Circular no.: MCX/COMP/488/2009 November 27, 2009

Anti Money Laundering and Know Your Customer (KYC) Norms

In terms of the provisions of Rules, Bye-Laws and Business Rules of the Exchange, the Members of the Exchange are notified as under:

Forward Markets Commission vide its letter no. 7/1/2008-MKT-II dated October 30, 2009 have directed Members/Intermediaries to follow and adopt the Prevention of Money Laundering Act 2002 and Prevention of Money laundering (Maintenance of records of the nature and value of transaction, the procedure and manner of maintaining and time for furnishing information and verification and maintenance of the identity of clients of the Banking companies, Financial Institutions and Intermediaries) Rules, 2005 and all other rules, regulations, notifications issued by the GOI from time to time.

The following framework as advised by Forward Markets Commission may be followed:

1. The Members/Intermediaries in the Commodity Derivative Market (CDM) shall have adequate controls and procedures in place so that they know the customers with whom they are dealing. Adequate and due diligence on new and existing customers is a key part of these controls. The standards adopted should be such that they adhere in letter and spirit to the requirements as listed out in detail by the Prevention of Money Laundering Act, 2002 (PMLA).

2. Appointment of Principal Officer:

The Members/ Intermediaries shall designate a senior management officer as Principal Officer. The Principal Officer shall be located at the head/corporate office and shall be responsible for monitoring and reporting of all transactions and sharing of information as required under the law. The Principal Officer will maintain close liaison with enforcement agencies, banks and any other institution which are involved in the fight against money laundering and combating financing of terrorism. The name, designation and addresses (including e-mail addresses) of the 'Principal Officer' may be intimated to the Office of the Director-FIU, 6th Floor, Hotel Samrat, Chanakyapuri, New Delhi – 110021, India on an immediate basis.

3. The Customer Due Diligence would include the following aspects:

a. Customer acceptance policy
b. Customer identification
c. Monitoring of transactions
d. Tracking and reporting suspicious transactions

a. Customer Acceptance Policy

3.1 The Members/Intermediaries should develop clear customer acceptance policies and procedures, including a description of the types of customers that are likely to pose a higher than normal risk to them. In preparing such policies factors such as customers' background, origin, public position, related accounts, business activities or other risk indicators should be considered. The Members/Intermediaries should develop graduated customer acceptance policies and procedures that require more extensive due diligence for higher risk customers. For example, the policies may require the fundamental account-

opening requirements for a working individual with a small CDM transaction. It is, however, important that the customer acceptance policy is not so restrictive that it results in a denial of access to the market participants, especially the targeted beneficiaries like farmers. On the other hand, quite extensive due diligence would be essential for an individual with a high net worth whose source of funds is unclear. Decisions to enter into business relationships with high risk customers, such as politically exposed persons, should be taken exclusively at senior management level.

b. Customer Identification

3.2 Customer identification is an essential element of KYC standards. A customer would include the person or entity that maintains an account with the member/intermediary or those on whose behalf an account is maintained (i.e., beneficial owners). The Member/Intermediary should undertake the following processes for proper identification of customers:

i) Identifying the customer and verifying that customer's identity using reliable, independent source documents;

ii) Identifying the beneficial owner, and taking reasonable measures to verify the identity of the beneficial owner such that the Member/Intermediary is satisfied that it knows who the beneficial owner is;

iii) In case of high value of transactions, obtaining information on the purpose and intended nature of the business relationship;

iv) Conducting ongoing due diligence on the business relationship and scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Members/Intermediaries knowledge of the customer, their business profile and risk profile, including, where necessary, the source of funds.

Indicative list of documents that may be obtained from the customers is enclosed at Annexure I.

3.3 It is felt that in some specific cases, the more rigorous identification procedures should be put in place. The following list is indicative, and the member/intermediary can have advanced process for the customer which it feels has high risk profile. Such high risk customers would include the following, but may not be restricted to depending on other customers having high risks associated to them:

- Companies having close family shareholdings or beneficial ownership
- Non-face-to-face clients
- Non resident clients
- High Networth clients,
- Trusts, Charities, NGOs and organizations receiving donations
- Politically exposed persons (PEP) of foreign origin
- 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 which are perceived to be sponsors of international terrorism, offshore financial centers, tax havens, countries where fraud is highly prevalent)
- Clients with dubious reputation as per public information available.

