

## POLICIES AND PROCEDURE FOR PREVENTION OF MONEY LAUNDERING

*(Issued as per the requirements of the PMLA Act 2002 and in compliance with the changes suggested by SEBI vide their Master Circular no. SEBI/HO/MIRSD/DOS3/CIR/P/2019/113 dated October 15, 2019)*

### **1 Background:**

Pursuant to the recommendations made by the Financial Action Task Force (formed for combating money laundering), Government of India had notified the Prevention of Money Laundering Act in 2002. SEBI had issued the Guidelines on Anti Money Laundering Standards vide their notification No. ISD/CIR/RR/AML/1/06 dated 18<sup>th</sup> January 2006 and vide letter No. ISD/CIR/RR/AML/2/06 dated 20<sup>th</sup> March 2006 had issued the obligations of the intermediaries registered under Section 12 of SEBI Act, 1992. As per these SEBI guidelines, all intermediaries have been advised to ensure that proper policy frameworks are put in place as per the Guidelines on Anti Money Laundering Standards notified by SEBI. The objective of the SEBI guidelines is that a registered intermediary and any of its representatives should implement, identify and discourage any money laundering or terrorist financing activities. The overriding principle is that the registered intermediary should be able to satisfy themselves that the measures taken by them are adequate, appropriate and follow the spirit of these measures and the requirements as enshrined in the Prevention of Money Laundering Act, 2002 (PMLA) and the Government of India Notification dated 1 July, 2005.

The PMLA has been further amended vide notification dated March 6, 2009 and inter alia provides that violating the prohibitions on manipulative and deceptive devices, insider trading and substantial acquisition of securities or control as prescribed in Section 12 A read with Section 24 of the Securities and Exchange Board of India Act, 1992 (SEBI Act) will now be treated as a scheduled offence under schedule B of the PMLA.

### **Prevention of Money Laundering Act, 2002**

Prevention of Money Laundering Act, 2002 (PMLA 2002) forms the core of the legal framework put in place by India to combat money laundering. PMLA 2002 and the Rules notified there under came into force with effect from July 1, 2005. The PMLA 2002 and Rules notified there under impose an obligation on intermediaries (including stock brokers and sub-brokers) to verify identity of clients, maintain records and furnish information to the Financial Intelligence Unit (FIU) - INDIA

### **Financial Intelligence Unit (FIU) – INDIA**

The Government of India set up Financial Intelligence Unit-India (FIU-IND) on November 18, 2004 as an independent body to report directly to the Economic Intelligence Council (EIC) headed by the Finance Minister. FIU-IND has been established as the central national agency responsible for receiving, processing, analyzing and disseminating information relating to suspect 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.

As per these SEBI guidelines, all intermediaries have been advised to ensure that proper policy frameworks are put in place as per the Guidelines on Anti Money Laundering Standards notified by SEBI.

NSE and BSE vide their circular dated January 25, 2006 had suggested the criteria on which suspicious secondary market transactions can be identified by a SEBI registered broker. CDSL vide their circular dated November 13, 2007 had notified criteria for generating alerts.

## **2 . Responsibility of VSE Stock Services Limited (VSSL)**

By virtue of being a SEBI Registered stock broker of BSE, NSE and MSEI, Depository Participant of CDSL, it is mandatory on the party of VSSL to have appropriate Anti Money Laundering policy and record All suspicious transactions whether or not made in cash and including, inter-alia, credits or debits into from any non-monetary account such as demat account, security account maintained by VSSL.

## **3 What is Money Laundering?**

Money Laundering can be defined as engaging in financial transactions that involve income derived from criminal activity, transactions designed to conceal the true origin of criminally derived proceeds and appears to have been received through legitimate sources/origins.

This is done in three phases – Placement Phase, Layering Phase & Integration Phase.

## **Objectives of the PMLA Act**

The objectives of the Act is to prevent money laundering and to provide for confiscation of property derived (including financial assets) from or involved in money laundering and punish those who commit the offence of Money laundering

## **4 . Objectives of the Policy:**

VSSL is committed to examining its Anti - Money Laundering strategies, goals and objectives on an on-going basis and maintaining an effective Anti - Money Laundering program for its business that reflects the best practices for a diversified, retail financial services firm.

VSSL AML Policy is designed to ensure that it complies with the requirements and obligations set out in India legislation, regulations, rules and Industry Guidance for the financial services sector, including the need to have adequate systems and controls in place to mitigate the risk of the firm being used to facilitate financial crime. The AML Policy sets out the minimum standards which must be complied with by VSSL and includes:

- The appointment of a Money Laundering Reporting Officer (MLRO) of sufficient seniority, who have responsibility for oversight of compliance with relevant legislation, regulations, rules and industry guidance;
- Establishing and maintaining a Risk Based Approach (RBA) towards assessing and managing the money laundering and terrorist financing risks to the Group;
- Establishing and maintaining risk-based customer due diligence, identification, verification and know your customer (KYC) procedures, including enhanced due diligence for those

