# Capital Wizard Stock Broking Pvt. Ltd

## 1. Introduction

1.1 The Guidelines as outlined below provide general procedures to be followed to ensure the compliance of the guidelines prescribed under the Prevention of Anti Money Laundering Act 2002.

1.2 These procedures have been designed considering the specific nature of our business, organizational structure, type of customers and transactions, etc.. We all must ensure that the suggested measures and procedures are effectively applied and implemented. The overriding principle is that we should be able to satisfy ourselves that the measures taken by us are adequate, appropriate and we must follow the spirit of these measures and the requirements as enshrined in the Prevention of Money Laundering Act, 2002. (PMLA)

## 2. Back Ground:

2.1 The Prevention of Money Laundering Act, 2002 came into effect from 1st July 2005. Necessary Notifications / Rules under the said Act were published in the Gazette of India on 1st July 2005 by the Department of Revenue, Ministry of Finance, Government of India. As per the provisions of the Act, every banking company, financial institution (which includes chit fund company, a co-operative bank, a housing finance institution and a non-banking financial company) and **intermediary (which includes a stock-broker, sub-broker,** share transfer agent, banker to an issue, trustee to a trust deed, registrar to an issue, merchant banker, underwriter, portfolio manager, investment adviser and any other intermediary associated with securities market and registered under section 12 of the Securities and Exchange Board of India Act, 1992) shall have to maintain a record of all the transactions; the nature and value of which has been prescribed in the Rules under the PMLA. Such transactions include:

- All cash transactions of the value of more than Rs 10 lacs or its equivalent in foreign currency.

- All series of cash transactions integrally connected to each other which have been valued below Rs 10 lakhs or its equivalent in foreign currency where such series of transactions take place within one calendar month.

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

It may, however, be clarified that for the purpose of suspicious transactions reporting, apart from 'transactions integrally connected', 'transactions remotely connected or related' should also be considered.

## 3. Policies and Procedures to Combat Money Laundering and Terrorist financing.

### 3.1 Guiding Principles

3.1.1 The detailed guidelines in Part II have outlined relevant measures and procedures to guide the registered intermediaries in preventing money laundering and terrorist financing. Considering the specific nature of its business, organizational structure, type of customer and transaction, etc. we should satisfy ourselves that we feel following measures are adequate and appropriate to follow the spirit of the suggested measures in Part II and the requirements as laid down in the Prevention of Money Laundering Act, 2002.

### 3.2 Obligation to establish policies and procedures

3.2.1 Under the Prevention of Money Laundering Act, 2002 as a Securities Market Intermediary, we must establish procedures of internal control aimed at preventing and impeding money laundering and terrorist financing. In order to fulfill these requirements, there is also a need for us to have a system in place for identifying, monitoring and reporting suspected money laundering or terrorist financing transactions to the law enforcement authorities.

3.2.2 In light of the above, senior management is 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.

3.2.3 **Our Policies and procedures to combat Money Laundering covers:**

a. Communication of group policies relating to prevention of money laundering and terrorist financing to all management and relevant staff that handle account information, securities transactions, money and customer records etc. whether in branches, departments or subsidiaries;

b. Customer acceptance policy and customer due diligence measures, including requirements for proper identification;

c. Maintenance of records;

d. Compliance with relevant statutory and regulatory requirements;

e. Co-operation with the relevant law enforcement authorities, including the timely disclosure of information; and

f. Role of internal audit or compliance function to ensure compliance with policies, procedures, and controls relating to prevention of money laundering and terrorist financing, including the testing of the system for detecting suspected money laundering transactions, evaluating and checking the adequacy of exception reports generated on large and/or irregular transactions, the quality of reporting of suspicious transactions and the level of awareness of front line staff of their responsibilities in this regard.

