GUIDELINES FOR ANTI MONEY LAUNDERING MEASURES

Anti-Money Laundering Procedures

SEBI vide Circular Ref No: ISD/CIR/RR/AML/1/06 dated January 18, 2006 issued the 'Guidelines for market intermediaries on Anti Money Laundering Standards'.

Each registered intermediary was advised to adopt written procedures to implement the anti money laundering provisions as envisaged under the Anti Money Laundering Act, 2002 and to comply with the Circular, Guidelines, Prevention of Money laundering Act, 2002 and the Rules issued thereunder.

The Prevention of Money Laundering Act, 2002 has come into effect from 1st July 2005. Necessary Notifications / Rules under the said Act have been published in the Gazette of India on 1st July 2005 by the Department of Revenue, Ministry of Finance, Government of India. The Act has also imposed certain responsibilities on the various financial institutions and intermediaries with regard to preventing terrorist financing and money laundering.

SEBI vide its circular dated January 18, 2006 and RBI vide its Notification dated February 21, 2005 (for NBFCs) have provided broad guidelines on Anti-Money Laundering Standards ('the Guidelines'). The banking companies, financial institutions and intermediaries (applicable entities) were also advised by SEBI/RBI, to ensure that a proper policy framework on anti-money laundering measures is put into place.

SEBI has in its circular dated March 20, 2006, invited attention to notifications dated July 01, 2005 and December 13, 2005, issued by the Central Government, notifying the rules under the Prevention of Money Laundering Act, 2002 (the Rules). These Rules cast certain obligations on the intermediaries in regard to preservation of records and reporting of transactions.

PPFAS being registered with SEBI as "Portfolio Manager" and PPFAS being registered as Stock Brokers shall ensure that all the important provisions pertaining to PMLA are included and implemented at all time and shall 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

Steps for Implementing the Policy

1. Appointment of Principal Officer

The Rules/Guidelines states that all the applicable entities as defined under the Act shall appoint a Principal Officer as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in identification and assessment of potentially suspicious transactions.

- **Mr. Ashish Shah is** the designated Officer for PPFAS Ltd. registered as Stock Broker and Portfolio Manager with SEBI.

Names, designation and addresses (including e-mail addresses) of 'Principal Officer' including any changes therein shall also be intimated to the Office of the Director-FIU

The Principal Officers mentioned above or any other officer authorized by him is responsible for the following:

- Communicating the Policy on Prevention of Money Laundering to the employees of respective companies
- Receiving reports from employees for any suspicious dealings noticed by them
- Clarifying any queries from employees on this matter
- Ensuring that the employees dealing with the clients / prospective clients are aware of the KYC guidelines of the Company and are advised to follow the same strictly
- Conduct a sample test of client dealings, by themselves or through an internal audit process, to satisfy them that no suspicious activities exist.
- Report any suspicious transactions to appropriate authorities

2. Client Identification and Due Diligence Policy

- All such documents as are specified in the KYC checklist maintained by the company for respective categories of customers must be received from the Client at the time of opening of account.
- If the documentation produced by the prospective client is not in conformity with the requirements specified from time to time or if there are any inconsistencies noticed therein, no account shall be opened and matter reported to the Principal Officer or any other officer authorized by him immediately.
- As far as possible using reasonable measures, the employee dealing with the Client should ensure that the person opening the account himself is the beneficial owner or there exists sufficient documentation to corroborate his transacting on behalf of the other person, in which case appropriate due diligence would be done on the beneficial owner as well.

- Wherever possible reasonably, efforts will be made by the employee dealing with the prospective Client to verify the details provided to him, using third party sources.
- On an ongoing basis, appropriate due diligence and scrutiny shall be performed on the account to ensure that the transactions being conducted are consistent with the Company's knowledge of the customer, its business & risk profile, taking into account, where necessary, the customer's sources of funds.
- In-Person Verification of Clients is carried out by employees of the company and the date of in-person verification, name & signature of the official who has done the in-person verification and the member's stamp incorporated in the client registration form and also the proofs of the clients are verified with the originals.
- If account in the name of more than one person has been opened from the same address, it will ensure that such persons really reside or are related to that address. In case of a company/firm, it will ensure that the firm operates from the address given by it in the KYC form.
- Documentary evidences and details as per "Know Your Client" guidelines issued by SEBI shall be sought from the client to establish the identity of the client.
- Each original document shall be seen prior to acceptance of its copy by the relationship manager and the same shall be confirmed by the respective official by him inscribing "Verified with originals" along with his/her name and signature on the copy of the document.
- Following clients are considered to the Clients of Special Category (CSC)
    - Non resident clients
    - High Net worth Individuals
    - Trusts, Charities, NGOs and organizations receiving donations
    - Companies having close family shareholding or beneficial ownership
    - Politically exposed persons (PEPs) of foreign origin: 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,
    - 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 centers, tax havens, countries where fraud is highly prevalent.
    - Non face to face clients
    - Clients with dubious reputation as per public information available etc.