**VSE Stock Services Limited**

- customers presenting higher risk, such as Politically Exposed Persons (PEPs), Non Resident Indians (NRIs);
- Establishing and maintaining risk based systems and procedures to monitor ongoing customer activity;
  - Procedures for reporting suspicious activity internally and to the relevant law enforcement authorities as appropriate;
  - The maintenance of appropriate records for the minimum prescribed periods;
  - Training and awareness for all relevant employees;
- 
- Customer acceptance policies and procedures, which are sensitive to the risk of money laundering (ML) and terrorist financing (TF) are adopted.
  - Customer Due diligence (CDD), to the extent that is sensitive to the risk of money laundering and terrorist financing depending on the type of customer, business relationship or transactions is undertaken
  - Staff Members' awareness and vigilance to guard against money laundering and terrorist financing is developed.
  - To have system in place for identifying, monitoring and reporting suspected Money Laundering or Terrorist Financing; and
  - The provision of appropriate management information and reporting to senior management of VSSL's compliance with the requirements;

In compliance with these obligations VSE Stock Services Limited (VSSL) had framed appropriate policies and procedures for prevention of Money laundering had released this updated version after incorporating the changes suggested by SEBI vide their Master Circular no. SEBI/HO/MIRSD/DOS3/CIR/P/2019/113 dated October 15, 2019. The said master circular had superseded the earlier master circular on AML/CFT dated July 4, 2018 by SEBI.

### **5 .(a) Principal Officer:**

To ensure the implementation of PMLA Act, with true spirit and to properly discharge the legal obligations to report suspicious transactions to the authorities, the company has designated **Mr/Mrs. \_\_\_\_\_ (Name & Designation)** of the Company as the Principal Officer for our Anti-Money Laundering Program. He would act as a central reference point in facilitating onward reporting of suspicious transactions and for playing active role in the identification and assessment of potentially suspicious transactions and shall report senior management i.e. Board of Directors. Any change in name, designation and addresses including email addresses of the Principal Officer to be intimated to the office of the Director –FIU.

The Principal Officer will constantly review the AML Policy of VSSL covering the areas of identification / verification / acceptance of customers and the parameters of identification of suspicious transaction.

The Principal Officer will give an orientation to all the concerned staff of VSSL on the guidelines of FIU/SEBI and the identification of Suspicious Transactions on a regular basis.

Some of these suggested measures may not be applicable in every circumstance to each business activity. However, keeping in mind, the specific nature of its business, type of customer and transactions in each business division, VSSL has to satisfy itself that the measures taken are adequate and appropriate to follow the spirit of these guidelines.

## **5 .(b) Designated Director**

An Executive/Non Executive Director is appointed as Designated Director (as per requirements under the PML Act / Rules) for the purpose of PMLA by way of Resolution by Board of Directors and the appointment is intimated to FIU and regulatory authorities, as required. Changes in the Designated Director are all intimated to FIU and regulatory authorities, as required. The

Designated Director is responsible for overall compliance of the obligations imposed under the PML Act and the Rules. The Principal Officer will keep the Designated Director informed of all measures taken for anti-money laundering and all suspicious transactions reported to FIU. Designated Director will bring to the notice of the other directors / Board of Directors all important matters as may be deemed fit. For non-compliance in AML/CFT measures the FIU may penalize the Designated Director.

## **6 .Procedures:**

**A. Procedures shall interlay include three specific parameters for Client Due Diligence Process (CDD) which comprises:**

- a. Policy for acceptance of Clients
- b. Procedure of identifying clients
- c. Transactions monitoring and reporting suspicious transactions (STR)

**B. Client Due Diligence (CDD) measures involve the following:**

Obtaining sufficient information about the client in order to identify who beneficially own or controls the securities account .If the beneficial owner is person other than the client then the party shall be identified by using client identification and verification process involving:

- Verify the client's identity using reliable, independent source documents, data or information
- Identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the client and/or the person on whose behalf a transaction is being conducted -

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, and includes a person who exercises ultimate effective control over a legal person or arrangement.

For clients other than Individuals and Trust, viz., Company, Partnership, or un-incorporated association/body of individuals, VSSL should identify the beneficial owners of the client and take reasonable measures to verify the identity of the person through following information:

- *the identity of the Beneficial person/natural person who is acting alone or together or through one or more juridical person, exercises control through ownership or who ultimately has a controlling ownership interest of more than 25% of shares or capital or profits of the*  
**VSE Stock Services Limited**

*juridical person, where juridical person is a Company.*

- *15% of shares / property or capital or profits of the juridical person, where juridical person is a partnership firm/Unincorporated association or body of individuals.*

*Control can be exercised through voting rights, agreement, arrangements or any other manner.*

*Where no natural person identified in the aforesaid paras the identity of relevant natural person who holds the position of senior managing official shall be considered as beneficiary.*

*In case of Trust beneficial owner or the natural person could be the settler of the trust, the trustee, the protector or the beneficiaries with more than 15% interest and any other natural person exercising ultimate effective control over the trust through a chain of control or ownership*

*Such indemnification of beneficiary is not mandatory in case of listed companies or majority owned subsidiary of such Company and in case of foreign investors)*

VSSL should be guided by SEBI circular CIR/MIRSD/11/2012 dated September 5, 2012 and CIR/MIRSD/07/2013 dated September 12, 2013 and such amendments thereto from time to time for identification of beneficial ownership of the Client or foreign investors Internal Auditors of VSSL shall monitor compliance of aforementioned provision on identification of beneficial ownership through half yearly audits.

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 6(B) and understand the ownership and control structure of the client.