## PART IIDETAILED POLICIES AND PROCEDURES

### 4. Written Anti Money Laundering Procedures

4.1 We as securities market intermediary hereby adopt written procedures to implement the anti money laundering provisions as envisaged under the Anti Money Laundering Act, 2002 which includes the following three specific parameters which are related to the overall **'Client Due Diligence Process'**:

a. Policy for acceptance of clients

b. Procedure for identifying the clients

c. Transaction monitoring and reporting especially Suspicious Transactions Reporting (STR)

### 5. Customer Due Diligence

5.1 The customer due diligence ("CDD") measures comprise the following:

(a) Obtaining sufficient information in order to identify persons who beneficially own or control securities account. Whenever it is apparent that the securities acquired or maintained through an account are beneficially owned by a party other than the client, that party should be identified using client identification and verification

procedures. 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. It also incorporates those persons who exercise ultimate effective control over a legal person or arrangement.

(b) Verify the customer's identity using reliable, independent source documents, data or information;

(c) 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;

(d)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

(e) 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 our intermediary's knowledge of the customer, its business and risk profile, taking into account, where necessary, the customer's source of funds.

## 5.2 Policy for acceptance of clients:

5.2.1 The following safeguards are to be followed while accepting the clients:

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

- To ensure this we must insist the client to fill up all the necessary details in the KYC form in our presence and obtain all the necessary documentary evidence in support of the information filled in KYC. We must verify all the documents submitted in support of information filled in the KYC form with the originals and in-person verification should be done by our own staff. Moreover new client should either be introduced by an existing customer or by the senior official of the company. In case we have doubt that in-complete / fictitious information is submitted by the client, we must ask for such additional information so as to satisfy ourself about the genuineness of the client and the information of the client before accepting his registration.

b) Factors of risk perception of the client :-

| Particulars | Risk Perception |
|---|---|
| **Factors of Risk Perception having regard to :** | |
| **Client`s Location ( Registered / Correspondence/ other address )** | |
| - Face to Face clients of Delhi & NCR | Low Risk |
| - Face to Face clients of other than Delhi & NCR | Low Risk |
| - Client Introduced by existing Face to Face Clients | Low Risk |
| - Client Introduced by other Existing Clients | Medium Risk |
| - Direct Clients of Delhi & NCR | Medium Risk |
| - Direct Clients of other than Delhi & NCR | High Risk |
| - Non resident Clients | High Risk |
| **Nature of Business Activity, Trading Turnover etc** | |
| -Retail clients ( average daily turnover < Rs 10 Lakhs or net settlement obligation < Rs 2 Lakhs ) | Low Risk |
| - Retail clients ( average daily turnover Rs.10- 25 Lakhs or net settlement obligation Rs.2-5 Lakhs ) | Medium Risk |
| - Retail Clients ( average daily turnover > Rs 25 Lakhs or net settlement obligation > Rs 5 Lakhs ) | High Risk |
| **Manner of Making Payment** | |
| - Regular payment through A/c payee cheque from the Bank A/c already mapped with us | Low Risk |
| - Payment through A/c payee cheque from the Bank A/c other than one already mapped with us | Medium Risk |
| - Payment through Banker`s Cheque / Demand Draft / Cash | High Risk |
| **Client of Special Categories as defined under Para 5.4 of these Guidelines** | Very High Risk |

c) 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.

c) Ensure that an account is not opened where we unable to apply appropriate clients due diligence measures / KYC policies. This shall be applicable in cases where it is not possible to ascertain the identity of the client, information provided to the intermediary is suspected to be non-genuine, perceived non co-operation of the client in providing full and complete information. We should not continue to do business with such a person and

file a suspicious activity report. We should also evaluate whether there is suspicious trading in determining whether to freeze or close the account.

We should be cautious to ensure that we do not return securities or money that may be from suspicious trades after consulting the relevant authorities in determining what appropriate action should be taken when we suspect suspicious trading.

e) In case the client propose to deal through a POA / authorised person we must analyse the circumstances under which the client wish to act on behalf of another person / entity. The authority letter / POA must specify in what manner the account will 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 intermediary, 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 and all the KYC document of the Agent / POA must be obtained in addition to that of the client.

f) Necessary checks and verification should be undertaken before opening an account so as to ensure that the identity of the client does not match 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 enforcement agency worldwide.

