

# **POLICY FORMULATED UNDER AMLA**

Inclusive of

**(Client Identification Procedure and Program at various stages forming part of the PMLA)**

## **1. Introduction / Background**

**1.1** Money Laundering in plain words can be stated as engaging in financial transaction that involve money derived from criminal activity/unaccounted sources which is camouflaged for routing as legitimate money through law full channels to conceal the true origin of criminally derived proceeds.

**1.2** International initiatives taken to combat drug trafficking, combat of financing of terrorism (CFT) and other organized and serious crimes have concluded that financial institutions including securities market intermediaries must establish procedures of internal control aimed at preventing and impeding money laundering and terrorist financing.

## **2. Prevention of Money Laundering Act 2002**

**2.1** The Prevention of Money Laundering Act, 2002 (PMLA) has been brought into force with effect from 1<sup>st</sup> July 2005. Necessary Notifications /Rules under the said Act have been published in the Gazette of India on 1<sup>st</sup> July 2005 by the Department of Revenue, Ministry of Finance, and Government of India. Further, Prevention of Money-Laundering (Maintenance of Records) Rules, 2005 published vide Notification G.S.R. 444(E), dated 1<sup>st</sup> July 2005, published in Gazette of India, Extraordinary, Part 2, Section 3(1).

**2.2** Financial Action Task Force (FATF) on Anti Money Laundering Standard has made recommendations based on which the SEBI has issued the Guidelines on Anti Money Standard vide their Circular Ref. No. ISD/CIR/RR/AML/1/06 Dated January 18, 2006. Further vide circular No ISD/CIR/RR/AMC/2/06 dated 20<sup>th</sup> March 2006 it has issued the obligation of the intermediates registered under Sector 12 of SEBI Act 1992.

## **3. Financial Intelligence Unit (FIU)- INDIA**

**3.1** To receive, process, analyses and monitor the information relating to suspicious financial transactions a body Financial Intelligence Unit- INDIA (FIU- INDIA) has been set up.

**3.2** Intermediates are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit- INDIA (FIU- INDIA) on the following address:

Director, FIU-IND  
Financial Intelligence Unit - India,  
6<sup>th</sup> Floor, Hotel Samrat,  
Chankyapuri,  
New Delhi - 110021

## **4. Obligation to Establish Policies & Procedure.**

**4.1** As per SEBI guidelines all intermediaries have been advised to ensure that a proper policy frame work on anti-money laundering is put in place.

**4.2** In order to fulfill these requirements, there is a need for registered intermediaries to have a system in place for identifying, monitoring and reporting suspected money laundering or terrorist financing transactions to the law enforcement authorities.

**4.3** Senior Management of a registered intermediary should be fully committed to establishing appropriate policies and procedures for the prevention of money laundering and terrorist financing and ensuring their effectiveness and compliance with all relevant legal and regulatory requirements.

## **5. AMLA Policy of Vivek Financial Focus Ltd.**

**5.1** Accordingly, Vivek Financial Focus Ltd. has initiated measures, as an internal policy, to implement the Guidelines on Anti Money Laundering standards as notified by the SEBI.

## **6. Implementation of PMLA Policy**

**6.1** Mr. Arvind Jaswal, the Principal Officer under PMLA is responsible for compliance of the provision of the PMLA and AML Guidelines and will act as central the reference point in onward reporting of suspicious transaction and will play an active role in the identification and assessment of potentially suspicious transactions.

**6.2** Mr. Ashok Kakar is appointed as designated director for the company for the purpose of PMLA and shall be ensuring the compliance according to SEBI circular number CIR/MIRSD/1/2014 dated March 12, 2014

## **7. Anti Money Laundering Procedures**

**7.1** The main aspect of anti-money laundering procedure is the Client Due Diligence (CDD) procedure which comprises the following:

- a)** Obtaining sufficient information in order to identify person who is the actual beneficial owner of the securities or the person on whose behalf the securities are acquired or maintained. In the case of corporate clients, identity of the persons who are beneficial owners (as prescribed in the SEBI circular dated January 24, 2013) shall also be verified in addition to the other usual details/information.
- b)** Verifying the customer's identity through reliable independent source documents, data or information.
- c)** Performing regular scrutiny of the transaction and account to ensure that the operations are consistent with the client's background, financial position and risk profile.

