STOCKHOLDING SERVICES LIMITED

(A WHOLLY OWNED SUBSIDIARY OF STOCKHOLDING CORPORATION OF INDIA LIMITED)

ANTI MONEY LAUNDERING(AML) POLICY

(Version 07/2025)

INDEX

1. BACKGROUND

The Prevention of Money Laundering Act, 2002 (hereinafter **"PMLA"**) has been brought into force with effect from July 1, 2005 and it provides for Anti-Money Laundering and Anti-Terrorist Financing measures to be taken in India and the rules framed thereunder provides guidance on the practical implementation of the provisions laid down in the Act. The Director appointed by the Financial Intelligence Unit-INDIA (FIU-IND) has been conferred with exclusive and concurrent powers under relevant sections of the Act to implement its provisions. The Act imposes an obligation on banking companies, financial institutions and intermediaries associated with the securities market and registered with the Securities and Exchange Board of India (SEBI) under section 12 of SEBI Act, 1992 to adhere to client opening procedures and maintain records of such transactions as per applicable rules and regulations with respect to SEBI, PMLA, Stock Brokers & other applicable law/ rule/ regulations. The stock brokers fall under the category of intermediaries under section 12 of the SEBI Act, 1992, and hence the provisions of PMLA are also applicable to all the stock brokers. The establishment of Anti-Money Laundering programs by Market Intermediaries are one of the central recommendations of the Financial Action Task Force (FATF).

SEBI has issued necessary directives from time to time vide its circulars covering issues related to Know Your client (KYC) norms, Anti Money Laundering (AML), Client Due Diligence (CDD) and Combating Financing of Terrorism (CFT). This policy document is based on the SEBI's master circular on PMLA bearing reference no. ISD/AML/CIR-1/2010 dated February 12, 2010 and subsequent circulars bearing reference no. CIR/ISD/AML/2/2010 dated June 14, 2010, CIR/ISD/AML/3/2010 dated December 31, 2010, SEBI/HO/MIRSD/DOP/CIR/P/2019/113 dated October 15, 2019, SEBI/HO/MIRSD/MIRSD-SEC-5/P/CIR/2023/022 dated February 3, 2023, and SEBI Circular No. SEBI/HO/MIRSD/MIRSDSECFATF/P/CIR/2024/78 dated June 06, 2024 which consolidates requirements/ obligations to be fulfilled by all the registered intermediaries. This policy will be subject to changes in order to incorporate further directives that SEBI may give vide its circulars on PMLA, from time to time.

Applicability of PMLA

- Banking Company
- Financial Institution
- Intermediary (which includes a stock broker, sub-broker, share transfer agent, portfolio manager, other intermediaries associated with securities market and registered under section 12 of the SEBI Act,1992).

The aforesaid entities shall have to maintain a record of all the transactions as per applicable rules and regulations with respect to SEBI, PMLA, Stock Brokers & other applicable law / rule / regulation; the nature and value of such transactions include:

- All cash transactions > ₹10 Lakh or its equivalent in foreign currency
- All integrally connected series of cash transactions < ₹10 Lakh or its equivalent in foreign currency within one calendar month.
- All suspicious transactions, whether or not made in cash and including inter-alia credits or debits from any non-monetary account such as Demat account, security account maintained by SSL.

Offence under PMLA

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 including its concealment, possession, acquisition or use and projecting or claiming] it as untainted property shall be guilty of offence of money-laundering.

[Explanation- For the removal of doubts, it is hereby clarified that,

(i) a person shall be guilty of offence of money-laundering if such person is found to have directly or indirectly attempted to indulge or knowingly assisted or knowingly is a party or is actually involved in one or more of the following processes or activities connected with proceeds of crime, namely:—
(a) concealment; or
(b) possession; or
(c) acquisition; or
(d) use; or
(e) projecting as untainted property; or
(f) claiming as untainted property,

in any manner whatsoever;

(ii) the process or activity connected with proceeds of crime is a continuing activity and continues till such time a person is directly or indirectly enjoying the proceeds of crime by its concealment or possession or acquisition or use or projecting it as untainted property or claiming it as untainted property in any manner whatsoever.]