Due Diligence performed in respect of clients of special category will be same as other clients like appropriate due diligence and scrutiny shall be performed on the account to ensure that the transactions being conducted are consistent with the Company's knowledge of the CSC, its business & risk profile, taking into account, where necessary, the his sources of funds

Client Risk Classification:

We have identified clients into high, medium and low risk and the same has been incorporated and implemented in our back office system based on following criteria:

- Timely Clients' Pay-in of funds and securities
- Cases of cheque bouncing of clients especially cheque bouncing due to insufficiency of funds
- Inconsistency in turnover pattern(sudden rise and fall)
- High trading activity for a short period with long spells of no-activity.
- Frequent changes in bank accounts/DP accounts
- Non-cooperation of client in furnishing vital information as and when required.

3. <u>Client Acceptance Policy</u>

The Department responsible for Account Opening shall also take steps to ensure that,

- It shall not accept any client who are unable to produce satisfactory documents establishing their identity, as required under the KYC checklist framed by PPFAS, as modified from time to time.
- No account is opened in anonymous or fictitious/ benami name(s). To prevent the opening of account in fictitious or benami name following steps shall be taken:

(a) The signature of the client is verified with the signature appearing on the proof of photo identity (PAN card).

(b) The details of PAN card are cross-verified from the Income- Tax/NSDL website.

(c) Relevant documents are collected from the clients and provided to the relationship manager.

(d) The KYC and agreements are signed by the client himself. Under no circumstances, account shall be opened on the basis of the signature of Power of Attorney holder.

- No client account is opened where it is not possible to apply appropriate client due-diligence measures/policies e.g. suspected non genuine/incomplete information, client's non-co-operation, incomplete KYC form, non-availability of documents with the client, reluctance of client to personally meet the officials etc.

- Where a client fails to provide such information, the matter shall be reported to the appropriate higher authority.

- Reasonable enquiries are made about the client's background including criminal background through the website (URL: http://www. watchoutinvestors.com) and banned entities list maintained by the Exchanges to ensure that the client is not banned in any manner by the regulators.

The Guidelines state that where it is not possible to ascertain the identity of the client, information provided to the applicable entities is suspected to be non-genuine, the client does not co-operate in providing full and complete information, applicable entities should

not deal with such clients and file a suspicious activity report. Therefore, the client will be accepted only after satisfying about their genuineness.

4. <u>Transaction Monitoring, record keeping and reporting : Suspicious Transactions Reporting (STR)</u>

- As a policy, PPFAS group companies shall not accept cash from any clients.
- The Principal Office or any other officer authorized by him, through the Internal Audit mechanism, arrange to review selection of transactions undertaken by clients so as to check if there are any suspicious transactions
- Record of all transactions and KYC documents collected from the Clients shall be maintained at least for such period as prescribed under the relevant Regulations.
- Any transactions needing special attention such as complex transactions, unusually large transactions / patterns which appear to have no economic rationale etc. shall be brought to the notice of the Principal Officer.
- Transactions in the nature as below are examples of suspicious transactions:
    - Clients whose identity verification seems difficult or client appears not to cooperate
    - Portfolio Management services for clients where source of funds is not clear or not in keeping with clients apparent standing / business activity
    - Clients in high risk jurisdictions or clients introduced by intermediaries / referral sources based in high risk jurisdictions
    - Substantial increase in business without apparent cause
    - Unusually large cash deposits made by an individual or business
    - Clients transferring large sums of money to or from overseas locations with instructions for payment in cash
    - Unusual transactions by CSC and business undertaken by offshore banks / financial services, business reported in the nature of export-import of small items etc
- Inconsistency in risk profile and turnover.
- Inconsistency in turnover pattern(sudden rise and fall)
- High trading activity for a short period with long +spells of no-activity.
- Frequent withdrawal of high amounts from trading accounts.
- Frequent changes in bank accounts/DP accounts
- Non-cooperation of client in furnishing vital information as and when required.
- Transfer of funds from one account to other accounts opened in the name of same person

PPFAS's CTCL and Back Office system is in place to generate alerts based on set parameters for suspicious transactions. Risk Management Team scrutinize and constantly monitor the alerts and take necessary steps, if required.
Any such suspicious transaction should be reported immediately to the Money Laundering Control Officer (Principal Officer) mentioned hereunder and his advice taken

<u>Timely access of data</u>: The Principal Officer/Money Laundering Control Officer and other appropriate compliance, risk management and related staff members shall have timely access to customer identification data and other Customer Due Diligence information, transaction records and other relevant information."