**7.2** The Client Due Diligence procedure includes the following specific parameters:

- a) Policy for acceptance of clients.
- b) Client identification procedures.
- c) Identification and reporting of suspicious transactions.

## **8. Policy For Acceptance Of Clients**

**8.1** In person verification of each client is a must. If due to any reasons any client is unable to come to office, concerned official may visit the client residence/office to get the client registration form completed.

**8.2** All the requirements of KYC norms to be complied with viz. all the forms are to properly filled, photograph of the client is attached, and required supporting documents like PAN, Residential Proof, Bank Account, Depository Account, etc. are enclosed with KYC. All photocopies of documents submitted by client are to be checked with originals without any exception. Digital KYC may also be done for verification of the client by capturing live photo of the client and “officially valid document” or proof of possession of Aadhaar, where offline verification cannot be carried out. The “Officially Valid Document” means passport, driving license, proof of possession of Aadhaar Number, Voter’s Identity Card issued by Election Commission of India, job card issued by NREGA duly signed by the officer of the State Department, letter issued by National Population Register containing details like name, address or any other document as notified by the Central Government.

**8.3** The client also needs to be registered with ‘Central KYC Registry’.

**8.4** The documents to be received from the clients for account opening and verification may be collected in the form of as “equivalent e-documents”. It means an electronic document, issued by issuing authority of such document with its valid digital signature including documents issued to the digital locker account. [As per rule 9 of the Information Technology (Preservation and Retention of Information by Intermediaries Providing Digital Locker Facilities) Rules, 2016]

**8.5** As far as possible try to ensure that new account is introduced by an existing client. Introduction should be checked with the introducer.

**8.6** In case of walk in clients additional care should be exercised to ensure that no undesirable person becomes a client.

**8.7** All supporting documents as specified by the SEBI/Exchange are to be obtained and verified for all categories of clients.

**8.8** In case of any deficiency in the documents/information or any suspicion about the genuineness of the account, do not accept the client registration form and bring it to the notice of higher authorities.

**8.9** Be careful about the Clients of Special Category (CSC) as specified by the SEBI/Exchange or any authority under PMLA. The document/records pertaining to clients belonging to this

category should be minutely scrutinized and account to be identified accordingly. The following is the list of such clients:

- a. Non resident clients
- b. High net worth clients,
- c. Trust, Charities, NGOs and organizations receiving donations
- d. Companies having close family shareholdings or beneficial ownership
- e. Politically exposed persons (PEP) of foreign origin
- f. 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)
- g. Companies offering foreign exchange offerings
- h. Clients in high risk countries (where existence / effectiveness of money laundering controls is suspect, where there is unusual banking secrecy, Countries active in narcotics production, Countries where corruption (as per Transparency International Corruption Perception Index) is highly prevalent, Countries against which government sanctions are applied, Countries reputed to be any of the following – Havens / sponsors of international terrorism, offshore financial centres, tax havens, countries where fraud is highly prevalent.
- i. Non face to face clients
- j. Clients with dubious reputation as per public information available etc.

The above mentioned list is only illustrative and independent judgment should be exercised to ascertain whether new clients should be classified as CSC or not.

**8.10** Where the intimation about the account opening is received back undelivered the address should be re-verified and matter to be brought to the notice of higher authority.

## **9. Client Identification Procedure**

**9.1** Client Identification Procedure involves procedures at three different stages as under:

- a) While establishing the relationship with the client.
- b) While carrying out transaction for the client.
- c) Any doubt about veracity or the adequacy of previously obtained client identification data at a later stage.

## **10. Client Identification Procedure While Establishing Relationship With The Client**

**10.1** The identification of the client at the time of account opening is very important. As stated under the Policy for acceptance of client documents/information as prescribed by SEBI must be obtained and original of all documents submitted must be verified.

