



Policies and Procedures to Combat Money Laundering and Terrorist Financing

Principal Officer

The company has designated Shri Himesh Lakhani as the Principal Officer and Ms. Shilpa Hirani as the Designated Director with full responsibility for the company's AML program.

1 Obligation to establish policies and procedures

- 1.1 As per Prevention of Money Laundering Act, 2002 all Intermediaries are obliged to establish procedures of Internal Control aimed at preventing and impeding money laundering & terrorist financing.
- 1.2 In order to fulfill these requirements, there is a need for the Company to have a system in place for identifying, monitoring and reporting suspected money laundering or terrorist financing transactions to the law enforcement authorities.

2 Anti Money Laundering Procedures

Procedures have been developed for the overall 'Client Due Diligence Process' focusing on 3 specific areas:

- 2.1 Policy for acceptance of clients
- 2.2 Procedure for identifying the clients
- 2.3 Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR)

3 Customer Due Diligence

- 3.1 The customer due diligence ("CDD") measures comprise the following:
- 3.2 Obtaining sufficient information in order to identify persons who are the beneficial owner of the securities account. Whenever it is apparent that accounts are operated through beneficial owner who is different person than the client, client identification and verification procedures should be used to identify that person.
- 3.3 Verify the customer's identity using reliable, independent source documents, data or information;



***Rosy Blue Securities
Private Limited***

154 / C, Mittal Court,
Nariman Point,
Mumbai - 400 021.
Tel : 67681111 Fax: 67681199
CIN : U65990MH1994PTC080450
Email : admin@rosyblue.co.in

- 3.4 Identify beneficial ownership and control, i.e. determine which individual(s) ultimately own(s) or control(s) the customer and/or the person on whose behalf a transaction is being conducted;
 - 3.5 Verify the identity of the beneficial owner of the customer and/or the person on whose behalf a transaction is being conducted, corroborating the information provided in relation to (c); and
 - 3.6 Conduct ongoing due diligence and scrutiny, i.e. perform ongoing scrutiny of the transactions and account throughout the course of the business relationship to ensure that the transactions being conducted are consistent with the company's knowledge of the customer, its business and risk profile, taking into account, where necessary, the customer's source of funds.
 - 3.7 We shall periodically update all documents, data or information of all clients and beneficial owners collected under the CDD process.
 - 3.8 The SEBI KRA/ CKYC process shall followed at all times as applicable
- 4 Policy for acceptance of clients:
- 4.1 Through Customer Acceptance Policy identify the types of customers that are likely to pose a higher than the average risk of money laundering or terrorist financing.
 - 4.2 No account is opened in a fictitious / benami name or on an anonymous basis.
 - 4.3 Factors of risk perception (in terms of monitoring suspicious transactions) of the client are clearly defined having regard to clients' location (registered office address, correspondence addresses and other addresses if applicable), nature of business activity, trading turnover etc. and manner of making payment for transactions undertaken.
 - 4.4 Documentation requirement and other information to be collected in respect of different classes of clients depending on perceived risk and having regard to the requirement to the Prevention of Money Laundering Act 2002, guidelines issued by RBI and SEBI from time to time.
 - 4.5 An account is not opened where the Company is unable to apply appropriate clients due diligence measures / KYC policies. The company shall not continue to do business with such a person and file a suspicious activity report.
 - 4.6 The circumstances under which the client is permitted to act on behalf of another person / entity should be clearly laid down. Specification shall be made for the manner in which the account should be operated, transaction limits for the operation, additional authority required for transactions exceeding a specified quantity / value and other appropriate details. Further the rights and responsibilities of both the persons (i.e. the agent- client



registered with the company, as well as the person on whose behalf the agent is acting should be clearly laid down). Adequate verification of a person's authority to act on behalf the customer should also be carried out.

- 4.7 No account shall be open where the identity of the client does match with any person having known criminal background or is banned in any other manner, whether in terms of criminal or civil proceedings by any enforcement agency worldwide.
- 4.8 The CDD process shall necessarily be revisited when there are suspicions of money laundering or financing of terrorism (ML/FT).

5 Risk-based Approach

The customer due diligence measures shall be applied on a risk sensitive basis. An enhanced customer due diligence process for higher risk categories of customers and simplified customer due diligence process may be adopted for lower risk categories of customers. It is generally recognized that certain clients may be of a higher or lower risk category depending on the circumstances such as the client's background, type of business relationship or transaction etc. As such, we shall apply each of the client due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is that we shall adopt an enhanced client due diligence process for higher risk categories of clients. Conversely, a simplified client due diligence process may be adopted for lower risk categories of clients. In line with the risk-based approach, the type and amount of identification information and documents that we shall obtain necessarily depend on the risk category of a particular client. Further, low risk provisions shall not apply when there are suspicions of ML/FT or when other factors give rise to a belief that the customer does not in fact pose a low risk.

6 Clients of special category (CSC)

Such clients include the following.