- Conduct ongoing due diligence and scrutiny of the account/client to ensure that transaction conducted are consistent with the client's background/financial status, its activities and risk profile. Every year the financial statements to be taken on record for all corporate clients.
- Though it is not possible to know all the details and exact details of the client's background and financial status, it should be our endeavor to make a genuine attempt towards achieving this.

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

In-person verification and verification of document copies of clients / prospective clients against originals are to be done and reliance on third parties / external entities, where necessary, in accordance with SEBI / Exchange / Regulatory guidelines in this regard as may be amended from time to time. *{At this point in time, in case of stock brokers, their sub-brokers or Authorized Persons i.e. APs (appointed by the stock-brokers after getting approval from concerned stock exchanges) can perform In-Person Verification – as per SEBI Circular dated December 23, 2011}.*

Apart from the above, for the purpose of client on-boarding, there may be reliance on third parties would for introducing prospective clients to VSE Stock Services Limited and to assist in (i) procuring documentation from them; (ii) completion of account opening formalities with such prospective clients. And (iii) to determine whether client is acting on behalf a beneficiary and conduct the verification of identity of the client

## **6(a) Policy for acceptance of Clients**

### **I. For New Clients**

- Each client should be met in person, before accepting the KYC. The client should be met at the address given in the KYC. This will ensure that the address is also verified. Verify the PAN details on the Income Tax website.
- All documentary proofs given by the client should be verified with original.
- Documents like latest Income Tax returns, annual accounts, etc. should be obtained for ascertaining the financial status. If required, obtain additional information/document from the client to ascertain his background and financial status. VSSL may seek additional documents based on the perceived risk of the clients
- Obtain complete information about the client and ensure that the KYC documents are properly filled up, signed and dated. Scrutinize the form thoroughly before forwarding it to HO for account opening.
- All the payment should be received from the clients through his bank account provided in the KYC form or subsequently mapped to his trading account through modification form. No payment should be received from third party account and if the client attempt to make the payment from third party account or wants to deposit cash, same should be noted as suspicious transactions for the purpose of STR
- Ensure that the details mentioned in the KYC matches with the documentary proofs provided and with the general verification done by us.
- If the client does not provide the required information, then we should not open the account of such clients.
- As far as possible, a prospective client can be accepted only if introduced by VSSL's existing client. However, in case of walk in client, extra steps should be taken to ascertain the financial and general background of the client.
- VSSL should not open any accounts in fictitious/benami/anonymous basis.
- VSSL should not open accounts if executives responsible for opening client accounts are unable to apply appropriate KYC procedures.
- The Accounts should not be opened where identity of client cannot be ascertained, or there is a non-co- operation from the client in providing full & complete information, VSSL should treat such cases VSSL as suspicious and report as STR.

### **II. Existing clients**

- Keep updating the financial status of the client by obtaining the latest Income Tax Return, Net worth Certificate, Annual Accounts or other prescribed documents.
- Update the details of the client like address, contact number, demat details, bank details etc. And keep the Account Opening Team at HO informed of the same. In case, at any point of time, Executive/s are not able to contact the client either at the address or on the phone number, please stop dealing for the client and inform the Principal Officer.
- Check whether the client's identity matches 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 local enforcement/regulatory agency. For scrutiny / back ground check of the clients / HNI / ultra - HNIs, websites such as [www.watchoutinvestors.com](http://www.watchoutinvestors.com) should be referred. Also, Prosecution Database/ List of Vanishing Companies available on [www.cibil.com](http://www.cibil.com) should be checked.

- Scrutinize minutely the records / documents pertaining to clients of special category (like Nonresident clients, High Net worth Clients, Trusts, Charities, NGOs, Companies having close family shareholding, Politically exposed persons of foreign origin, Current/Former Head of State, Current/Former senior high profile politician, Companies offering foreign exchange offerings, etc.) or clients from high-risk countries (like Libya, Pakistan, Afghanistan, etc.) or clients belonging to countries where corruption/fraud is highly prevalent.
- Review the above details ongoing basis to ensure that the transactions being conducted are consistent with our knowledge of customers, its business and risk profile, taking into account, where necessary, the customer's source of funds
- Role of Relationship Manager/Dealer/Corporate Settlement/Accounts Department .They should not collect cash from the client and all dues and payments should be made directly from the designated bank account of the client to the broker's account ,collections of cheques may be avoided.
- Ensure that there are no third party receipts into / payment from the clients account. Ensure that any information gathered during formal or informal conversation with clients relating to Money Laundering is passed on to the Principal Officer through your Branch/Department Head.

## **I. RISK PROFILING OF THE CLIENT**

### **1. RISK-BASED APPROACH AND RISK PROFILING OF THE CLIENT**

The Company should accept the clients based on the risk they are likely to pose. The aim is to identify clients who are likely to pose a higher than average risk of money laundering or terrorist financing. For this purpose, we need to classify the clients as Low risk, medium risk and high risk clients. By classifying the clients, we will be in a better position to apply appropriate customer due diligence process. That is, for high risk client we have to apply higher degree of due diligence. The factors of risk perception depend on client's KYC details, location, nature of business/trading activity, turnover, nature of transaction, manner of payment etc.

