected transactions –
    - The origin of the funds
    - The form in which the funds were offered or withdrawn, e.g. cheques, demand drafts etc.
    - The identity of the person undertaking the transaction;
    - The destination of the funds;
    - The form of instruction and authority.

In addition to the above, DSL has also put in place a system of maintaining proper record of the nature and value of transactions which has been prescribed under Rule 3 of PML Rules as mentioned below –

a. All cash transactions of the value of more than ten lakh rupees 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. (*Note: for suspicious transaction 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 DSL.

Note:

- Incase DSL does not have records of the identity of its existing clients, it shall obtain the records forthwith, failing which DSL shall close the account of the clients after giving due notice to the client.
- The expression "records of the identity of clients" shall include updated records of the identification date, account files and business correspondence and result of any analysis undertaken under Rules 3 and 9 of the PML Rules

Retention of Records

Following documents shall be retained:

a. All necessary records on transactions, both domestic and international, shall be maintained at least for the minimum period prescribed under the relevant Act and Rules (PMLA and rules framed thereunder as well SEBI Act) and other legislations, Regulations or exchange bye-laws or circulars.

b. Records on client identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence shall also be kept for the same period.

Note: Incase DSL does not have the records of the identity of any of its existing client(s), it shall obtain the same forthwith. Incase the client does not provide the required documents / details i.e. the client is non-cooperative, then DSL shall proceed to terminate the business relationship with the said client i.e. close the client's account by giving him/her/it 30 days closure notice.