5. Monitoring of sources of funds and securities:

As per regulations issued by SEBI, a stock broker cannot accept shares/funds from third parties, on behalf of a client. Similarly, a stock broker cannot make payment/delivery of money and shares to third party account. The Designated Department and/or Back Office Operations will therefore initiate necessary steps to ensure that no third-party funds/securities are accepted. Similarly, the Designated Department and/or Back Office Operations shall ensure that no funds/securities are paid to a third-party account or to any account other than the designated account of the client. The Back Office Department of the Company has a system in place to monitor third party checks.

6. Reporting of Suspicious Transactions:

a. Reporting to the Principal Officer

The Guidelines provide that any suspicious transaction needs to be immediately notified to the Money Laundering Control Officer (Principal Officer) or any other designated officer of the intermediary.

The Designated Department will analyse and furnish a report of any such transactions to the Principal Officer as and when it is noticed and on a consolidated basis at the end of every month for his analysis and review.

A detailed report along with specific reference to the clients' transactions and the nature/reason for suspicion shall be furnished to the Principal Officer.

In case the Designated Department comes to know about any suspicious transactions, intimation of the same shall be sent to the Principal Officer as per Annexure -1 within 2 working days from the date on which the Department became aware of such a transaction.

There is no requirement in the Guidelines to send a "NIL Report" to the FIU-IND if no suspicious activity or transaction is observed.

b. Reporting to the FIU-IND

The following procedure shall be adopted for the reports to be sent to the FIU-IND,

The Principal Officer shall arrange to forward the report in the given format to the FIU-IND within the stipulated time, through the Compliance Team.

The Compliance Team will maintain a record of all such reports forwarded to the FIU-IND.

A copy of the above report shall also be forwarded by the Compliance Team to the Designated Department. Compliance Team shall, in parallel, maintain records of clients reported to FIU-IND.

7. Suspension of Transactions

The Guidelines also state that every applicable entity shall ensure that tipping-off does not take place i.e. the client is not directly or indirectly intimated about the reporting.

As per the Guidelines, there shall be continuity to deal with the client as normal until the FIU-IND has intimated otherwise.

As per the Guidelines suspension of transactions of the client shall be done in exceptional circumstances. This requirement has been stipulated to ensure that the client, who is reported to the FIU-IND, is not alerted about any such reporting. The criteria for suspension shall be formulated by the Designated Department.

8. Record maintenance

With regard to record keeping and maintenance, the Guidelines provide the following:

- Maintaining records of clients for a period of ten years from the date of cessation of the transactions between the clients and the applicable entity.

- In case where investigations have been initiated by FIU-IND or transactions have been subject matter of suspicious activity reporting, records may be preserved until it is confirmed that ongoing investigations have been closed.

In order to meet the requirements of the aforesaid guidelines and also reproduce the required details to FIU-IND, when called for, the below mentioned action shall be co-ordinated by the Compliance Team, with regard to clients who have been reported to FIU-IND:

Following records of the client shall be maintained by the Compliance Team in parallel and in addition to the records maintained by the concerned department.

- KYC form along with necessary details/documents.

- Statement of accounts of the client.

- Details of trades executed by the client.

  - Trades executed by the client during the past five years and the statement of account for five years, shall be added to the file.

  - Details of subsequent trades executed by the client and statement of account of the client shall be appended to the file, every calendar half-year.

9. Role of the Compliance Team

The Compliance Team shall conduct the following activities:

- Intimation of appointment of Principal Officer to FIU-IND.
- Formulating the Policy in co-ordination with other departments.
- Intimating and creating awareness
- Periodic review of the Policy.
- The Compliance Team shall review the policy regularly
- The Guidelines state that the person conducting the review shall be different from the one who framed such policies and procedures.
- On going Training of staff for implementation of the Policy
- Compliance Team in co-ordination with the Human Resources Department (HRD) shall undertake necessary training for employees for implementing the Policy.