- In order to achieve this objective, all clients should be classified in the following category:
  - Category A – Low Risk
  - Category B – Medium Risk
  - Category C – High risk

#### **High Risk**

- a. Nonresident clients
- b. High net worth clients
- c. Trust, Charities, NGOs and organizations receiving donations
- d. Politically exposed persons (PEP) of foreign origin
- e. Current / Former Head of State, Current or Former Senior High profile politicians and connected persons (immediate family, Close advisors and companies in which such individuals have interest or significant influence)
- f. Companies offering foreign exchange offerings

- g. Clients in high risk countries. While dealing with clients from or situate 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 suspect, intermediaries apart from being guided by the Financial Action task Force (FATF) statements that inter alia identify such countries or geographic areas that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website ([www.fatf-gafi.org](http://www.fatf-gafi.org)) from time to time, shall also independently access and consider other publicly available information along with any other information which they may have access to. However, this shall not preclude intermediaries 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. on face to face clients
- h. Clients with dubious reputation as per public information available etc.

### **Medium Risk**

Individual and Non-Individual clients falling under the definition of Speculators, Day Traders.

### **Low Risk**

Senior Citizens, Salaried Employees and a major portion of client who indulge in delivery based trading.

- Company has to be careful while monitoring the transactions of B and C category clients. Where a client is classified under Medium or High Risk category, said accounts should be kept under supervision of Principal Officer and take action as and when required.
- Apart from this company need to exercise extra caution while monitoring the transactions of NRI/NRE/PIO and foreign clients, especially when the payment is being made in foreign currency.
- Any change in the risk profile of the client same is modify in our system as per risk category defined above.



## 2. RISK ASSESSMENT

Broker Name shall carry out risk assessment to identify, assess and take effective measures to mitigate its money laundering and terrorist financing risk with respect:

- Clients.
- Countries or geographical areas,
- Nature and volume of transactions,
- Payments methods used by clients,
- large number of accounts having a common account holder,
- Unexplained transfers between multiple accounts with no rationale,
- Unusual activity compared to past transactions,
- Doubt over the real beneficiary of the account,
- Payout/pay-in of funds and securities transferred to /from a third party,
- Off market transactions especially in illiquid stock and in F&O, at unrealistic prices, Large sums being transferred from overseas for making payments,
- In consistent with the clients' financial background.
- 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 reference shall be made to the updated list of individuals and entities who are subjected to sanction measures as required under the various United Nations' Security Council Resolutions which shall be accessed from [http://www.un.org/sc/committees/1267/aq\\_sanctions\\_list.shtml](http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml), And <http://www.un.org/sc/commitees/1988/list.shtml>.

The risk assessment carried out shall consider all the relevant risk factors before determining the level of overall risk and the appropriate level and type of mitigation to be applied.

The assessment shall be documented, updated regularly and made available to competent authorities as and when required.

- A detailed search to be carried out to ensure that the Client is not in defaulters / negative list of regulators. (Search shall invariably be carried out on SEBI website [www.sebi.gov.in](http://www.sebi.gov.in), Ministry of Corporate Affairs sponsored website [www.watchoutinvestors.com](http://www.watchoutinvestors.com) and UN website at [http://www.un.org/sc/committees/1267/aq\\_sanctions\\_list.shtml](http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml).)

## 3. CLIENTS OF SPECIAL CATEGORY

- Non-resident clients,
- High net-worth clients [high net worth client could be classified as, if at the account opening time or during the course of the trading relationship, it is realized that the client's investment or the appetite for investment is very high.]
- Trust, Charities, NGOs and organizations receiving donations,
- Companies having close family shareholdings or beneficial ownership,

- Politically exposed persons (PEP). Politically exposed persons 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 /military officers, senior executives of state-owned corporations, important political party officials, etc. The additional norms applicable to PEP as contained in the subsequent clause 5.5 (Page 19 of the Master Circular) shall also be applied to the accounts of the family members or close relatives of PEPs,
- 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 center, tax havens, countries where fraud is highly prevalent,
- Non face to face clients,
- Clients with dubious reputation (define : If a client’s reputation during the opening of the account or post opening the account is known to be not good, then the same is marked in “client with dubious public reputation” category.) as per public information available etc.
- Where the client is a juridical person, verify that any person purporting to act on behalf of such client is so authorized and verify the identity of that person.

#### **6 b. Procedure of identifying clients:**

##### **Objective:**

To have a mechanism in place to establish identity of the client as prescribed by regulations to mitigate opening of fictitious / benami accounts.

##### **➤ Client identification procedure:**

##### **We follow the following principles:**

1. VSSL should carry out the identification process at the time of on boarding the client, during the transaction stage and there arises any doubts over veracity and adequacy of information submitted by the clients.
2. The client identification process should be enhanced when there is an apprehension that an existing client or potential client is politically exposed person .The source of fund of PEP should be verified.
3. The approval of senior management should be in place if an existing client becomes PEP.
4. SEBI has prescribed the minimum requirements relating to KYC for certain class of the registered intermediaries from time to time The client should be identified by using reliable sources (as permitted by SEBI, Exchanges, Depositories or other regulators) including documents / information.
5. The information should be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed in compliance with the Guidelines. Each original document must be seen before accepting copy.
6. Failure by prospective client to provide satisfactory evidence of identity or inconsistencies in the documentation provided by prospective client should be noted and reported to the higher

- authority within the organization before opening such account.
7. No minimum or threshold /category wise exemption is available for carrying out CDD this should be strictly implemented and non-compliance shall be attract appropriate sanctions.
  8. To conduct ongoing due diligence

**Documents which can be relied upon identifying the clients:**

Whereas most of the clients are acquired through the personal contacts of relationship manager/dealers, additionally veracity of following documents plays a pivotal in identification of clients:

**PAN CARD:** It is a mandatory and most reliable document as only one card is issued to an individual and once can independently check its genuineness through IT website.