- i. Non resident clients
- ii. High net-worth clients
- iii. Trust, Charities, Non-Governmental Organizations (NGOs) and organizations receiving donations
- iv. Companies having close family shareholdings or beneficial ownership
- v. 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. The



additional norms applicable to PEP as contained in the subsequent para of this policy shall also be applied to the accounts of the family members or close relatives of PEPs.

vi. Companies offering foreign exchange offerings

vii. 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 centers, tax havens, countries where fraud is highly prevalent. While dealing with clients in high risk countries where the existence/effectiveness of money laundering control is suspect, we, apart from being guided by the Financial Action Task Force (FATF) statements that identify countries that do not or insufficiently apply the FATF Recommendations, published by the FATF on its website (www.fatf-gafi.org), shall also independently access and consider other publicly available information.

viii. Non face to face clients

ix. Clients with dubious reputation as per public information available etc.

The above mentioned list is only illustrative and we shall exercise independent judgment to ascertain whether any other set of clients shall be classified as CSC or not.

7 Client identification procedure:

We shall be in compliance with the following requirements while putting in place a Client Identification Procedure

- 7.1 We shall proactively put in place appropriate risk management systems to determine whether their client or potential client or the beneficial owner of such client is a politically exposed person. Such procedures shall include seeking relevant information from the client, referring to publicly available information or accessing the commercial electronic databases of PEPs. Further, the enhanced CDD measures as outlined above shall also be applicable where the beneficial owner of a client is a PEP.
- 7.2 We will obtain senior management approval for establishing business relationships with PEPs. Where a client has been accepted and the client or beneficial owner is subsequently found to be, or subsequently becomes a PEP,



***Rosy Blue Securities
Private Limited***

154 / C, Mittal Court,
Nariman Point,
Mumbai - 400 021.
Tel : 67681111 Fax: 67681199
CIN : U65990MH1994PTC080450
Email : admin@rosyblue.co.in

we shall obtain senior management approval to continue the business relationship.

- 7.3 We shall also take reasonable measures to verify the sources of funds as well as the wealth of clients and beneficial owners identified as PEP.
- 7.4 The client shall be identified by us by using reliable sources including documents / information. We shall obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.
- 7.5 The information must be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by us in compliance with the directives. Each original document shall be seen prior to acceptance of a copy.
- 7.6 Failure by prospective client to provide satisfactory evidence of identity shall be noted and reported to the higher authority
- 7.7 Taking into account the basic principles enshrined in the KYC norms which have already been prescribed or which may be prescribed by SEBI from time to time, we shall frame our own internal directives based on our experience in dealing with their clients and legal requirements as per the established practices. Further, we shall conduct ongoing due diligence where it notices inconsistencies in the information provided. The underlying objective shall be to follow the requirements enshrined in the PMLA, SEBI Act and Regulations, directives and circulars issued thereunder so that we are aware of the clients on whose behalf we are dealing.
- 7.8 The client should be identified by the company by using reliable sources including documents / information.
- 7.9 Each original documents should be seen prior to acceptance of a copy.
- 7.10 Failure by prospective client to provide satisfactory evidence of identity should be noted and reported to the higher authority within the company.
- 7.11 The company should maintain continuous familiarity and follow-up where it notices inconsistencies in the information provided.



- 8 Procedure for freezing of funds, financial assets or economic resources or related services
- 8.1 We are aware that under section 51A of Unlawful Activities (Prevention) Act, 1967, the Central Government is empowered 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 in the Schedule to the Order, or any other person engaged in or suspected to be engaged in terrorism. The Government is also further empowered to prohibit any individual or entity from making any funds, financial assets or economic resources or related services available for the benefit of the individuals or entities listed in the Schedule to the Order or any other person engaged in or suspected to be engaged in terrorism.
- 8.2 In case if any client is found to be guilty under the PMLA provisions then the following procedure will be followed by the Company:
- 8.2.1 If the particulars of any of customer/s match the particulars of designated individuals/entities, the Company shall immediately, not later than 24 hours from the time of finding out such customer, inform 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 Joint Secretary (IS.I), Ministry of Home Affairs, at Fax No.011-23092569 and also convey over telephone on 011-23092736. The Company would also convey the information through e-mail at jsis@nic.in.
- 8.2.2 The Company would inform the IS-I Division of MHA so that they may take effective action like informing the State Police and /or the Central Agencies for conducting the verification of the individuals/ entities identified by the registered intermediaries.
- 8.2.3 The Company to provide full support to the appointed agency for conducting of the verification so that the verification gets completed within a period of 5 working days
- 8.2.4 The Company would not provide any prior notice to the designated individuals/entities.