- Implementation
  - Ensure that policies, procedures and controls stipulated in regard to the Guidelines are effectively implemented.

10. Staff Training

The Guidelines provide that staff of the applicable entities shall be provided proper training on anti-money laundering and anti-terrorist financing measures and high standards are maintained while hiring employees.

The Guidelines also state that an applicable entity shall assess key roles within the organization with regard to risk of money laundering and terrorist financing and ensure that employees taking up such key roles are suitable and competent to perform their duties.

In view of the same, training programs shall be conducted in consultation/co-ordination with Compliance Team, for employees who handle activities under the Guidelines. Audit and Inspection section within Compliance will lead the exercise.

The HRD shall undertake the following activities:

- Making arrangements for conducting training program on anti money-laundering and anti terrorist-financing measure for the staff, by the Compliance Team, in order to equip them to meet the requirements of the Guidelines.

- Adequate screening procedures shall be put in place to ensure high standards when hiring employees. Key positions within the organization structures having regard to the risk of money laundering/terrorist financing and size of business shall be identified. It shall be ensured that employees taking up such key positions are suitable and competent to perform their duties.

Clients are also sensitized and made aware about the requirements of provisions emanating from AML and CFT framework through the ‘guidelines for Anti-Money Laundering Measures’ made available on the website of the company

PREVENTION OF MONEY-LAUNDERING GUIDELINES : POLICY & PROCEDURES

Introduction

The Prevention of Money Laundering Act, 2002 has come into effect from 1st July 2006. Necessary Notifications / Rules under the said Act have been published in the Gazette of India on 1st July 2005 by the Department of Revenue, Ministry of Finance, Government of India. The Act has also imposed certain responsibilities on the various financial institutions and intermediaries with regard to preventing terrorist financing and money laundering.

SEBI vide its circular dated January 18, 2006 and RBI vide its Notification dated February 21, 2005 (for NBFCs) have provided broad guidelines on Anti-Money Laundering Standards ('the Guidelines'). The banking companies, financial institutions and intermediaries (applicable entities) were also advised by SEBI/RBI, to ensure that a proper policy framework on anti-money laundering measures is put into place.

SEBI has in its circular dated March 20, 2006, invited attention to notifications dated July 01, 2005 and December 13, 2005, issued by the Central Government, notifying the rules under the Prevention of Money Laundering Act, 2002 (the Rules). These Rules cast certain obligations on the intermediaries in regard to preservation of records and reporting of transactions.

PPFAS being registered with SEBI as "Portfolio Manager" and PPFAS being registered as Stock Brokers shall ensure that all the important provisions pertaining to PMLA are included and implemented at all time and shall have to maintain a record of all the transactions; the nature & value of which has been prescribed under the Prevention of Money Laundering Act. Such transactions include:

- All cash transactions of the value 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 lacs 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 demat account, security account maintained by us.
- For the purpose of suspicious transactions reporting, apart from transactions integrally connected, transactions remotely connected or related are also to be considered.
- 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.

As per the Rules, the following information needs to be maintained in respect of the aforesaid transactions,

- Nature of transaction
- Amount of transaction and currency in which it was denominated
- Date of transaction

- Parties to the transaction

Maintenance and preservation of records

Under the Rules, records of client are required to be maintained for a period of 10 years from the date of cessation of transactions between the client and the applicable entity.

Reporting to Financial Intelligence Unit – India

The Rules state that every financial intermediary shall appoint a Principal Officer who shall act as a central reference point for interacting with FIU-IND. Details of the Principal Officer as prescribed in the Rules, shall be furnished to the FIU-IND.

As per the Rules, information of cash and suspicious transactions are to be reported **by the Principal Officer** to the Director, Financial Intelligence Unit – India (FIU -IND) in manual and electronic formats, as per the given Guidelines, at the address given below:

Director, FIU-IND
Financial Intelligence Unit – India,
6th floor, Hotel Samrat
Chanakyapuri
New Delhi 110021

The Rules also state that applicable entities who are not in a position to file electronic reports, may file manual reports to FIU-IND. The applicable entities are required to adhere to the following,

- The Cash Transaction Report (CTR) for each month should be submitted to FIU)IND by 15th of the succeeding month

- The Suspicious Transaction Report (STR) should be submitted within 7 days of arriving at a conclusion that any transactions, whether cash or non-cash, or a series of transactions, integrally connected are of suspicious nature.