**Other Identity Proofs:** Many a times Pan Card carries the old photograph of the client which does not match current facial features of the client or the signature affixed on the same might have changed by the client due to passage of time. In such a scenario other ID proofs like passport, voter id, Aadhar Card or any other proofs issued by Government or PSU bank may additionally take and relied upon.

**Address Proof:** For valid address proof we can rely on Voter's Identity Card, Passport, Bank Statement, Aadhar card, Ration card and latest Electricity/telephone bill in the name of the client.

**In case of corporate clients, duly certified copies of following documents can be obtained**

- Copy of the Registration/Incorporation Certificate
- Copy of the Memorandum & Articles of the Association
- Copy of the PAN card and the Director Index No. (DIN)
- Copy of the latest audited Annual Statements of the corporate client
- Latest Net worth Certificate
- Latest Income Tax return filed.
- Board Resolution for appointment of the Authorized Person who will operate the account.
- Proof of address and identity of Authorized Person

**In case of partnership firm one certified copy of the following must be obtained:**

- Registration certificate
- Partnership Deed
- PAN card of partners
- Authorization letter for the person authorized to open and operate the account
- Proof of identity and address of the authorized person.
- Annual statement/returns of the partnership firm

**In case of a Trust, one certified copy of the following must be obtained:**

- Registration certificate
- Trust Deed
- PAN card
- Authorization letter for the entity authorized to act on their behalf
- Officially valid documents like PAN card, voters ID, passport, etc. of person(s) authorized to transact on behalf of the Trust.

In case of unincorporated association or a body of individuals, one certified copy of the following must be obtained:

- Resolution of the managing body of such association or body of individuals
- POA in favor of person authorized to transact
- Officially valid documents like PAN card, voters ID, passport, etc. of the person(s) authorized to transact
- Any document required by VSSL to establish the legal existence of such an association or body of individuals.

In cases of an NRI account – Repatriable / non-repatriable, the following documents are required:

- Copy of the PIS permission issued by the bank
- Copy of the passport
- Copy of PAN card
- Proof of overseas address and Indian address
- Copy of the bank statement
- Copy of the demat statement
- If the account is handled through a mandate holder, copy of the valid POA/mandate

### Procedure for identifying politically Exposed Persons (PEP)

- Politically Exposed Persons' (PEP) 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/military officers, senior executives of state-owned corporations, important political party officials, etc.
- Hence Besides obtaining declaration from the client on the KYC form about his PEP status where ever possible the concerned RMs/Branch Heads or person responsible for acquiring clients should independently check the antecedents of the clients and verify whether they fall into the category of PEP as per the definition given in Para (a).
  - In case of the clients who are PEP or subsequently found to be PEP or become PEP, the concerned RMs/Branch Heads or any other person should obtain the approval of CEO or Business Head for continuing the business relationship with such client.

#### **FOR NEW CLIENTS:**

#### **Additional checks at the time of account opening / account modifications:**

1. In case of corporate clients, we shall validate and confirm the CIN, registered address and directors of the corporate, as provided in the KYC form with the information freely accessible on the Government portals such as MCA (Ministry of Corporate Affairs) before opening the account.
2. Similarly at the time of intimation by the corporate entity regarding change in directors or address, similar verification will be done by the account opening team with details on MCA / ROC portals before effecting such changes. .
3. In case no satisfactory explanation of the discrepancy is obtained and the discrepancy is not resolved and it is felt that there are suspicious reasons for the same, the matter along with reasons for suspicion should be brought to the notice of the Principal Officer (FIU) and Principal Officer shall file an STR with FIU regarding such account.
4. In case of accounts of partnership firms, account opening team shall check the Partnership Deed of the entity to ensure no HUF is a partner in the firm. In case an HUF is a partner in the firm, the account shall not be opened.
5. In case of accounts of LLPs, account opening team shall check the Deed of the LLP and the list of partners of the LLP to ensure no HUF is a partner. In case an HUF is a partner in the LLP, the account shall not be opened. (Ref. MCA Circular dated 29.07.2013)

#### **General Guidelines to Relation Managers and persons involved in client acquisition and registration**

- Always check original documents before accepting the copies
- Obtain the latest photograph of account holder/ authorized person(s)
- Check for latest IT return of the client/ Net worth Certificate for ascertaining the financial status of the client to know the client suitability of the product being sold to the client
- Review the above details on-going basis to ensure that the transactions being conducted are consistent with our knowledge of customers, its business and risk profile, taking into account, where necessary, the customer's source of funds.