## 5.3 Risk-based Approach

5.3.1 It is generally recognized that certain customers may be of a higher or lower risk category depending on circumstances such as the customer's background, type of business relationship or transaction etc. As such, we should apply for each of the customer due diligence measures on a risk sensitive basis. The basic principle enshrined in this approach is that we should adopt an enhanced customer due diligence process for higher risk categories of customers. Conversely, a simplified customer due diligence process may be adopted for lower risk categories of customers. In line with the risk-based approach, the type and amount of identification

information and documents that we should obtain necessarily depend on the risk category of a particular customer.

### 5.4 Clients of special category (CSC):

Such clients include the following-

a. Non resident clients

b. High networth clients ( Clients having , Networth >= 25 Lakh and/or Annual Income exceeding Rs 10 Lakh)

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 we should exercise independent judgment to ascertain whether new clients should be classified as CSC or not.

### 5.5 Client identification procedure:

# Capital Wizard Stock Broking Pvt. Ltd

- The 'Know your Client' (KYC) policy :-
  - **while establishing the intermediary – client relationship**

    No account shall be opened unless all the KYC Norms as prescribed from time to time by the SEBI / Exchanges are duly complied with, all the information as required to be filled in the KYC form (including financial information, occupation details and employment details) is actually filled in and the documentary evidence in support of the same is made available by the client. Moreover all the supporting documents should be verified with originals and client should sign the KYC & MCA in presence of our own staff. Moreover client should be introduced by an existing clients or the known reference.

  - **while carrying out transactions for the client**

    RMS department should monitor the trading activity of the client and to exercise due diligence to ensure that the trading activity of the client is not disproportionate to the financial status and the track record of the client.

    Payments department should ensure that payment received form the client is being received in time and through the bank account the details of which are given by the client in KYC form and the payment through cash / bearer demand drafts should not be entertained.

  - When the intermediary has doubts regarding the veracity or the adequacy of previously obtained client identification data.

    The information provided by the client should be checked though independent source namely:

  - Pan No must be verified from Income Tax Web Site
  - Address must be verified by sending Welcome Letter / Qtly Statement of Account, and in case any document returned undelivered the client should be asked to provide his new address proof before doing any further transaction.

- In case we have reasons to believe that any of our existing / potential customer is a politically exposed person (PEP) we must exercise due diligence, to ascertain weather the customer is a politically exposed person (PEP), which would include seeking additional information from clients and accessing publicly available information etc.

- The dealing staff must obtain senior management`s prior approval for establishing business relationships with Politically Exposed Persons. In case an existing customer is subsequently found to be, or subsequently becomes a PEP, dealing staff must obtain senior management`s approval to continue the business relationship.

- We must take reasonable measures to verify source of funds of clients identified as PEP.

- The client should be identified by using reliable sources including documents / information and we should obtain adequate information to satisfactorily establish the identity of each new client and the purpose of the intended nature of the relationship.

- The information should be adequate enough to satisfy competent authorities (regulatory / enforcement authorities) in future that due diligence was observed by the intermediary in compliance with the Guidelines. Each original documents should be seen prior to acceptance of a copy.

- Failure by prospective client to provide satisfactory evidence of identity should be noted and reported to the higher authority.

- While accepting a client we must follow the KYC guidelines as prescribed by SEBI as the minimum requirements relating to KYC from time to time. Further, we must also maintain continuous familiarity and follow-up where we notice inconsistencies in the information provided. The underlying objective should be to follow the requirements enshrined in the PML Act, 2002 SEBI Act, 1992 and Regulations, directives and circulars issued there under so that we are aware of the clients on whose behalf we are dealing.