2. DEFINITION OF MONEY LAUNDERING

Money Laundering is the processing of criminal proceeds to disguise their illegal origin. It is a process by which persons with criminal intent or persons involved in criminal activities attempt to hide and disguise the true origin and ownership of the proceeds of their criminal activities, thereby avoiding prosecution, conviction and confiscation of illegal funds.

Although money laundering is a complex process, it generally follows three stages:

Placement is the initial stage in which money from criminal activities is placed in financial institutions. One of the most common methods of placement is structuring— breaking up currency transactions into portions that fall below the reporting threshold for the specific purpose of avoiding reporting or recordkeeping requirements.

Layering is the process of conducting a complex series of financial transactions, with the purpose of hiding the origin of money from criminal activity and hindering any attempt to trace the funds. This stage can consist of multiple securities trades, purchases of financial products such as life insurance or annuities, cash transfers, currency exchanges, or purchases of legitimate businesses.

Integration is the final stage in the re-injection of the laundered proceeds back into the economy in such a way that they re-enter the financial system as normal business funds. Banks and financial intermediaries are vulnerable from the Money Laundering point of view since criminal proceeds can enter banks in the form of large cash deposits.

Three most common stages of Money Laundering, as mentioned above are resorted to, by the launderers. The laundered proceeds re-enter the financial system appearing to be normal business funds and Market Intermediaries may unwittingly get exposed to a potential criminal activity while undertaking such normal business transactions. Market Intermediaries are therefore placed with a statutory duty to make a disclosure to the Authorized Officer when knowing or suspecting that any property, in whole or in part, directly or indirectly, representing the proceeds of a predicated offence, or was or is intended to be used in that connection is passing through the Market Intermediaries. Law protects such disclosures, enabling the person with information to be able to disclose the same without any breach of confidentiality. Market Intermediaries likewise need not abstain themselves from providing such information pertaining to its customers.

3. ADVERSE CONSEQUENCES OF MONEY LAUNDERING

1. **Finances Terrorism:**

   Money laundering provides terrorists with funds to carry out their activities

2. **Undermines rule of law and governance:**

   Rule of Law is a precondition for economic development – Clear and certain rules applicable for all. However, money laundering undermines rule of law by fueling corruption, weakening public trust in institutions, facilitating organized crime, and distorting economic markets

3. **Affects macro economy:**

   Money launderers put money into unproductive assets to avoid detection.

4. **Affects the integrity of the financial system:**

   Financial system advancing criminal purposes undermines the function and integrity of the financial system.

5. **Reduces Revenue and Control:**

   Money laundering diminishes government tax revenue and weakens government control over the economy.

6. **Suspicious Transaction**

   Suspicious Transaction means a transaction whether or not made in cash which, to a person acting in good faith:

   - Gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime

- Appears to be made in circumstances of unusual or unjustified complexity
- Appears to have no economic rationale or *bona-fide* purpose
- Gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.
- Identity verification or address details seems difficult or found to be forged/ false. Asset management services where the source of the funds is not clear or not in keeping with apparent standing/ business activity.
- Substantial increases in business without apparent cause.
- Unusual & Unexplained large value of transaction.
- Transfer of large sums of money to or from overseas locations.
- Unusual & Unexplained activity in dormant accounts.

4. FINANCIAL INTELLIGENCE UNIT (FIU)-INDIA

The Government of India has set up Financial Intelligence Unit (FIU)-INDIA on November 18, 2004 as an independent body to report directly to the Economic Intelligence Council (EIC) headed by Finance Minister.

FIU-IND has been established as the Central National Agency responsible for receiving, processing, analyzing and disseminating information related to suspected financial transactions. FIU-IND is also responsible for coordinating and stretching efforts of national and international intelligence and enforcement agencies in pursuing the global efforts against money laundering and related crimes.