- If the Relationship Manager or such persons involved in client acquisition or client servicing, during his course of interactions with the client, becomes aware of any Income Tax cases or other prosecutions or regulatory actions against the client or any financial issues that the client has got into or if any of his large / substantial assets such as house, factory, office etc. are now subject matter of any dispute, then in such case the employee should make a fresh “Client Information Sheet” with updated facts and submit the same to KYC team. KYC team in turn will alert Compliance or Risk Management team Business Head, as deemed fit, for further action.
  - Scrutinize the forms submitted by the client thoroughly and cross-check the details with various documents obtained like source of income. If required, ask for any additional details like salary slips, etc. to satisfy yourself whenever there
  - Vanishing Companies available on [www.sebi.gov.in](http://www.sebi.gov.in) and RBI Defaulters is a doubt.
  - For scrutiny / background check of the clients, websites such as [www.watchoutinvestors.com](http://www.watchoutinvestors.com) should be referred. Also, Prosecution Database / List of Database available on [www.cibil.com](http://www.cibil.com) can be checked.
  - Keep watch on the welcome kits returned with reason - undelivered. Business Head should be alerted, client be contacted immediately on telephone and the trading, if suspected, should be suspended
- Employee of VSSL should not preferably sign as witness on the CRF
  - If Employee of VSSL Group introduces the client, exact relation of the client with such employee should be documented.
  - The RM / Dealer / BM should meet the client in person at least once before opening the account at the address given by the client. In the process he may reasonably verify the living standards, source of income, financial status, etc. of the client and ensure that the details mentioned in the CRF (Client Registration Form) matches with the actual status.
- If the client is a ‘walk-in client’, then the concerned branch official should make independent verification about the background, identity and financial worthiness of the client.
- All mandatory proofs of identity, address and financial status of the client must be collected as prescribed by the regulatory authorities, from time to time. The proofs so collected should be verified with the originals. If the prospective client is refusing to provide any information do not forward his/ her account opening form to HO.
- In Person verification should be done only by authorized employees or registered Authorized Persons /Sub broker for their client where ever applicable
- The Concerned regional head or branch head has to be completely satisfied about the background, genuineness and financial status of the client before recommending for opening the account. If required, the regional head or branch head may seek additional information/documents from the client.
- If the account is to be handled by a POA /authorized representative then find out what is the relationship between the client and the POA/authorized representative, establish the identity and background of the client and the POA/authorized representative.
- In case of a corporate account, the branch officials should ensure that the authorized person has got the required mandate by way of Board Resolution. Also, the identity and background of the authorized person has to be established by obtaining the additional documents if required

## **FOR ALL EXISTING CLIENTS**

On an on-going basis, the branches should ensure that the details given in the KYC, by the client, matches with the current details of the client. If required, we can seek additional documents/information from the client to verify the financial/general status of the client.

In cases where:

- There is any material negative change in the financial details of the client from what is given in the KYC.
- If the client is not contactable/traceable or contracts notes/ communications sent are received back undelivered.
- In case the client is prohibited by any regulatory authority.
- The client refuses to provide additional information/document asked for.
- There is a material change in the mandate holder profile/details
- Branches should immediately bring the same to the notice of the Business Head. The Business Head will, in turn, discuss the same with the Principal Officer to decide on the necessary course of action, including reporting to FIU, New Delhi.

## **Transactions monitoring and reporting suspicious transactions**

VSSL, on an ongoing basis, should monitor the transactions executed by the client which could be ultimately termed as suspicious FIU, India.

Monitoring of transactions:

- To identify the transactions which is in deviation with normal transactions or activities of the client?
- To pay attention to unusually large and complex transactions making no economic sense.
- To have internal thresholds for each class of accounts and pay special attention when it exceeds the limits
- The background, documents, records, memorandum & clarifications etc. sought for such transactions should be examined carefully and findings should be recorded.
- And such findings should be made available to auditors, SEBI, stock exchanges FIUIND & other relevant regulators during audit & inspection.
- These records should be preserved for 5 years from the date of transaction between client and intermediary.
- The record of transactions under section 12 PMLA should be preserved and Suspicious transaction in terms of section 12 reported to Director FIU-IND.STR should be reported to higher authorities within the Member
- The compliance officer shall randomly examine the selection of transactions and ascertain suspicious or not.

## **SUSPICIOUS TRANSACTIONS MONITORING AND REPORTING**

### **Circumstances of suspicion**

Suspicious Transactions are those which:

- gives rise to reasonable grounds of suspicious that it may involve proceeds of crime
- appears to be made in circumstances of unusual or unjustified complexity
- appears to have no economic rationale or bona-fide purpose

### **1 Factors giving rise to suspicion are:**

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

### **2 CRITERIA FOR ASCERTAINING SUSPICIOUS TRANSACTIONS**

- Surveillance / RMS Alerts based on the client's transactions on NSE/BSE/CDSL.
- Unusually large transactions like, clients having traded in scrip/shares of a company over a threshold quantity /value in a single day and volume in that scrip of that client is above a threshold percentage of the total volume in that scrip of the Exchange.
- Negotiated trades /matched trades.
- Client's Turnover not commensurate with financials
- Relation of the client with the company / directors / promoters.
- Clients making huge and regular losses and are still placing trades/orders and further identifying the transfers, above a threshold quantity, in an ISIN, in a single transaction or series of transactions threshold
- Sources of funds in such cases.
- Large volume in proprietary account of Sub Brokers/Affiliates
- Alerts generated by CDSL based on transactions in Depository Accounts Debit and Credit transactions due to off market or Inter- depository quantity/value, in an ISIN, in a single transaction or series of transactions executed during the fortnight.
  - Details of debit and credit transactions above a threshold quantity/value whichever is smaller , in an ISIN, which exceed a threshold multiplier
  - Details of Off Market transactions (within CDSL or Inter depository where there are more than a threshold number of transactions in an account, for the past fortnight
- Any debit transaction in a dormant account for exceeding a threshold quantity/value whichever is smaller, will be reported as an alert. An account having no 'Debit' Transaction' in the last 'n' months will be considered as Dormant' account for this purpose.



