AML and KYC Policy

1. INTRODUCTION

This Policy has been framed by Alphaware Advisory Services Private Limited (“the Company”) in order to comply with the applicable Anti Money Laundering Standards and to take measures to prevent the Company from being used as a vehicle for Money Laundering and Terrorist Financing.

Money Laundering and Terrorist Financing

Money Laundering may be defined as cleansing of dirty money obtained from legitimate or illegitimate activities with the objective of hiding its source and rendering it in legally usable form. The process of money laundering involves creating a web of financial transactions so as to hide the origin of and true nature of these funds. The process of money laundering is also an illegal activity involving financial jugglery. In fact, the activity of money laundering is an activity separate from the activity from which the money sought to be laundered is obtained.

Although the process of money laundering has only come to the attention of the international community in recent years, the practice has long ago been present, dating back to the time of the pirates in European seas. But it was only in the 1920s that the term money laundering was used to refer to these kinds of activities.

According to historians, the term was first coined in the United States, referring to criminal gangs who used business establishments such as car washes and laundry shops to mask their illegal activities. Payments in laundry shops as well as vending machines in general are coins. The coins put into the machines are the only proof of how the business is going. Seeing that there will be no paper trail to point out the “additional” earnings that came from their illegal activities, crime groups intentionally add coins to the daily business income, making it appear that the coins were put there by paying customers. Some however, place the origin of the term money laundering to mean “the act of washing clean dirty money.”

But the true hazards of money laundering came into light when the world was shocked when United States of America was hit by terror on September 11, 2001 which brought down the twin towers of WTC in New York. It was then when the world started taking notice of the terrorist financing activities and the hazards of money laundering. Soon after the 9/11 attacks, the Government of United States enacted the USA Patriot Act on October 26, 2001 and the Government of United Kingdom adopted the FSA (Financial Services Authority) Regulations for adoption of stringent policies for combating the menace of money laundering.

Several other countries have already enacted legislations to detect and curb money laundering activities. Finally, the Government of India succeeded in enacting such legislation after four years of presenting the Anti-Money Laundering Bill in 1998, which later got enacted as the Prevention of Money Laundering Act in 2002, with the objective of preventing or controlling the basic crimes related to Indian Penal Code, narcotics, corruption, tax-evasion, etc.

Need for this Policy

In India, the Reserve Bank of India (“RBI”) issued the Know Your Customer (KYC) Guidelines — Anti Money Laundering Standards on November 29, 2004 keeping in mind the requirements of PML Act, 2002, which all the banks in India had to adopt by December 31, 2005 (compliance to AML standards). The Government has also setup a Financial Intelligence Unit-India (FIU-IND), in line with Financial Action Task Force (FATF) recommendations. FATF is an inter-governmental body whose purpose is the development and promotion of national and international policies to combat money laundering and terrorist financing. The FIU would receive the Suspicious Activity Reports from all Financial Institutions and would analyze them before passing them to the Enforcement Directorate for investigation and prosecution.

Securities and Exchange Board of India (SEBI) has issued guidelines on Know Your Customer (KYC) standards and AML (Anti-Money Laundering) Measures vide circulars dated January 18, 2006 and March 20, 2006. The circulars require all registered intermediaries, which are covered under Section 12 of SEBI Act, 1992 to prepare and put in place proper policy framework as per the guidelines on anti-money laundering measures. The guidelines issued with the circular are in the context of the recommendations made by the FATF on anti-money laundering standards. The policy framework incorporates salient aspects of the measures and obligations of registered intermediaries under the Prevention of Money Laundering Act, 2002 (PMLA) and Rules to Prevention of Money Laundering (Amendment) Act, 2005 (PMLA Rules) that have come into force on July 1, 2005.

The guideline provides a general background on the subjects of money laundering and terrorist financing and provides guidance on the practical implications of the Act. The Guidelines also sets out the steps that a registered intermediary and any of its representatives, should implement to discourage and identify any money laundering or terrorist financing activities.

The term “CATCH” is a shorthand way of helping you to remember the five main elements of the implementation of these rules, regulations and guidelines.