PAN has to be verified from Income Tax records independently. A list of documents required for each category of clients is stated in KYC. If any other information/document is deemed necessary the same can be requested from the client.

## **11. Client Identification Procedure During Operation**

**11.1** This involves maintaining continuous familiarity and follow up with the client account. This should be done keeping in view the information/document furnished by the client at the time of account opening to be able to detect any inconsistency with the information provided. The following are some steps in this direction.

- a) Order is placed by the client or his authorized/natural representative and in case of any doubt personal identification like date of birth, phone no. etc. is asked for.
- b) Orders of any unusual nature to be brought to the notice of higher authorities before execution.
- c) While confirming the trade after execution the identity of the client is to be ensured and checked.
- d) Contract note should be dispatched at the address provided or handed over to the client or his authorized/natural representative only.
- e) Pay-In and Pay-Out should be in the respective client accounts only and in no case payments/securities are to be received or delivered otherwise
- f) No cash payments to the clients are allowed. Cash receipts are also to be avoided. However in case of minor amounts towards cost of documents, depository charges and in exceptional cases of sticky/overdue accounts cash may be received at head office only with the approval of higher authorities.

## **12. Subsequent Verification**

**12.1** In case of any doubt about the veracity or the adequacy of previously obtained information about any client efforts should be made to call for additional information/documents to check the veracity of information/documents earlier provided. Failure of the client to provide such additional information/documents or if the new information/document is found to be contrary to the earlier ones the same should be noted and immediately brought to the notice of higher authority.

**12.2** In case of any request from the client for change in the existing particulars written request along with necessary supporting documents is required.

## **13. Risk Based Approach**

**13.1** As each client poses different risk we need to identify clients who pose higher risk than the others in term of monitoring suspicious transactions under the money laundering or terrorist activities. Suspicious transaction means a transaction referred to including an attempted transaction, whether or not made in cash, which to a person including in good faith:

- gives rise to reasonable grounds of suspicion that it may involve proceeds of an offence
- appears to be made in circumstances of unusual or unjustified complexity
- appears to have no economic rationale

- gives rise to reasonable grounds of suspicion that it may involve financing of activities relating to terrorism

**13.2** The clients can be classified into three categories.

- a) Low Risk
- b) Medium Risk
- c) High Risk

**13.3** The classification can be done on the basis of location of the client, nature of business, trading turnover, nature of transaction and manner of making payments.

**13.4** Our client's due diligence should take into account the risk profile at every stage of operation.

**13.5 Category A:** Clients may be classified as having nil or very little risk. These can be identified as corporate, individuals, HNI who have respectable official/social/financial standings, who are regular in payments and operate within defined parameters.

**Category B:** Clients are those clients who take more exposure than their capacity and are very aggressive traders.

**Category C:** Clients who have low financial standing with very aggressive trading.

## **14. Maintenance of Records of Transactions (nature and value)**

**14.1** The company shall maintain records of all transactions including record of:

- a) All cash transactions of value of more than Rs. 10 lakh or its equivalent foreign currency
- b) All series of cash transactions integrally connected to each other which have been individually valued below Rs. 10 lakhs or its equivalent foreign currency where such series of transactions have taken place within a month and the monthly aggregate exceeds an aggregate amount of Rs. 10 lakhs or its equivalent foreign currency.
- c) All transactions involving receipts by non profit organisations of value more than Rs. 10 lakhs or its equivalent foreign currency.
- d) 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 transaction
- e) All cross border wire transfers of the value of more than Rs. 5 lakhs

**15.** It is important to realize that the underlying principle of total regulatory requirement is that the company is fully aware of the client on whose behalf the company is dealing.

**16.** Vivek Financial has adopted an ongoing employee training program so that the members of the staff are adequately trained in AML and CFT procedures. Training requirements have specific focuses for front line staff, back office staff, compliance staff, risk management staff and staff dealing with new customers. It is crucial that all those concerned fully understand the rationale behind these guidelines, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements. Implementation of such measures requires the staff to demand certain information from investors which may be

of personal nature or which have hitherto never been called for. Such information can include documents evidencing source of funds/income tax returns bank records etc. this can sometimes lead to raising of questions by the customer with regard to the motive and purpose of collecting such information.