### **3 Reporting of Suspicious Transaction**

- All employees of VSSL shall monitor transactions on a continuous basis and shall report all Cash Transactions and / or Suspicious Transactions to the Principal Officer. It is likely that in some cases transactions are abandoned/aborted by Clients on being asked to give some details or to provide documents. It is clarified that employees should be vigilant and report all such attempted transactions to the MLRO or directly to the Principal Officer as a Suspicious Transaction, even if not completed by Clients, irrespective of the amount of the transaction.
- In any case, all employees are required to exercise diligence and proactively alert “Concerns” in compliance with the VSSL Group’s Whistleblower Policy and therefore, this policy be read and implemented in conjunction with the Whistleblower Policy, particularly Clause 37 of the Whistleblower Policy, without disregard to any other provisions thereof.
- Any suspicious transactions, identified by the MLRO or brought to the notice of the Principal Officer, will be analyzed by the MLRO for FIU reporting, accompanied by reassessment by Principal Officer, where required. If the Principal Officer decides that the transactions need to be reported to FIU he will report the transaction to FIU. If the Principal Officer decides not that the transactions is not suspicious enough to be reported to FIU, he will record the reasons for the same and document it.
- STR to be reported to FIU to their designated web site after registration in the requisite format within 7 days from the date of ascertainment of transactions as suspicious. The principal officer shall be responsible for timely submission of STR to FIU No nil report is necessary.
- No restrictions to put on the accounts reported under STR. No tipping off to the client are allowed. STR should be filed in utmost confidence.

In case of clients of high risk countries, FATF partially compliant or non-compliant such clients should be subject to enhanced scrutiny of transactions enhanced reporting mechanisms or systematic reporting of financial transactions.

- If any transaction has been reported, as suspicious, to FIU, the Principal Officer has to keep the same confidential. The transaction of the client will be executed, as usual, unless and until told specifically by the Principal Officer or Designated Director to discontinue dealing/close the account of such clients. No suspicion should be created in the client’s mind on the steps taken by VSSL. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended or other action taken.
- If there is a case of abrupt / unusual request for closure of accounts and / or refund of significant monies by clients, who have been determined to be suspicious or for whom STR has been filed, and such request has come to the notice of any employee, who is aware of the STR / suspicious nature of activities of the client, then employee must consult with the concerned MLRO and Principal Officer before fulfilling the request/taking any action. The MLRO and Principal Officer will consult the regulatory authorities in determining what action in such case.
- Trading exposure/turnover limits to be given to clients based on their margin available in the system.

It is also the duty of Risk Management to validate such exposures with the financial details provided by the client in KYC forms. If the trading activity of the client, which is not commensurate with the financial details declared by the client, it should be analyzed and referred to the MLRO with reasons of suspicion, who in turn shall analyze and refer the fit cases for filing of STR to Principal Officer. (can only be done offline after having a utility to capture financial details / net worth of the client).

In terms of the PMLA rules, brokers and authorized persons are required to do online report of information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit India (FIUIND) within 7 working days of establishment of suspicious at the level of principal officer. In view of the same, Branches/Departments/Sub brokers are requested to report the said transactions within 3 working days of establishment of suspicion to enable the Principal Officer to report the same to the Director, Financial Intelligence Unit India (FIU-IND) within the stipulated time.

## **7 Maintenance of Records**

- All records evidencing the identity of its clients and beneficial owners, all KYC related documents as well as all transaction related information, account files and business correspondence shall be maintained, in full, and preserved for a period of 5 (five) years after the business relationship of VSSL with the client has ended / terminated or the account has been closed, whichever is later.

The information that needs to be maintained is:

- Nature of transactions
- Amount of the transaction and the currency in which it was denominated
- Date on which the transaction was conducted
- Parties to the transaction
- Specific information that needs to be stored are:
  - all cash transactions of more than Rs.10.00 lakhs value or its equivalent in foreign currency
  - all series of cash transactions integrally connected to each other which might have been, individually, valued at less than Rs.10.00 lakhs but the aggregated of such transactions might be over Rs.10.00 lakhs
- All suspicious transactions whether or not made in cash.
- Deposits/withdrawals into or from any account, in any currency by way of third party cheques (or) pay orders
- (or) demand drafts (or) transfer from one account to another within VSSL (or) overseas receipts or payments

Records of information reported to the Director, Financial Intelligence Unit- India (FIU- IND): VSSL shall maintain and preserve the record of information related to transactions, whether attempted or executed, which are reported to the Director, FIU-IND, for a period of 5 (five) years from the date of the transactions between the client and VSSL or up to end of investigation / inquiry by FIU/ any statutory / government authority (in cases where such authority has intimated VSSL that such investigation is underway), whichever is later.

## **Audit trail**

To enable competent investigating authorities to trace through the audit trail, the following information for the accounts of customers shall be maintained.