1. **C**ontrol your business by having anti money laundering systems in place
2. **A**ppoint Principal Officer
3. **T**rain your staff
4. **C**onfirm the identity of your customers
5. **H**old all records for at least 8 years

2. POLICY OBJECTIVES

- To prevent criminal elements from using our business for money laundering or terrorist financing activities
- To understand the investor/client and their financial dealings better, which in turn would help us to manage the risk prudently
- To put in place a robust customer onboarding process, which minimizes the risk of getting those customers on board that pose a risk from a compliance, money laundering or terrorist financing perspective
- To put in place appropriate controls for detection and reporting suspicious transactions in accordance with applicable laws/laid down procedures
- To comply with applicable laws and regulatory guidelines.

3. KEY ELEMENTS OF THE POLICY

- No cash transaction: The company will not enter into any cash transactions with clients for any reason whatsoever. All monetary exchange with clients will take place electronically, using methods including but not exclusive to net banking, UPI and payment gateways.
- Client Due Diligence Process:
    - **Principles to be followed:**

        - Verify the identity of clients using reliable, independent source documents, data or information.
        - Verify other information that the user provides, that is critical for making transactions, or that is information that can be used to double-check identity.
        - Forge partnerships with multiple credible agencies for the purpose of verification to avoid loopholes in the system.
        - Conduct ongoing due diligence and scrutiny to ensure that the transactions being conducted are consistent with our knowledge of the client, his risk profile, taking into account where necessary, the client's source of funds.
    - **Client acceptance policy:**
        - All employees have to ensure that the guidelines issued from time to time regarding Client Acceptance are strictly followed. Existing/past relationships with the client should be verified regularly to check for continued authenticity.
        - Clients are to be classified into different categories of risk (low, medium and high) depending on the volume of transactions, trading turnover, manner of payment, etc.
        - **Risk assessment of clients:** Clients are classified into three types.
            - The below mentioned list should be considered as **High-Risk Clients**
                - Non-resident clients
                - High net worth individuals (individuals with a disclosed net worth of greater than Rs. 10 crore
                - Trust, charities, NGOs and organizations receiving donations
                - Politically exposed persons of foreign origin
                - Clients with dubious reputation as per public information available
                - Clients with mismatches in verification data across different checks

In case of High-Risk category, due care and caution should be exercised at the acceptance stage itself. The profile of such clients, particularly their contact details and financial status has to be monitored and updated regularly.

- **Medium-Risk Clients:** Such clients are those who invest more than Rs. 1 crore up to Rs. 10 crore.
- **Low-Risk Clients:** Such clients are those who invest up to Rs. 1 crore.

- An assessment should be made of the financial worthiness of the client by obtaining appropriate declarations at the KYC stage. The information should be subsequently used for monitoring whether transactions of the clients are within the declared means and if the value of the transactions is increasing disproportionately when compared to the stated income, the client should be asked to disclose the sources of the increase in income.
- No account should be opened in a fictitious name / benami name or on an anonymous basis.
- No transactions should be allowed without the bank account of the client being verified in terms of their name and the account's status of functionality.
- A thorough assessment should be carried out to ascertain whether the investor/ client is dealing with us on his own behalf or someone else is the beneficial owner; for example while Mr. A may be our investor/client as per the documents, Mr. B may be giving instructions all the time. If there are doubts, before acceptance of the investors/clients, thorough due diligence should be carried out to establish the genuineness of the claims of the investors/clients. Secrecy laws shall not be allowed as a reason not to disclose true identity of the beneficiary/transacting party.
- No Investor/Client should be accepted where it is not possible to ascertain the identity of the investor/client, or the information provided is suspected to be non- genuine, or if there is perceived non-cooperation of the investor/client in providing full and complete information.

- **Client identification policy:**
  - Before opening the accounts, all checks including but not exclusive to identity verification, photo verification, bank account verification and

video verification should be in place; if the KYC records aren't available with a KRA.