5. ANTI MONEY LAUNDERING PROGRAM (AML)

The objective of having an AML Program is to have in place adequate policy, practice and procedure that help to prevent money-laundering activities. Such procedures would include the following:

- Appointment of Principal Officer
- Appointment of Designated Director
- Client Due Diligence is the main part of the policy and includes following:
    - Client Acceptance Policy
    - Client Identification Procedure
- Transaction monitoring to identify & report Suspicious Transactions (STR). The rules for identifying and reporting suspicious transactions would be mentioned separately in an AML procedure document.
- Record keeping & retention of records
- Co-operating with law enforcement agencies in their efforts to trace the money laundering transactions and persons involved in such activities
- On-going training to the employees to ensure strict adherence to Customer
- Due diligence requirements
- Reports to Financial Intelligence Unit-India (FIU-IND)

SSL has implemented the AML (PMLA regulations) Software procured from TSS Consultancy. This Anti Money Laundering System provides a means to prevent or report money laundering activities in the form of suspicious transactions by the clients using the risk based approach. With the help of this system SSL monitors, investigates and reports patterns of transactions of a suspicious nature. This enhances due diligence and also ensures compliance with AML regulations.

These procedures and standards would assist in knowing and understanding the activities of its existing and prospective clients and to prevent StockHolding Services Limited (SSL) from being used as a medium, intentionally or unintentionally for carrying out money laundering activities. The chapters ahead detail the AML program adopted by the company.

6. APPOINTMENT OF PRINCIPAL OFFICER

The Compliance Officer of the SSL shall act as the Principal Officer.

Responsibilities of Principal Officer:

The Principal Officer will ensure that:

1. The Board approved PMLA policy and AML Program is implemented effectively by the company.
2. The identification and assessment of potentially suspicious transactions are done on the regular basis.
3. SSL reports the suspicious transactions to the concerned authorities within the stipulated time as per the PMLA policy.
4. SSL is regularly updated regarding any changes/ additions/ modifications in PMLA provisions obtained through circulars etc.
5. SSL responds promptly to any request for information, including KYC related information, made by the regulators, FIU-IND and other statutory authorities.
6. Any other responsibilities assigned by Managing Director or any other official authorized by Managing Director with respect to the implementation of PMLA guidelines issued by SEBI/ Regulator/ Government Authority from time to time.

7. APPOINTMENT OF DESIGNATED DIRECTOR

MD & CEO of SSL shall act as Designated Director duly authorized by the Board as per the provisions of PMLA. Designated Director shall ensure overall compliance with the obligations imposed under chapter IV of the PMLA and the Rules as included in a) to f).

As per Rule 2(ba) of the PMLA Rules, the definition of a Designated Director reads as under:

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

8. CONSTITUTION OF PMLA COMMITTEE

The Designated Officer shall constitute a Surveillance PMLA Committee to facilitate operational convenience. This committee shall have representation from Operations, Risk Management and Legal departments.

The Committee shall have a Chairman appointed by the Designated Officer.

9. CLIENT DUE DILIGENCE:

9.1 Client Acceptance Policy:

Considering the potential threat of usage of the financial services by a money launderer, it is essential to make reasonable efforts to determine the true identity of clients. SSL has to put in place effective procedures to obtain requisite details for proper identification of new customers.

1. No account is opened in a fictitious/ benami name or on an anonymous basis.

2. All the clients shall require to disclose the details of designated bank account and designated demat account in the Account Opening Form. All the pay-in / pay–out of funds/ securities shall be routed through designated bank/ demat account only. No cash/ DD shall be accepted.

3. All KYC Documentations and Procedures shall be followed at the time of account opening and no account shall be opened where SSL is unable to apply appropriate CDD measures/ KYC policies. This may be applicable in cases where it is not possible to ascertain the identity of the client, or the information provided to the SSL is suspected to be non-genuine or there is perceived non-cooperation of the client in providing full and complete information

4. The submission of all documents required under this policy shall be pre- requisite for account opening for all clients. Incomplete application including incomplete documentation will be rejected. SSL will follow the industry standard for implementing client identification procedure.

5. The authorized official/ employees of company and Authorized person (AP's) shall personally verify the photograph of the client affixed on the Account Opening Form (AOF) and the proof of identity documents with the person concerned. A stamp of "Identity Verified in Person" must be affixed (as a proof of in Person Verification) on the AOF against the photograph of the client & on the proof of identity documents. The authorized official of the company and AP's who has done in- person verification and verified the documents with original should also sign on the AOF and ID proof.