- The Principal Officer shall be responsible for timely submission of the reports.

- Utmost confidentiality should be maintained in filing the reports. The reports should be forwarded to FIU-IND by speed/registered post/fax.

No restrictions should be placed on clients whose transactions have been reported to FIU-IND. No tipping off to the client should be done at any level.

The Act provides that, in case an applicable entity or its officers have failed to comply with the provisions of the Act, such applicable entity shall be liable for a fine of Rs. 10,000/- which may extend upto Rs. 1,00,000/- for each failure.

Scope of the Guidelines

This document containing policy and procedures on Anti-Money-Laundering has been drafted as a compendium of all the circulars and guidelines which were circulated previously. This has been prepared for ease of reference and proper dissemination amongst the Company for implementation of the Guidelines.

The Policy

This policy has been drafted keeping in view the aforesaid Guidelines and Rules.

As provided in the Guidelines/ Rules, the policy identifies the major areas of activity related to dealing with clients such as customer identification and acceptance, reporting of suspicious transactions and maintenance of records for implementation by PPFAS.

The policy mainly focuses on:

1. Appointment of Principal Officer.
2. Client Identification Policy.
3. Client Acceptance Policy
4. Transaction monitoring
5. Monitoring of sources of funds and securities.
6. Reporting of suspicious transactions
7. Suspension of transactions.
8. Record maintenance.
9. Role of the Compliance Team.
10. Staff training.
11. Do’s and Don’ts for employees and sub-intermediaries of PPFAS.

The above-mentioned functions shall be suitably assigned to the departments which handle the respective activities.

Steps for Implementing the Policy

. Appointment of Principal Officer

The Rules/Guidelines states that all the applicable entities as defined under the Act shall appoint a Principal Officer as a central reference point in facilitating onward reporting of suspicious transactions and for playing an active role in identification and assessment of potentially suspicious transactions.

- **Mr. Parag Parikh** would be the designated Officer for PPFAS Ltd. registered as Stock Broker with SEBI

- **Mr. Rajeev Thakkar** would be the designated officer for PPFAS, registered as Portfolio Manager with SEBI.

Names, designation and addresses (including e-mail addresses) of 'Principal Officer' including any changes therein shall also be intimated to the Office of the Director-FIU

The Principal Officers mentioned above or any other officer authorized by him is responsible for the following:

- Communicating the Policy on Prevention of Money Laundering to the employees of respective companies
- Receiving reports from employees for any suspicious dealings noticed by them
- Clarifying any queries from employees on this matter
- Ensuring that the employees dealing with the clients / prospective clients are aware of the KYC guidelines of the Company and are advised to follow the same strictly
- Conduct a sample test of client dealings, by themselves or through an internal audit process, to satisfy them that no suspicious activities exist.
- Report any suspicious transactions to appropriate authorities

2. Client Identification and Due Diligence Policy

- All such documents as are specified in the KYC checklist maintained by the company for respective categories of customers must be received from the Client at the time of opening of account.
- If the documentation produced by the prospective client is not in conformity with the requirements specified from time to time or if there are any inconsistencies noticed therein, no account shall be opened and matter reported to the Principal Officer or any other officer authorized by him immediately.
- As far as possible using reasonable measures, the employee dealing with the Client should ensure that the person opening the account himself is the beneficial owner or there exists sufficient documentation to corroborate his transacting on behalf of the other person, in which case appropriate due diligence would be done on the beneficial owner as well.

- Wherever possible reasonably, efforts will be made by the employee dealing with the prospective Client to verify the details provided to him, using third party sources.
- On an ongoing basis, appropriate due diligence and scrutiny shall be performed on the account to ensure that the transactions being conducted are consistent with the Company's knowledge of the customer, its business & risk profile, taking into account, where necessary, the customer's sources of funds.
- In-Person Verification of Clients is carried out by employees of the company and the date of in-person verification, name & signature of the official who has done the in-person verification and the member's stamp incorporated in the client registration form and also the proofs of the clients are verified with the originals.
- If account in the name of more than one person has been opened from the same address, it will ensure that such persons really reside or are related to that address. In case of a company/firm, it will ensure that the firm operates from the address given by it in the KYC form.
- Documentary evidences and details as per "Know Your Client" guidelines issued by SEBI shall be sought from the client to establish the identity of the client.
- Each original document shall be seen prior to acceptance of its copy by the relationship manager and the same shall be confirmed by the respective official by him inscribing "Verified with originals" along with his/her name and signature on the copy of the document.
- Following clients are considered to the Clients of Special Category (CSC)
    - Non resident clients
    - High Net worth Individuals
    - Trusts, Charities, NGOs and organizations receiving donations
    - Companies having close family shareholding or beneficial ownership
    - Politically exposed persons (PEPs) of foreign origin: 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,
    - 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 centers, tax havens, countries where fraud is highly prevalent.
    - Non face to face clients
    - Clients with dubious reputation as per public information available etc.