3.4 The above mentioned list is only illustrative and the Member/Intermediary should exercise independent judgment to ascertain whether new clients should be classified for more rigorous identification.

c. Monitoring of Transactions

3.5 The Member/Intermediary should put in place a mechanism to monitor the transactions being conducted through it, for ensuring effectiveness of the Anti Money Laundering procedures. For this, the Member/Intermediary should keep a tab on the transaction profile of the clients. This would help them in identifying the abnormal trade profile of the suspected clients.

3.6 The Member/Intermediary should pay attention to all complex, unusually large transactions / patterns which appear to have no financial or commercial justification. Very high account turnover, inconsistent with the size of the balance, may indicate that funds are being "routed / washed" through the account. Examples of suspicious activities can be very helpful to the member/intermediary and should be included as part of a jurisdiction's anti-money laundering procedures and/or guidance. The Member/Intermediary may also implement internal reporting mechanism and have threshold limits for each class of customers and pay special attention to the transaction which exceeds these limits.

3.7 The Member/Intermediary should ensure that a record of transactions is preserved and maintained **for a period of ten years** and that any transaction of suspicious nature is reported to the appropriate regulatory / other authority.

d. Tracking and Reporting Suspicious Transactions

3.8 It is emphasized that considering the sensitivity of the issue, the Suspicious transaction reporting should be taken up with utmost care and seriousness. The Members/Intermediaries should ensure to take appropriate steps to enable suspicious transactions be recorded. They should have appropriate internal procedures for reporting of suspicious transactions. Indicative list of circumstances / profile of the customer is indicated below to serve as a guidance to the Member/ Intermediary for recognizing them:

i) Clients whose verification is complex and not confirmed from other sources;
ii) Substantial increases in turnover without any reason;
iii) Large cash deposits made with the member/intermediary;

3.9 The suspicious transaction should be immediately notified to the Principal Officer or any other designated officer within the member/intermediary. The compliance cell of the member/intermediary should randomly examine a selection of transaction undertaken by clients to comment on their nature, i.e., whether they are suspicious transactions.

4. Reporting of Transaction to Financial Intelligence Unit-India

In terms of the PMLA rules, Members/Intermediaries are required to report information relating to cash and suspicious transactions to the Director, Financial Intelligence Unit-India (FIU-IND)

i. Cash Transaction Reports: The Prevention of Money-laundering Act, 2002, and rule thereunder require every member/intermediary to furnish to FIU-IND information relating to

- All cash transactions of the value of more than rupees ten lakhs or its equivalent in foreign currency;
- All series of cash transactions integrally connected to each other which have been valued below rupees ten lakhs or its equivalent in foreign currency where such series of transactions have taken place within a month;

The cash transaction report (CTR) (wherever applicable) for each month should be submitted to FIU-IND by 15th of the succeeding month as per the enclosed format at Appendix I.

Members may refer to our Circular No. MCX/COMP/401/2009 dated October 1, 2009 with respect to dealings in cash.

ii. Suspicious Transaction Reports: Every Member/Intermediary shall furnish to FIU-IND information of all suspicious transactions whether or not made in cash. Suspicious transaction means a transaction whether or not made in cash which, to a person acting in good faith –

- gives rise to a reasonable ground of suspicion that it may involve the proceeds of crime; or
- appears to be made in circumstances of unusual or unjustified complexity; or
- appears to have no economic rationale or bonafide purpose; or
- gives rise to a reasonable ground of suspicion that it may involve financing of the activities relating to terrorism.

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 as per enclosed Appendix II. 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.

Members/Intermediaries should carefully go through all the reporting requirements and formats given in the website of Financial Intelligence Unit, India – http//fiuindia.gov.in/

The related hardware and technical requirement for preparing reports in manual/electronic format, the related data files and data structures thereof are also given in the website. Members/Intermediaries, which are not in a position to immediately file electronic reports, may file manual reports to FIU-IND as per the formats prescribed.

The Principal Officer will be responsible for timely submission of CTR and STR to FIU-IND. 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.

The Principal Officer and other designated staff may visit the website of FIU – http:/fiuindia.gov.in/ for detailed guidelines and updates regarding the PMLA, 2002 and notifications issued from time to time.

Members/Intermediaries of the Exchange are hereby advised to ensure compliance with the above.

Parag Jain
Chief – Membership & Inspection

Encl: As above

Kindly contact Compliance Team on 022 – 66494090 or send an email at compliance@mcxindia.com for any clarification

---------- Corporate office ----------
Multi Commodity Exchange of India Limited
Exchange Square, CTS No. 255, Suren Road, Chakala, Andheri (East), Mumbai – 400 093
Tel.: 022 – 6649 4000 Fax: 022 – 6649 4151
www.mcxindia.com email: customersupport@mcxindia.com