6. Each original document shall be seen prior to acceptance of a copy. Stamp of "documents verified with originals" must be affixed along with the signature of the authorized person.

7. In case of any discrepancy or non-provision of information by the client, employees/ AP's shall seek necessary clarification from the applicant and activate the account only when the discrepancy is resolved or the deficiency is fulfilled. E.g. cases where names mentioned on the AOF and that on the PAN Card do not match etc.

8. Verify the customer's identity using reliable, independent source documents, data or information by following procedure:

    a. The PAN Card details should be verified with the name(s) appearing on the website of the Income Tax Department, http://incometaxindiaefiling.gov.in/challan/enterpanforchallan.jsp?pAction=Post and /or TIN website of NSDL e-governance. In case the name(s) do not match or the PAN Card details are not present in the PAN Card database, employees/ AP's should seek necessary clarification from the applicant(s) and activate the account only when the

discrepancy is resolved.

9. Reasonable precaution to be taken that no account is opened in a fictitious/ benami name or on an anonymous basis.

10. The applicant shall be required to disclose his/ her financial status and occupation details as required by PMLA.

11. Account Opening Form (AOF) shall strictly be as prescribed by Security Exchange Board of India.

12. If the applicant has completed KYC procedure with any KYC Registration Agency (KRA), in-person-verification shall be adequate.

13. In case of clients other than an Individual or trust, viz., company, partnership firm or un incorporated association / body of individuals, is shall be mandatory for such clients to disclose the beneficial ownership in them. In particular, following information shall be obtained from such clients:

    a. Shareholding pattern of the company having more than 10% holding in the share capital
    b. Profit sharing ratio of partners having more than 15% share in profit
    c. Any juridical person having more than 15% of the property or capital in an unincorporated association or body of individuals

In case the client is trust, the following information shall be obtained from such clients:

    a. List of 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.

14. With regard to client with a dubious reputation, SSL will obtain the information from various other legitimate sources like

    a. http://www.sebi.gov.in,
    b. http://www.sebi.gov.in/pmd/debarredco1.html, http://www.sebi.sebi.gov.in/pmd/debardirector1.html,
    c. http://www.sebi.gov.in/cis_prosecutiondata.html, http://www.sebi.gov.in/cis/noncisdata.html,
    d. http://www. watchoutinvestors.com/default2a.asp,
    e. UN Security Council website - http:// www.un.org/en/sc/,
    f. OFAC website - http://www.treasury.gov/about/organizational-structure/offices/Pages/Office-of-Foreign-Assets-Control.aspx etc.

15. SSL shall comply with the provisions of the Government order dated August 27, 2009 for implementation of Section 51A of the Unlawful Activities Prevention Act, 1967.

16. SSL shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process

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

9.2 Client Identification Process:

Guidelines on information needed to be obtained to identify BO.

In case of Natural Persons

Employee/ Dealer shall obtain sufficient data to verify identity of the customer, his address, his location and his recent photograph. It is required to find out whether customer is acting on behalf of another person as intermediary.

Employee/ Dealer shall ask for receipt of satisfactory evidence of the identity of the intermediary and person on whose behalf intermediary is acting and nature of arrangement.

In case of legal/ juridical persons

Employee/ Dealer shall verify legal status through the documents submitted.

Employee/ Dealer shall understand the ownership and control structure of such legal person and ascertain who are the natural persons in ultimate control of the legal person. Dealer shall identify such beneficial owners who control the legal person. Even the authorized signatories of the legal persons shall be ascertained and identified.