- We must follow a client identification programme as prescribed in the Notification No. 9/2005 dated July 01, 2005 (as amended from time to time), which notifies rules for maintenance of records of the nature and value of transactions, the procedure and manner of maintaining and time for furnishing of information and verification of records of the identity of the clients of the banking companies, financial institutions and intermediaries of securities market and such other additional requirements that it considers appropriate to enable it to determine the true identity of its clients.

- It may be noted that while risk based approach may be adopted at the time of establishing business relationship with a client; there is no exemption from obtaining the minimum information/documents from clients in respect of any class of investors.

## 6. Record Keeping

6.1 We must ensure compliance with the record keeping requirements contained in the SEBI Act, 1992, Rules and Regulations made there-under, PML Act, 2002 as well as other relevant legislation, Rules, Regulations, Exchange Bye-laws and Circulars.

6.2 We must maintain such records as are sufficient 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.

6.3 Should there be any suspected drug related or other laundered money or terrorist property, the competent investigating authorities would need to trace through the audit trail for reconstructing a financial profile of the suspect account. To enable this reconstruction, we should retain the following information for the accounts of our customers in order to maintain a satisfactory audit trail:

(a) the beneficial owner of the account;

(b) the volume of the funds flowing through the account; and

(c) for selected transactions:

- the origin of the funds;
- the form in which the funds were offered or withdrawn, e.g. cash, cheques, etc.;
- the identity of the person undertaking the transaction;
- the destination of the funds;
- the form of instruction and authority.

6.4 All should ensure that all customer and transaction records and information are available on a timely basis to the competent investigating authorities.

6.5 We must maintain proper record of transactions prescribed under Rule 3, notified under the Prevention of Money Laundering Act (PMLA), 2002 as mentioned below:

(i) all cash transactions of the value of more than rupees ten lakh or its equivalent in foreign currency;

(ii) all series of cash transactions integrally connected to each other which have been valued below rupees ten lakh or its equivalent in foreign currency where such series of transactions have taken place within a month and the aggregate value of such transactions exceeds rupees ten lakh;

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

(iv) all suspicious transactions whether or not made in cash and by way of as mentioned in the Rules.

## 7. Information to be maintained

We must maintain and preserve the following information in respect of transactions referred to in Rule 3 of PMLA Rules:

I. the nature of the transactions;

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

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

IV. the parties to the transaction.

## 8. Retention of Records

8.1 We must maintain and preserve such records and information in a manner that allows easy and quick retrieval of data as and when requested by the competent authorities and such record have to be maintained and preserved for a period of ten years from the date of cessation of the transactions between the client and intermediary.

8.2 We have to maintain the records of the identity of clients have to be maintained and preserved for a period of ten years from the date of cessation of the transactions between the client and intermediary.

8.3 Thus the following document retention terms should be observed:

(a) All necessary records of transactions (namely financial statements, DP Account statements, Contract Notes, statement of securities etc ), for both domestic and international, should 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.

(b) 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 should also be kept for the same period.

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

## 9. Monitoring of transactions

9.1 Regular monitoring of transactions is vital for ensuring effectiveness of the Anti Money Laundering procedures. This is possible only if we understand the normal activity of the client so that we can identify the deviant transactions / activities.

9.2 We must pay special attention to all complex, unusually large transactions / patterns which appear to have no economic purpose. We must monitor internal threshold limits for each class of client account as defined in Para 5.2.1(b) of these guidelines and pay special attention to the transaction that exceeds these limits.

9.3 We should ensure that record of transaction is preserved and maintained in terms of section 12 of the PMLA 2002 and that 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 also be regularly reported to the higher authorities / head of the department.

9.4 Further the RMS / Compliance Department should 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.

## 10. Suspicious Transaction Monitoring & Reporting

10.1 We must examine a selection of transaction undertaken by clients on regular basis to enable suspicious transactions as defined in PML Rules as amended from time to time to be recognised and have follow appropriate procedures for reporting suspicious transactions.