Due Diligence performed in respect of clients of special category will be same as other clients like appropriate due diligence and scrutiny shall be performed on the account to ensure that the transactions being conducted are consistent with the Company's knowledge of the CSC, its business & risk profile, taking into account, where necessary, the his sources of funds

Client Risk Classification:

We have identified clients into high, medium and low risk and the same has been incorporated and implemented in our back office system based on following criteria:

- Timely Clients' Pay-in of funds and securities
- Cases of cheque bouncing of clients especially cheque bouncing due to insufficiency of funds
- Inconsistency in turnover pattern(sudden rise and fall)
- High trading activity for a short period with long spells of no-activity.
- Frequent changes in bank accounts/DP accounts
- Non-cooperation of client in furnishing vital information as and when required.

3. <u>Client Acceptance Policy</u>

The Department responsible for Account Opening shall also take steps to ensure that,

- It shall not accept any client who are unable to produce satisfactory documents establishing their identity, as required under the KYC checklist framed by PPFAS, as modified from time to time.
- No account is opened in anonymous or fictitious/ benami name(s). To prevent the opening of account in fictitious or benami name following steps shall be taken:

(b) The signature of the client is verified with the signature appearing on the proof of photo identity (PAN card).

(b) The details of PAN card are cross-verified from the Income- Tax/NSDL website.

(c) Relevant documents are collected from the clients and provided to the relationship manager.

(d) The KYC and agreements are signed by the client himself. Under no circumstances, account shall be opened on the basis of the signature of Power of Attorney holder.

- No client account is opened where it is not possible to apply appropriate client due-diligence measures/policies e.g. suspected non genuine/incomplete information, client's non-co-operation, incomplete KYC form, non-availability of documents with the client, reluctance of client to personally meet the officials etc.

- Where a client fails to provide such information, the matter shall be reported to the appropriate higher authority.

- Reasonable enquiries are made about the client's background through the website (URL: http://www. watchoutinvestors.com) to ensure that the client is not banned in any manner by the regulators covered by the website.

The Guidelines state that where it is not possible to ascertain the identity of the client, information provided to the applicable entities is suspected to be non-genuine, the client does not co-operate in providing full and complete information, applicable entities should

not deal with such clients and file a suspicious activity report. Therefore, the client will be accepted only after satisfying about their genuineness.

4. <u>Transaction Monitoring, record keeping and reporting : Suspicious Transactions Reporting (STR)</u>

- As a policy, PPFAS group companies shall not accept cash from any clients.
- The Principal Office or any other officer authorized by him, through the Internal Audit mechanism, arrange to review selection of transactions undertaken by clients so as to check if there are any suspicious transactions
- Record of all transactions and KYC documents collected from the Clients shall be maintained at least for such period as prescribed under the relevant Regulations.
- Any transactions needing special attention such as complex transactions, unusually large transactions / patterns which appear to have no economic rationale etc. shall be brought to the notice of the Principal Officer.
- Transactions in the nature as below are examples of suspicious transactions:
    - Clients whose identity verification seems difficult or client appears not to cooperate
    - Portfolio Management services for clients where source of funds is not clear or not in keeping with clients apparent standing / business activity
    - Clients in high risk jurisdictions or clients introduced by intermediaries / referral sources based in high risk jurisdictions
    - Substantial increase in business without apparent cause
    - Unusually large cash deposits made by an individual or business
    - Clients transferring large sums of money to or from overseas locations with instructions for payment in cash
    - Unusual transactions by CSC and business undertaken by offshore banks / financial services, business reported in the nature of export-import of small items etc
- Inconsistency in risk profile and turnover.
- Inconsistency in turnover pattern(sudden rise and fall)
- High trading activity for a short period with long +spells of no-activity.
- Frequent withdrawal of high amounts from trading accounts.
- Frequent changes in bank accounts/DP accounts
- Non-cooperation of client in furnishing vital information as and when required.
- Transfer of funds from one account to other accounts opened in the name of same person

Any such suspicious transaction should be reported immediately to the Money Laundering Control Officer (Principal Officer) mentioned hereunder and his advice taken

PPFAS's CTCL and Back Office system is in place to generate alerts based on set parameters for suspicious transactions. Risk Management Team scrutinize and constantly monitor the alerts and take necessary steps, if required.