Also following precautions will have to be taken by SSL in order to ascertain that accounts are not misused by the clients or by any third parties for money laundering activities:

1. SSL will obtain information about the client as per the requirement mentioned in the AOF for the different categories of clients.
2. Verify client's identity by taking adequate documents/ information. The information must be adequate to satisfy competent authorities.
3. SSL will register clients as per SEBI/ BSE/ NSE/ MSEI/ MCX/ ICEX/ CDSL/ NSDL/ PMS guidelines and it will develop appropriate reporting system to monitor client's trades.
4. SSL shall periodically update all documents, data or information of all clients and beneficial owners collected under CDD process provided the client provides the information.
5. SSL shall implement the procedure to determine whether the potential client is a politically exposed person. PEPs are individuals who are or have been entrusted with prominent public functions in a foreign country e.g. Heads of States or of Governments, senior politicians, senior government, judicial or military officers, senior executives of the state owned corporations, important political party officials etc. In case of PEPs enhanced CDD measures shall be applicable as noted in the procedure It is required to obtain senior management approval for establishing/ continuing business relationship with PEPs.
6. Identify beneficial ownership and control i.e. determine which individual(s) ultimately own(s) or control(s) the client and/or the person, verify the identity of the beneficial owner
7. of the client and /or the person on whose behalf transaction is being conducted and understand the ownership and control structure of the client
8. Reasonable measures to be taken to verify the source of funds as well as the wealth of clients and beneficial owners identified as PEPs.
9. SSL shall conduct ongoing due diligence where inconsistencies in the information provided is noticed to follow the requirements enshrined in the PMLA, SEBI Act and Regulations, directives and circulars issued thereunder.
10. Undertake client due diligence ("CDD") measures to an extent that is sensitive to the risk of ML and TF depending on the type of client, business relationship or transaction

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

9.3 Parameters to Identify the level of Risk of Clients

At the time of acceptance: HNI, Trusts, PEPs and NRIs clients are considered as high risk clients.

During the course of Trading:

a. **High Risk Clients:** The clients whose single trade value in a day is more than Rs.5 lac are considered as high risk clients.
b. **Medium Risk Clients:** The clients whose single trade value in a day is less then Rs.5 lac and more than Rs. 2 lac are considered as Medium risk clients.
c. **Low Risk Clients:** The clients whose single trade value in a day is less then Rs.2 lac are considered as Low risk clients.

The transactions carried out by high and medium risk clients shall be monitored with special attention commensurate with the income declared by clients.

In addition to above, special emphasis shall be on identification of client/ BO who might be political exposed person (PEPs) from the various sources available in public domain and availing the services of the specialized agencies. Further, approval from the senior management shall be obtained for establishing business relationships with PEPs in case of a new client and where a client has been accepted and the client or beneficial owner is subsequently found to be PEP, approval from senior management shall be obtained to continue the business relationship with such client.

SSL shall carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect to its clients, countries or geographical areas, nature and volume of transactions, payment methods used by clients, etc. The risk assessment shall also take into account any country specific information that is circulated by the Government of India and SEBI from time to time, as well as, the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions (these can be accessed at the URL

http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml and http://www.un.org/sc/committees/1988/list.shtml)

The aforesaid parameters shall be revised from time to time.

10. RELIANCE ON THIRD PARTY FOR CARRYING OUT CLIENT DUE DILIGENCE (CDD)

1. SSL may rely on a third party for the purpose of (a)identification and verification of the identity of a client and (b) determination of whether the client is acting on behalf of a beneficial owner, identification of the beneficial owner and verification of the identity of the beneficial owner. Such third party shall be regulated, supervised or monitored for, and have measures in place for compliance with CDD and record-keeping requirements in line with the obligations under SEBI, PMLA, Stock Brokers & other applicable law / rule / regulations.

2. 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. SSL shall be ultimately responsible for CDD and undertaking enhanced due diligence measures, as applicable.

11. RECRUITMENT & TRAINING OF EMPLOYEES

SSL shall ensure adequate screening procedures at the time of hiring its staff. It shall also ensure that the employees dealing with PMLA requirements are suitable and competent to perform their duties.

SSL shall conduct PMLA awareness program for its existing employees to ensure that they are aware of their obligations under the provisions of PMLA.

SSL shall ensure that the new staff recruited by them is also given initial PMLA awareness training.

SSL shall also arrange for periodical refresher training to the staff to keep them updated on new developments and to communicate any changes in AML and CFT procedures, policies, etc.

