Vogue Commercial Co. Ltd

Risk Management Policy

Monitoring of transaction is done with co-ordination of our Account Opening department, Accounts and Risk Management Department, Technical and Compliance Department.

All these department co-ordinate and watch the client activity and assign the limit to the clients and his risk profiling accordingly..

Risk based approach:- Classification of both the new and existing clients into high, medium or low risk category depending on parameters such as the customer's background, type of business relationship, transactions etc. Application of each of the client due diligence measures on a risk sensitive basis and adoption of an enhanced customer due diligence process for high risk categories of customers and vice-á-versa.

Limit Setting:- Limits shall be monitored on daily basis, taking following criteria's: Turnover, Exposure, past trends, Location, Deposit/Collateral.

Margins:- Margin must be collected on all derivative trades. Client level margin will be at management discretion in cash segment. Criteria to collect margin will be on the basis of volume of client and Past history of clients. Same client should not figure in default list in more than 5 days in a month

Trading:- Trading in illiquid scrip shall not be permitted. On detection of such trading, the risk manager shall use his discretion to shutdown the terminal after intimating branch manager and sub broker

Pay-in Of Fund & Stock: - Third party pay-in of securities & fund will not be accepted. Same way pay out of shares and fund will be directly done to client account only. No securities belonging to one client be used/transferred for Own purpose or for other client.

Collections: - Cash will not be accepted under any circumstances. Collection of cheques from clients must be done by T+2 days except clients who have authorized us to have running account balance.

Exposure: We shall not grant further exposure to the clients when debit balances arise out of client's failure to pay the required amount and such debit balances continues beyond the fifth trading day, as reckoned from date of pay-in. **(**Refer SEBI Circular CIR/HO/MIRSD/MIRSD2/CIR/P/2017/64**)**

Apart from this there is also proper system to generate, monitor and report the suspicious transaction report.

1. Generation of STR

We have adequate system to get STR files from NSDL/CDSL on fortnightly basis and we keep the log of the same for our records.

2. Monitoring of STR

Once we received the STR files we check and verify the details of each and every client with the records available with us in respect of bank account and volume of transactions by means of their financial capabilities.

For monitoring the large volumes done by the clients we at the end of day scrutinize and analyze the volumes of each and every client with the help of trial balance of the particular trade date and assess his financial capabilities based on the financial information provided by them to us. If there is any discrepancy found then we call the client and take the reasons and source of funds for these trades for our satisfaction.

3. Reporting of STR

As we verify the STR in detail and same is found not suspicious and hence ‘NIL’ record is kept by us and there is no need to report the same to FIU-India.

.ORGANIZATION ACCESS POLICY

Organization Access Policy/Password Policy: At the time of account opening, all the clients are allocated a unique client code and the same is intimated to them via email with specific instructions. The password of the client gets generated from the system and is printed on a discrete stationary. The usage of discrete stationary ensures that the password cannot be compromised in transit and is sent only at clients designated address.

The password gets stored in the application database in encrypted form so that even the administrators of the system cannot view it. Nobody has the access rights to change the password except based on client's request to regenerate the same.

When the client logs in for the first time, he is forced to change the password.

Following password guidelines have been implemented in the system

- Client ID and password should not be same
- The new password should not be same as the old password
- Password must be at least 8 characters and a maximum of 12 characters
- Password should not be all alphabets or all numbers and should contain a mix of alphabets (a-z/A-Z), numbers (0-9) and at least one special character
- Password should not contain white spaces
- Password should not be same as last three passwords¬ Transaction password should not be same as the Login password
- Password will automatically expire after 90 calendar days
- Two factor authentication

A client logging into the system is forced to change his or her password if it has expired before he or she is allowed to do any activity in the account.

For Vogue Commercial Co. Ltd

Director