10.2 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:

a) Clients whose identity verification seems difficult or clients appears not to cooperate

b) Asset management services for clients where the source of the funds is not clear or not in keeping with clients apparent standing /business activity;

c) Clients in high-risk jurisdictions or clients introduced by banks or affiliates or other clients based in high risk jurisdictions;

d) Substantial increases in business without apparent cause;

e) Unusually large cash deposits made by an individual or business;

f) Clients transferring large sums of money to or from overseas locations with instructions for payment in cash;

g) Transfer of investment proceeds to apparently unrelated third parties;

h) 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.

10.3 Any suspicious transaction should be immediately notified to the Money Laundering Control Officer or and the Principle Officer, Sanjay Dutt Sharma. 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. **However, it should be ensured that there is continuity in dealing with the client as normal until told otherwise and the client should not be told of**

**the report/suspicion**. In exceptional circumstances, consent may not be given to continue to operate the account, and transactions may be suspended, in one or more jurisdictions concerned in the transaction, or other action taken.

10.4 It is likely that in some cases transactions are abandoned/aborted by customers on being asked to give some details or to provide documents. We must take a note of the same and report all such attempted transactions in STRs, even if not completed by customers, irrespective of the amount of the transaction.

## 11. Reporting to Financial Intelligence Unit-India

11.1 In terms of the PMLA rules, we are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND) at the following address in the format as prescribed in PMLA Rules:

Director, FIU-IND,
Financial Intelligence Unit-India,
6th Floor, Hotel Samrat,
Chanakyapuri,
New Delhi-110021.
Website: http://fiuindia.gov.in

11.2 We should carefully go through all the reporting requirements and formats enclosed with this circular. These requirements and formats are divided into two parts- Manual Formats and Electronic Formats. Details of these formats are given in the documents (Cash Transaction Report- version 1.0 and Suspicious Transactions Report version 1.0) which are also enclosed with this circular. These documents contain detailed guidelines on the compilation and manner/procedure of submission of the manual/electronic reports to FIU-IND. The related hardware and technical requirement for preparing reports in manual/electronic format, the related data files and data structures thereof are also detailed in these documents. In case we are not in a position to immediately file electronic reports, we may file manual reports to FIU-IND as per the formats prescribed. While detailed instructions for filing all types of reports are given in the instructions part of the related formats, we should adhere to the following:

(a) The cash transaction report (CTR) (wherever applicable) for each month should be submitted to FIU-IND by 15th of the succeeding month.

(b) The Suspicious Transaction Report (STR) should 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 should record his 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.

(c) The Principal Officer will be responsible for timely submission of CTR and STR to FIU-IND;

(d) Utmost confidentiality should be maintained in filing of CTR and STR to FIU-IND. The reports may be transmitted by speed/registered post/fax at the notified address.

(e) No nil reporting needs to be made to FIU-IND in case there are no cash/suspicious transactions to be reported.

11.3 We should not put any restrictions on operations in the accounts where an STR has been made moreover we all {directors, officers and employees (permanent and temporary)} are prohibited from disclosing ("tipping off") the fact that a STR or related information is being reported or provided to the FIU-IND to the client at any level.

## 12. Designation of an officer for reporting of suspicious transactions

12.1 To ensure that we properly discharge our legal obligations to report suspicious transactions to the authorities, We have already appointed Mrs. Mamta Goswami as the Principal Officer, who 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.

## 13. Employees' Hiring/Employee's Training/ Investor Education

### 13.1 Hiring of Employees

Having regard to the risk of money laundering and terrorist financing and the size of our business, we have identified various screening procedures to ensure high standards

when hiring employees at the key positions and that employees taking up such key positions are suitable and competent to perform their duties.

## 13.2 Employees' Training

We have implemented an ongoing employee training programme so that the members of the frontline staff, back office staff, compliance staff, risk management staff and staff dealing with new customers are adequately trained in AML and CFT procedures. 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.

## 13.3 Investors Education

Implementation of AML/CFT measures requires us to demand certain information from investors which may be of personal nature or which 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 customer with regard to the motive and purpose of collecting such information. There is, therefore, a need to educate the customer of the objectives of the AML/CFT programme.