SSL shall make periodic updates to the PMLA Policy on the intranet for creating awareness on PMLA among the employees.

12. INVESTOR EDUCATION:

SSL shall take measures to educate the Investor about the requirements, importance and necessity of the PMLA including any amendments, circulars and notifications through new letters, personal meetings etc, once the AML/ CFT measures are implemented investor is required to provide the sensitive information like documents evidencing his source of funds, his income tax returns, bank statements etc. Clients are likely to voice their apprehensions about the motive and purpose of collecting such information by SSL. In such case Dealer / back office staff members are required to make the investor aware that these requirements are arising from the AML/CFT framework. The Dealer / back office staff should prepare specific literature & pamphlets so as to educate the investor/ customer about the objectives of the AML/ CFT Program.

The letters are also required to be sent to the clients on the updates of the said program.

13. RECORD KEEPING & RETENTION OF RECORDS

SSL has put in place a system of maintaining proper record of the nature and value of transactions which has been prescribed under Rule 3 of PML Rules as mentioned below:

i) PMLA stipulates that records pertaining to all cash transactions greater than Rs. 10 lakhs its equivalent in foreign currency;

ii) all series of cash transactions integrally connected to each other which have been individually valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an amount of ten lakh rupees or its equivalent in foreign currency are maintained as per applicable rules and regulations with respect to SEBI, PMLA, Stock Brokers & other applicable law / rule / regulations. It may, however, be clarified that for the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' shall also be considered.

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

iv) all suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into or from any non-monetary account such as demat account, security account maintained by the registered intermediary.

Information to be maintained:

SSL shall maintain and preserve the following information in respect of transactions referred to in Rule 3 of PML Rules:

i. the nature of the transactions;

ii. the amount of the transaction and the currency in which it is denominated;

iii. the date on which the transaction was conducted; and

iv. the parties to the transaction.

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

PMLA further stipulates that all relevant documents like Account Opening Forms and their supporting documents, business correspondence and all instructions for operating the account given by client or its duly registered Power of Attorney shall be maintained for a period of five years as per applicable rules and regulations with respect to SEBI, PMLA, Stock Brokers & other applicable law / rule / regulations after the business relationship between a client and intermediary has ended or the account has been closed, whichever is later.

Records of information related to transactions, whether attempted or executed, which are reported to the Director, FIU – IND as per applicable rules and regulations with respect to SEBI, PMLA, Stock Brokers & other applicable law / rule / regulations shall be maintained and preserved for a period of five years from the date of the transaction between the client and the intermediary.

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

In view of above, SSL shall maintain the records in terms of the provisions of applicable rules and regulations with respect to SEBI, PMLA, Stock Brokers & other applicable law / rule / regulation. The retention period shall be modified on receiving appropriate instructions from any regulatory authority like SEBI, FIU-IND or any other statutory authority or change in applicable law.

14. MONITORING OF TRANSACTIONS

In addition to the parameters laid down in clause no 9.3, SSL shall pay special attention to all complex, unusually large transactions and all unusual patterns which have no apparent economic or visible lawful purpose.

The Compliance Department shall ensure adherence to the KYC policies and procedures. Internal Auditors shall specifically check and verify the application of KYC procedures and comment on the lapses if any observed in this regard. All staff members shall be provided training on Anti Money Laundering. The focus of training shall be different for frontline staff, compliance staff and staff dealing with new customers. SSL shall pay special attention to all complex unusually large transactions / patterns which appear to have no economic purpose.

The Compliance Department shall randomly examine a selection of transactions/ clients and comment whether any suspicious transactions are done or not. While monitoring the transactions, SSL may shift the clients from one category to another depending upon the risk perceived by SSL.

15. IDENTIFYING OF SUSPICIOUS TRANSACTIONS

SSL shall maintain records of debits and credits of transactions through various services to the clients, as per their specific instructions.