- The beneficial owner of the account;
- The volume of the funds flowing through the account / and for the selected transactions: The origin of the funds
- The form in which the funds were offered or withdrawn, e.g. cheques, bank drafts / pay order etc.
- The identity of the person undertaking the transaction; The destination of the funds;
- The form of instruction and authority
- The identity of the official who made in person verification
- The identity of the official who verified copies documents obtained from client with originals

## **8 Employees Hiring /Training/Investor Education**

### **I . High Standard of hiring policies**

#### **Role of Human Resource Department:**

The Human Resource Department of VSSL has adequate screening procedure in place to ensure high standards in hiring new employees. It is ensured we are not hiring people who have a criminal or suspicious back ground or who does not have the requisite knowledge as to how the security market functions.

### **II. Training**

VSSL should conduct ongoing training programme to adequately train frontline staff, back office staff, compliance staff, RMS staff and staff dealing with new clients in AML & CFT procedures and to understand the rationale behind the directives, obligations and requirement of AML and being sensitive to risks of the system being used by unscrupulous elements.

The Principal Officer will arrange to conduct regular training to all the employees to ensure that the contents of the guidelines are understood develop awareness and vigilance to guard against money laundering and terrorist financing

### **III. Investor Education**

Branch Managers/RMS or any associate persons dealing with clients must educate and sensitize their clients regarding requirements of information and documents evidencing source of funds/income tax returns/bank records etc. for implementation of AML/CFT measures.

## **9 . Designated Officers Ensuring compliance of PMLA**

- i. Principal Officer-Act as central reference point for reporting Suspicious transactions to FIU after identifying and examining the potentially suspicious transactions
- ii. Designated Director-MD/Whole time Director duly authorized by Board should be appointed by intermediary to act as designated director for and on behalf of the intermediary before FIU.
- iii. The details of Principal Officer and Designated Director should be reported to FIU.

- iv. FIU-IND can levy penalty for noncompliance of AML/CFT against the Designated Director.

#### Assistance

Any assistance required in understanding this policy and in implementation of this Policy, please contact the Principal Officer on email ID [compliance@vselindia.com](mailto:compliance@vselindia.com)

### **10. List of Designated Individuals/Entities**

- a) 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 [http://www.un.org/sc/committees/1267/aq\\_sanctions\\_list.shtml](http://www.un.org/sc/committees/1267/aq_sanctions_list.shtml) (Al-Qaida Sanctions List) and <http://www.un.org/sc/committees/1988/list.shtml> (Taliban Sanctions List). Updated list should be obtained from the web-links from time to time and maintained on the records of VSSL. Also list should be updated based on circulars received from Exchanges, Depositories and SEBI from time to time.
- b) Pre-account opening check: Before opening any new account, it should be ensured by the Account Opening team that the name of the proposed client does not appear on any of these lists.
- c) VSSL shall, from time to time, scan the existing list of accounts to ensure that no account is held by any of the persons whose name appears in the any such sanctions lists
- d) In case of resemblance of any account-holder with any of the persons in the Sanctions List, the same shall be intimated to the Principal Officer (FIU) and Compliance Officer (for the exchanges). The Principal Officer shall, in turn, intimate the same to FIU along with filing of STR for all transactions in such account and the Compliance Officer (Exchanges / SEBI) shall intimate the same to SEBI and Stock Exchanges. Also details of such customer, along with 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 competent authority (at this time, it is to the Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and telephone on 011-23092736 and as may be modified from time to time). The particulars apart from being sent by post should necessarily be conveyed through e-mail at [jsis@nic.in](mailto:jsis@nic.in) or such other e-mail id as may be modified and intimated by regulatory authorities from time to time.
- e) VSSL shall send the particulars of the communication mentioned in (d) above to through post/fax and through e-mail ([sebi\\_uapa@sebi.gov.in](mailto:sebi_uapa@sebi.gov.in)) to the UAPA nodal officer of SEBI, Officer on Special Duty, Integrated Surveillance Department, Securities and Exchange Board of India as well as the UAPA nodal officer of the state/UT where the account is held. (List of UAPA nodal officers is available at [http://megpolice.gov.in/notification/list\\_Nodal-officer\\_UAPA.pdf](http://megpolice.gov.in/notification/list_Nodal-officer_UAPA.pdf) or such other website or we blink as may be updated from time to time)
- f) Risk rating of such account-holder should immediately be marked as 'High' and such accounts should be subject to increased surveillance / risk monitoring.

## **11. Freezing of funds, financial assets or economic resources or related services**

Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA), relating to the purpose of prevention of, and for coping with terrorist activities was brought into effect through UAPA Amendment Act, 2008. In this regard, the Central Government has issued an Order dated August 27, 2009 (Annexure 1) detailing the procedure for the implementation of Section 51A of the UAPA.6

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, the Government has modified the earlier order dated August 27, 2009 by the order dated March 14, 2019 (Annexure 2) for strict compliance.

## **12. Review**

This policy will be reviewed annually by the Principal Officer, Designated Director for FIU (PMLA) and Designated Directors for the Stock Exchange memberships. Views of concerned Business Heads and chief of Internal Audit, if any, may be taken into account where the management finds it necessary. Revised versions of the policy shall be reviewed, approved and adopted by the Board of Directors of VSSL

This PMLA Policy is prepared by Compliance Officer Mr/Mrs. \_\_\_\_\_, (Designation) and was reviewed by our Principal Officer and Designated Director.

This Policy was placed before the board in the Board of Directors meeting held on 13<sup>th</sup> December, 2019 at our Head office and was approved on 13<sup>th</sup> December, 2019