Any such suspicious transaction should be reported immediately to the Money Laundering Control Officer (Principal Officer) mentioned hereunder and his advice taken

Timely access of data: The Principal Officer/Money Laundering Control Officer and other appropriate compliance, risk management and related staff members shall have timely access to customer identification data and other Customer De Diligence information, transaction records and other relevant information."

5. Monitoring of sources of funds and securities:

As per regulations issued by SEBI, a stock broker cannot accept shares/funds from third parties, on behalf of a client. Similarly, a stock broker cannot make payment/delivery of money and shares to third party account. The Designated Department and/or Back Office Operations will therefore initiate necessary steps to ensure that no third-party funds/securities are accepted. Similarly, the Designated Department and/or Back Office Operations shall ensure that no funds/securities are paid to a third-party account or to any account other than the designated account of the client. The Back Office Department of the Company has a system in place to monitor third party checks.

6. Reporting of Suspicious Transactions:

a. Reporting to the Principal Officer

The Guidelines provide that any suspicious transaction needs to be immediately notified to the Money Laundering Control Officer (Principal Officer) or any other designated officer of the intermediary.

The Designated Department will analyse and furnish a report of any such transactions to the Principal Officer as and when it is noticed and on a consolidated basis at the end of every month for his analysis and review.

A detailed report along with specific reference to the clients' transactions and the nature/reason for suspicion shall be furnished to the Principal Officer.

In case the Designated Department comes to know about any suspicious transactions, intimation of the same shall be sent to the Principal Officer as per Annexure -1 within 2 working days from the date on which the Department became aware of such a transaction.

There is no requirement in the Guidelines to send a "NIL Report" to the FIU-IND if no suspicious activity or transaction is observed.

b. Reporting to the FIU-IND

The following procedure shall be adopted for the reports to be sent to the FIU-IND,

The Principal Officer shall arrange to forward the report in the given format to the FIU-IND within the stipulated time, through the Compliance Team.

The Compliance Team will maintain a record of all such reports forwarded to the FIU-IND.

A copy of the above report shall also be forwarded by the Compliance Team to the Designated Department. Compliance Team shall, in parallel, maintain records of clients reported to FIU-IND.

7. Suspension of Transactions

The Guidelines also state that every applicable entity shall ensure that tipping-off does not take place i.e. the client is not directly or indirectly intimated about the reporting.

As per the Guidelines, there shall be continuity to deal with the client as normal until the FIU-IND has intimated otherwise.

As per the Guidelines suspension of transactions of the client shall be done in exceptional circumstances. This requirement has been stipulated to ensure that the client, who is reported to the FIU-IND, is not alerted about any such reporting. The criteria for suspension shall be formulated by the Designated Department.

8. Record maintenance

With regard to record keeping and maintenance, the Guidelines provide the following:

- Maintaining records of clients for a period of ten years from the date of cessation of the transactions between the clients and the applicable entity.

- In case where investigations have been initiated by FIU-IND or transactions have been subject matter of suspicious activity reporting, records may be preserved until it is confirmed that ongoing investigations have been closed.

In order to meet the requirements of the aforesaid guidelines and also reproduce the required details to FIU-IND, when called for, the below mentioned action shall be co-ordinated by the Compliance Team, with regard to clients who have been reported to FIU-IND:

Following records of the client shall be maintained by the Compliance Team in parallel and in addition to the records maintained by the concerned department.

- KYC form along with necessary details/documents.

- Statement of accounts of the client.

- Details of trades executed by the client.

- Trades executed by the client during the past five years and the statement of account for five years, shall be added to the file.

- Details of subsequent trades executed by the client and statement of account of the client shall be appended to the file, every calendar half-year.

9. Role of the Compliance Team

The Compliance Team shall conduct the following activities:

- Intimation of appointment of Principal Officer to FIU-IND.
- Formulating the Policy in co-ordination with other departments.
- Intimating and creating awareness
- Periodic review of the Policy.
- The Compliance Team shall review the policy regularly
- The Guidelines state that the person conducting the review shall be different from the one who framed such policies and procedures.
- On going Training of staff for implementation of the Policy
- Compliance Team in co-ordination with the Human Resources Department (HRD) shall undertake necessary training for employees for implementing the Policy.