The Rules notified under the PMLA defines a "suspicious transaction" as a transaction whether or not made in cash which, to a person acting in good faith. The list mentioned below 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 Give rise to reasonable ground of suspicion that it may involve proceeds of crime
b) Clients appears to be made in circumstances of unusual or unjustified complexity; or
c) Clients appears to have no economic rationale or bona fide purpose.
d) Clients whose identity verification seems difficult or clients that appear not to cooperate
e) Clients based in high risk jurisdictions;
f) Substantial increases in business without apparent cause
g) Clients transferring large sums of money to or from overseas locations with instructions for payment in cash
h) Attempted transfer of investment proceeds to apparently unrelated third parties
i) Unusual transactions by CSCs and businesses undertaken by offshore banks/financial services

16. REPORTING OF SUSPICIOUS TRANSACTIONS:

The staff of the operations department concerned shall monitor all transactions executed by clients and report to the PMLA Committee any transaction that appears to be of suspicious nature. Also system generates file of suspicious transactions based on few set parameters and informs CR staff to download such data for further investigation. The Principal Officer shall analyze and examine such data and then decide if any transaction listed therein warrants a closer inspection or not. He shall maintain the records of all such data received from authority and record the action taken against any client for suspicious transactions.

In case the Principal Officer comes across any transaction that appear to be of suspicious nature, he shall also submit the report of such transactions directly to The Director, FIU-IND in the prescribed format, within seven working days of establishment of suspicion.

SSL shall not put any restriction on operation in the accounts of any client where an STR has been made and the same has been reported to FIU-IND. SSL shall also be prohibited from disclosing the same to the client for whom the STRs have been reported to FIU-IND. However, in exceptional circumstances consent may not be given to continue to operate the account, and transaction may be suspended.

17. FREEZING & UNFREEZING OF FUNDS, FINANCIAL ASSETS OR ECONOMIC RESOURCES OR RELATED SERVICES

For implementation of section 51A of the Unlawful Activities (Prevention) Act,1967 (UAPA) i.e. freezing and unfreezing of funds, financial assets or economic resources, SSL will follow the procedure as laid down in Order issued by Central Government dated March 14, 2019.

PMLA software also updates the list of individuals / entities linked to Al – Qaida, UN or other specified list. As such before opening any new trading account it is ensured that name of the proposed customer does not appear in the said lists. Also existing trading accounts are scanned to ensure that no account is linked to any of the entities or individuals included in the list. As such, SSL strictly follows the procedure laid down in the UAPA order dated August 27, 2009.

SSL shall time to time abide and comply with the circulars and guidelines issued by the Regulators/Exchanges and other law enforcement agencies.

18. PROCEDURE FOR IMPLEMENTATION OF SECTION 12A OF THE WEAPONS OF MASS DESTRUCTION AND THEIR DELIVERY SYSTEMS (PROHIBITION OF UNLAWFUL ACTIVITIES) ACT, 2005 – DIRECTIONS TO STOCK EXCHANGES AND REGISTERED INTERMEDIARIES

The organization adheres to the provisions of Section 12A of the Weapons of Mass Destruction and their Delivery Systems (Prohibition of Unlawful Activities) Act, 2005, (hereinafter "WMD") as well as the Ministry of Finance Order dated January 30, 2023 (F. No. P-12011/14/2022-ES Cell-DOR).

The detailed procedure is governed by the Government of India Order accessible at: **DoR_Section_12A_WMD.pdf.**

19. DISCLOSURES

The Policy shall be uploaded on the website of the Company www.stockholdingservices.com.

20. REVIEW OF POLICY

The Board shall review the Policy at least once a year for making suitable amendments for better implementation of the Policy. The Company shall reserve the rights to review and make amendment to the Policy from time to time as it deems fit in accordance with the applicable laws, rules and regulations for the time being in force. The power to interpret and administer the Policy shall rest with the Board whose decision shall be final and binding.

21. LIMITATION

In the event of any conflict between the provisions of this Policy and of the provisions laid down under PMLA, or any other legal requirement dealing with the Money Laundering ("Applicable Law"), and/ or for the matter not provided for in the Policy, the provisions of the Applicable Law shall prevail accordingly.

22. AMENDMENT IN LAW

Any subsequent amendment/ modification to the Applicable Law shall automatically apply to this Policy.

****