## **17. Record Keeping**

**17.1** It is important to maintain records in a manner that the desired information is retrievable on a timely basis. It is therefore necessary to keep proper records of all documents relating to client registration, other correspondence with the clients, account files or other records as required under the SEBI Act, Rules & Regulations framed there under, PMLA 2002, other relevant legislation, Rules and Regulation of the Exchange or circulars etc.

**17.2** In case of any suspected drug related or other laundered money or terrorist property, the following information has to be maintained:

- i. Beneficial owner of the account
- ii volume of funds flowing through the account
- iii origin of funds
- iv mode of transaction i.e. cheque or demand draft
- v Form of instruction and authority

**17.3** Proper records of transactions under Rule 3 of PML Rules that covers the following:

- i. All cash transactions of the value of more than ten lakh rupees or its equivalent in foreign currency
- ii. Preservation and maintenance of records of identities, beneficial owner details for a period of 5 years after the business relationship between a client and intermediary has ended or the account has been closed, whichever is later.

**17.4** Under the PMLA the minimum prescribed period is 5 years. In case, where the record relates to an ongoing investigation or have been the subject of suspicious transaction reporting, the same should be retained until it is confirmed that the case has been closed.

## **18. Suspicious Transactions Monitoring & Reporting**

**18.1** It is the duty of all to be vigilant to identify, analyse and report any suspicious transaction. Some of the reasons which can raise suspicion are as under:

- a) Identity of the client becomes suspicious due to any reason.
- b) Background of the client is found to be suspicious or criminal.
- c) Operation of multiple accounts with no apparent reasons.
- d) Unusual activity in the account like substantial increase in business without apparent cause.
- e) Insistence of cash transaction by the clients.
- f) Efforts to transfer money to or from apparently third party accounts with no linkage.
- g) Any unusual transaction in the accounts of CSC.

This list is illustrative and there can be many other reasons which may cause suspicious and therefore there is necessity of continuous vigilance.

**18.2** Any suspicious transaction should be immediately noted and brought to the notice of the higher authority giving detail of client, transaction, nature/reason of suspicion. It is to be ensured that this action is kept secret from client and activity with the concerned client should be kept normal unless and until instructed otherwise.

**18.3** The following details are to be maintained for such transactions:

- a) Nature of transactions.
- b) Amount of the transaction.
- c) Date of transaction.
- d) The parties to the transaction.

**18.4** The report to the FIU-India should be submitted within the stipulated time frame which is 15<sup>th</sup> of succeeding month in case of cash transaction and within 7 days of arriving at a conclusion that any transaction whether cash or non-cash is suspicious.

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

19.1 Section 51A of the Unlawful Activities (Prevention) Act, 1967 (UAPA) brought into effect through UAPA Amendment Act, 2008, relating to purpose of prevention of coping with terrorist activities empowers the government to freeze, seize or attach funds and other financial assets or economic resources held by, on behalf of, or at the direction of the individuals or entities listed.

19.2 As per the UAPA Order dated August 27, 2009, the following needs to be expedited:

19.2.1 The updated list shall be maintained and shall check if any of such accounts are opened with the company. If yes, whether such accounts are holding any funds, financial assets or economic resources in the form of securities.

19.2.2 In case of any such account holder holding any of securities, the same needs to be updated to the following within 24 hours to the Joint Secretary (ISI), Ministry of Home Affairs telephonically at 011-23092736 and through email at [jsis@nic.in](mailto:jsis@nic.in).

19.2.3 The same information has to be updated to SEBI through email at [sebi\\_uapa@sebi.gov.in](mailto:sebi_uapa@sebi.gov.in)

19.2.4 It shall also be filed as Suspicious Transaction Report (STR)

**20.** Mr. Arvind Jaswal is designated principal officer and can be contacted for any information/classification in the regard.