- In case of individuals, proof of identify (as prescribed by SEBI) should be produced by way of any of the following documents (un-expired original document shall be verified):
- PAN Card
- Proof of address: Aadhar card has to be obtained (un-expired, original should be verified)
- For bank account verification, pennydropping services should be used to electronically deposit Re 1/- into the account of the user, and to consequently validate authenticity and validity of the account.

4. MONITORING OF TRANSACTIONS

- All the high-risk investor/client accounts should be monitored at least once in a calendar quarter and any exceptions need to be reported to the management and to the Principal Officer.
- If any transaction appears to be suspicious it is to be reported to the Principal Officer immediately.
- For identifying the suspicious transactions, the following illustrative questions may be considered:
  - Is the investor/client willing to accept economic terms without apparent reason?
  - ls the transaction inconsistent with legitimate business activity?
  - Is the transaction inconsistent with the normal pattern of the investor/client's investment activity?
  - Is the transaction inconsistent with the investor/client's account-opening documents?
  - ls the investor/client financially capable of the transactions lie has asked for?
  - Sudden activity in dormant accounts;
  - Multiple transactions of value just below the threshold limit specified in PMLA so as to avoid possible reporting;

    - Investors/Clients in high-risk jurisdictions or investors/clients introduced by banks or affiliates or other investors/clients based in high risk jurisdictions.
- The Principal Officer shall undertake random checks as to the nature of the transactions and if they are suspicious transactions.

5. MAINTENANCE OF RECORDS

- All records including client identification, account files and business correspondence shall be maintained in hard and soft form for a period of eight years.
- In the case of transactions where any investigations by any authority has been commenced and in the case of transactions which have been the subject of suspicious transactions reporting all the records shall be maintained till the authority informs of closure of the case.

6. PRINCIPAL OFFICER

- The Company has designated the Chief Executive Officer as the Principal Officer who shall be responsible for implementation and compliance of this policy. The duties of the Principal Officer shall include the following:
    - Monitoring the implementation of Anti Money Laundering (AML) and Combating Financing of Terrorism (CFT) Policy including customer due diligence.
    - Reporting of transactions and sharing of information as required by the law
    - Liasoning with law enforcement agencies
    - Ensuring submission of periodical reports to Board of Directors. The report shall mention of any suspicious transactions are being looked into by the respective business groups and if any reporting is to be made to the authorities.
    - Providing clarifications to staff members on the provisions of the act, rules, guidelines and the policy of the company.

7. STAFF AWARENESS AND TRAINING

The staff who deal directly with the public are the first point of contact with potential money launderers. Their efforts are therefore vital to the reporting system for such transactions. Staff should keep abreast of the practices to identify suspicious

transactions and on the procedure to be adopted when a transaction is deemed to be suspicious. In short, employees must familiarize themselves with their clients' normal trading activities and usual market practices in order to recognize anomalous behaviour. Suspicions concerning the source of assets or the nature of transactions should not be ignored. It is the active responsibility of every person in the company to seek to ensure that the company's facility is not being misused.

Staff should not disclose to the client concerned nor to other third persons that their transactions are deemed suspicious or if any information may be transmitted to the authorities.

Principal Officer provides AML training to all employees on at least an annual basis.

8. INVESTOR EDUCATION

Implementation of the measures outlined herein may require us to demand certain information from clients which may be of personal nature or his 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 client with regard to the motive and purpose of collecting such information. Staff/authorized persons must, therefore, sensitize clients about these requirements as the ones emanating from Anti Money Laundering (AML) and Combating Financing of Terrorism (CFT) framework. Specific literature/pamphlets etc may also be prepared so as to educate the client of the objectives of the AML/CFT program.

9. Reporting to FIU

The Company will submit Suspicious Transaction Report (STR) to the FIU in the prescribed format within the prescribed time. STR would be submitted within 7 days of arriving at a conclusion that any transaction, whether cash or non-cash, or a series of transactions integrally connected are of suspicious nature. The Principal Officer would record his / her reasons for treating any transaction or a series of transactions as suspicious. It should be ensured that there is no undue delay in arriving at such a conclusion.