- Implementation
  - Ensure that policies, procedures and controls stipulated in regard to the Guidelines are effectively implemented.

10. Staff Training

The Guidelines provide that staff of the applicable entities shall be provided proper training on anti-money laundering and anti-terrorist financing measures and high standards are maintained while hiring employees.

The Guidelines also state that an applicable entity shall assess key roles within the organization with regard to risk of money laundering and terrorist financing and ensure that employees taking up such key roles are suitable and competent to perform their duties.

In view of the same, training programs shall be conducted in consultation/co-ordination with Compliance Team, for employees who handle activities under the Guidelines. Audit and Inspection section within Compliance will lead the exercise.

The HRD shall undertake the following activities:

- Making arrangements for conducting training program on anti money-laundering and anti terrorist-financing measure for the staff, by the Compliance Team, in order to equip them to meet the requirements of the Guidelines.

- Adequate screening procedures shall be put in place to ensure high standards when hiring employees. Key positions within the organization structures having regard to the risk of money laundering/terrorist financing and size of business shall be identified. It shall be ensured that employees taking up such key positions are suitable and competent to perform their duties.

Clients are also sensitized and made aware about the requirements of provisions emanating from AML and CFT framework through the 'guidelines for Anti-Money Laundering Measures' made available on the website of the company

11. Do's and Dont's for Employees

All the employees shall also strictly observe the following,:

- Any suspicious activity which comes to the notice of any employee shall be reported by them to the Compliance Team for further action. Strict confidentiality of such a reporting shall be maintained.

- The client shall not be informed about the report/suspicion. Tipping off the client shall not be done at any level

- The employees shall continue to deal with the client in the usual manner.

SEBI has forwarded a public statement issued by Financial Action Task Force (FATF) which urges all jurisdictions to strengthen preventive measures to protect their financial sectors from money laundering and financing of terrorism (ML/FT) risk posed by certain countries. A copy of the FATF statement dated February 25, available at url: http://www.fatf-gafi.org/dataoecd/18/28/42242615.pdf *is maintained by the Compliance Team and the note is taken for the contents of the FATF statement for necessary action and compliance.*

NSE circular no NSE/INVG/2006/44 dated September 05, 2006 and NSE/INVG/2005/05 dated March 10, 2005 have advised the members that they do not deal on behalf of entities restrained from dealing in securities market by SEBI vide its orders. In accordance with that, the compliance team ensures strict compliance with SEBI orders by maintaining and updating a banned entities list for ensuring that none of the clients against whom SEBI restraint orders are passed trade on the Exchange.

SEBI vide its letter ISD/SR/AK/GK/179130/2009 dated October 05, 2009 has advised that the The Financial Action Task Force (FATF) has issued a fresh public statement dated June 26, 2009 to protect the international financial system from the abuse of money laundering and terrorist financing emanating from certain jurisdictions and urging all jurisdictions to apply effective counter measures. A copy of the FATF statement dated June 26, 2009 is available at url: http://www.fatf-gafi.org/document/15/0,3343,en_32250379_32236836_43193871_1_1_1,00.html *is maintained by the Compliance Team and the note is taken for the contents of the FATF statement for necessary action and compliance.*

The updated Consolidated List established and maintained by the 1267 Committee with respect to Al-Qaida, Usama bin Laden and the Taliban and other individuals, groups, undertakings and entities associated with them is made available at url: http://www.un.org/sc/committees/1267/consolist.shtml *the track of which is kept by the compliance team on regular basis for necessary action and compliance.*

All the important provisions of the aforesaid Act have been included in this policy and the same are being implemented. This policy and procedures are regularly reviewed to ensure its effectiveness. It is ensured that the person doing the review is different from the one who has framed this policy.

Annexure 1: Money Laundering Suspicion Report

Strictly Private & Confidential

To: Compliance Officer	From:	Date:

Client/Business Name	Transaction Date(s)
Client Account No(s)	Copies of Transactions & Account Details Attached Yes _____ No _____
Descriptions of Transaction(s)	
Source of Funds/ securities and Purpose of Transaction *(If you can, try to tactfully ask client)*	
Reasons why you think the transaction is suspicious *(Give as much detail as possible)*	
Signature of Staff	