9 Record Keeping

- 9.1 Sufficient records shall be maintained to permit reconstruction of individual transactions (including the amounts and types of currencies involved, if any) so as to provide, if necessary, evidence for prosecution of criminal behavior.
- 9.2 Company shall also retain the following information for the accounts of their customers in order to maintain a satisfactory audit trail:
 - 9.2.1 the beneficial owner of the account;
 - 9.2.2 the volume of the funds flowing through the account; and
 - 9.2.3 for selected transactions:
 - 9.2.3.1 the origin of the funds;
 - 9.2.3.2 the form in which the funds were offered or withdrawn, e.g. cash, cheques, etc.;
 - 9.2.3.3 the identity of the person undertaking the transaction;
 - 9.2.3.4 the destination of the funds;
 - 9.2.3.5 the form of instruction and authority.
- 9.3 Company ensures that all customer and transaction records and information are available on a timely basis to the competent investigating authorities.

10 Retention of Records

- 10.1 The following document retention terms should be observed:
 - 10.1.1 All necessary records on transactions, both domestic and international, shall be maintained at least for the minimum period prescribed under the relevant Act (PMLA, 2002 as well SEBI Act, 1992) and other legislations, Regulations or exchange bye-laws or circulars.
 - 10.1.2 Records on customer identification (e.g. copies or records of official identification documents like passports, identity cards, driving licenses or similar documents), account files and business correspondence shall also be kept for the same period.
- 10.2 In situations where the records relate to on-going investigations or transactions which have been the subject of a suspicious transaction reporting, they shall be retained until it is confirmed that the case has been closed.

11 Monitoring of transactions

- 11.1 Company shall pay attention to all complex, unusually large transactions / patterns which appear to have no economic purpose. The company may specify internal threshold limits for each class of client accounts and pay special attention to the transaction which exceeds these limits.



***Rosy Blue Securities
Private Limited***

154 / C, Mittal Court,
Nariman Point,
Mumbai - 400 021.
Tel : 67681111 Fax: 67681199
CIN : U65990MH1994PTC080450
Email : admin@rosyblue.co.in

- 11.2 Transaction of suspicious nature or any other transaction notified under section 12 of the act is reported to the appropriate law authority. Suspicious transactions should be regularly reported to the higher authorities / head of the department.
 - 11.3 Further the compliance cell of the company shall randomly examine a selection of transaction undertaken by clients to comment on their nature i.e. whether they are in the suspicious transactions or not.
- 12 Suspicious Transaction Monitoring & Reporting
- 12.1 Company should ensure to take appropriate steps to enable suspicious transactions to be recognised and have appropriate procedures for reporting suspicious transactions. A list of circumstances which may be in the nature of suspicious transactions is given below. This list is only illustrative and whether a particular transaction is suspicious or not will depend upon the background, details of the transactions and other facts and circumstances:
 - 12.1.1 Clients whose identity verification seems difficult or clients appears not to cooperate
 - 12.1.2 Asset management services for clients where the source of the funds is not clear or not in keeping with clients apparent standing /business activity;
 - 12.1.3 Clients in high-risk jurisdictions or clients introduced by banks or affiliates or other clients based in high risk jurisdictions;
 - 12.1.4 Substantial increases in business without apparent cause;
 - 12.1.5 Unusually large cash deposits made by an individual or business;
 - 12.1.6 Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;
 - 12.1.7 Transfer of investment proceeds to apparently unrelated third parties;
 - 12.1.8 Unusual transactions by CSCs and businesses undertaken by shell corporations, offshore banks /financial services, businesses reported to be in the nature of export-import of small items.
 - 12.2 Any suspicion transaction should be immediately notified to the Money Laundering Control Officer or any other designated officer within the company. The notification may be done in the form of a detailed report with specific reference to the clients, transactions and the nature /reason of suspicion.
- 13 Designation of an officer for reporting of suspicious transactions
- 13.1 To ensure that company properly discharge it's legal obligations to report suspicious transactions to the authorities, the Principal Officer would act as a central reference point in facilitating onward reporting of suspicious



transactions and for playing an active role in the identification and assessment of potentially suspicious transactions.

14 Employees' Hiring/Employee's Training/ Investor Education

14.1 Hiring of Employees

We shall have adequate screening procedures in place to ensure high standards when hiring employees. They shall identify the key positions within their own organization structures having regard to the risk of money laundering and terrorist financing and the size of their business and ensure the employees taking up such key positions are suitable and competent to perform their duties.

14.2 Employees' Training

We shall have an ongoing employee training programme so that the members of the staff are adequately trained in AML and CFT procedures. Training requirements shall have specific focuses for frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new clients. It is crucial that all those concerned fully understand the rationale behind these directives, obligations and requirements, implement them consistently and are sensitive to the risks of their systems being misused by unscrupulous elements.

14.3 Investors Education

Implementation of AML/CFT measures requires us to demand certain information from investors which may be of personal nature or has 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. There is, therefore, a need for us to sensitize their clients about these requirements as the ones emanating from AML and CFT framework.

For Rosy Blue Securities Pvt. Ltd.

SD/-

Shilpa Hirani

Director