Market Abuse

Market abuse can be classified into two categories, insider dealing or market manipulation.

1. Insider dealing/trading is trading or the attempt to trade on a public company's stock based on information of a precise nature that has not been made public. If it were made public, it would be likely to affect the price of financial instruments.

2. Market Manipulation is the deliberate attempt to interfere with the free and fair operation of the market including creating false or misleading appearances with respect to the price of, or market for, a product, security or commodity.

FIs must have safeguards in place to identify and reduce the risk of market abuse. Key preventative measures FIs can establish for Market Abuse and Insider Trading include:

- Risk Assessments to identify areas of the businesses / departments more vulnerable to Market Abuse/Insider Trading;

- Policies outlining definitions, regulations, red flags, due diligence measures, incident reporting, consequences for breaches, record keeping;

- Training & Awareness;

- Whistleblowing;

- Security controls: segregation of duties, data mining, employee checks, authorisation limits, IT controls (user restrictions, email monitoring, IT surveillance); Director supervision.

Data Security & Cyber-Crime

Data security is the process of protecting data from unauthorized access and data corruption. Cyber-crime refers to the act of obtaining financial gain through criminal activities, including identify fraud, ransomware attacks, email and internet fraud, and attempts to steal financial account information, credit card, or other payment card information. Financial institutions collect and store vast amounts of customer information

and any data breach could have serious implications for the business.

Key preventative measures FIs can establish for data security & cybercrime include:

- Designing and implementing policies and procedures to safeguard customer and any third-party information;
- Clear communications and training of employees to protect sensitive information;
- Reviewing and managing third-party handling of customer information and ensuring adequate protection;
- Monitor access to personally identifiable information of customers;
- Designing and implementing an effective incident response plan.