Fraud Policy

Introduction

Fraud is the act of obtaining by deception money or assets belonging to another which will benefit the fraudster and expose the victim to a loss. Fraud may be committed against individuals and firms, for example, through:

- The use of false or stolen identities to defraud financial services organisations; or
- The use of the internet, for example, the setting up of websites purporting to belong to a reputable institution.

The FCA requires firms to take reasonable care to establish and maintain effective systems and controls for countering the risk that the firm might be used to further financial crime.

Preventing Fraud

Makor has adopted policies and procedures to detect and respond to fraud in a timely and effective manner. All staff are required to fully co-operate with any investigations and ensure that they adhere to Makors policies and procedures at all times.

There are numerous ways Makor protects itself against fraud, which include:

1. Established and clear reporting lines;
2. Regular analysis of risks;
3. Appropriate internal procedures covering all areas of the business;
4. Segregation of duties;
5. Employment screening;

6. Taping and monitoring of phone calls;
7. Staff training;
8. Compliance monitoring programme;
9. Detailed KYC processes; and
10. IT security measures.

The above bullet points are expanded on further in other sections of this Manual.

All staff should be aware of the key indicators of fraud listed below.

1. Increased levels of stress without a high workload;
2. Lifestyle not commensurate with salary;
3. Reluctance to take annual leave;
4. Results 'too good to be true';
5. Reported and forecast figures the same or similar; and
6. Complex or unique business arrangements.

It should be noted that no single or multiple indicators necessarily mean an individual is involved in fraud, but should be considered in conjunction with any suspicious behaviour.

It is the responsibility of every employee to take an active role in the prevention of fraud. Makor has set out policies and procedures below to assist you in helping to prevent fraud. In addition, training will be provided both initially and on an annual basis.

Policies and Procedures

All staff members must report any concerns or suspicions of actual, attempted or suspected fraud to the Fraud Prevention Officer ("FPO")[1]. The FPO will verify and investigate fraud in accordance with Makor's Fraud Response Plan, escalating any concerns to senior management, if appropriate. All discussions with the FPO will be kept confidential.

It is important that you do not discuss your concerns or suspicions with anyone other than the FPO, regardless of their seniority. The **only** exception is if your concerns relate to the FPO, in these circumstances you should discuss your concerns with a senior Director.

Fraud Response Plan

In determining whether to launch a full investigation into the suspected fraud, the FPO will consider:

1. The evidence readily available (i.e. That which can be collected without alerting the

[1] The FPO should be an individual with sufficient authority to carry out this role effectively. This will generally be an individual specifically recruited for the role, the Money Laundering Reporting Officer, the Compliance Officer or a Director.

individual/s that he/she is being investigated);

2. Any potential motives the individual/s may have;
3. The type and size of the suspected fraud;
4. The risk to the business; and
5. The individual/s' access to sensitive information and/or systems and controls.

If the FPO is satisfied that there are reasonable grounds to suspect fraud, a fraud committee will be established. The FPO will lead the investigation and involve senior people from different teams (e.g. Compliance, legal, HR, IT, audit, security), as appropriate and on a need to know basis.

The type of investigation will be largely dependent on the type of suspected fraud (e.g. Expenses fraud, payroll fraud, target manipulation, funds diversion, data theft and asset theft), but is likely to include:

1. Establishing a list of evidence to be gathered and task staff with the delivery by a certain date;
2. Restricting the suspected individual/s' access to e-mails, systems and controls, and sensitive information;
3. Suspending the suspected individual/s with pay during the investigation;
4. Securing evidence;
5. Conducting formal interviews with relevant staff members; and
6. Identifying and targeting any areas of weakness.

It is important that HR are fully involved throughout the investigation and consulted before any action is taken. The FPO should also inform Makor's professional indemnity insurers, consult clients and hold internal discussions with staff members.

A report from the fraud committee should be presented to the board, outlining the findings of the investigation and any systemic areas of weakness. If there is evidence of fraud, Makor should obtain legal advice before proceeding with any action against the individual/s involved.

Where the report highlights any systemic areas of weakness, measures should be immediately adopted to strengthen these controls.

Examples of Potential Fraudulent Activities

Potential Fraudulent Activities	Mitigating Factors
Misreporting Only reporting the most favourable possible results or not providing complete results, with the aim to increase the assets under management in the fund and therefore the fund manager's remuneration.	Ensure all published information has been properly verified.
Insider trading – including front running This involves trading stock based on non-public information.	Ensure all members of staff are aware of Makor's market abuse policies and procedures, and have received training. Keep insider and restricted lists up to date.
Internet Fraud – 'Pump and Dump' This involves disseminating false and/or fraudulent information in chat rooms, forums, internet boards and via e-mail (generally spamming), with the purpose of driving up the share price in thinly traded stocks. When the price reaches a certain level, the individuals sell off their holdings realising a substantial profit before the stock price falls.	Restrict and/or monitor internet access to forums and chat rooms. Monitor personal account dealing logs for suspicious transactions.
Late trading This involves placing trades after the close of the market, as if they had been placed before the close of the market. This may be done to take advantage of information which has been released after the market has closed which would affect the share price of a particular stock.	Monitor trading activity to ensure that trading takes place within market hours. Any trading outside these hours should be checked against market release or the opening share price on the next business day.
Market timing This involves allowing some investors to trade more than the fund prospectus allows, raising the administrative costs for all investors in the fund.	Monitor funds for any unusual administrative costs.

'Names later' basis This involves an order placed with a broker on the basis that the names will be provided later. If the price of the stock goes in a favourable direction, the trade becomes a personal account or favoured fund transaction. If the stock goes in an unfavourable direction, it becomes a fund transaction.	Ensure all staff members obtain permission before being allowed to trade on their personal account. If they do not trade, ensure explanations are sought and records are monitored for any suspicious patterns.
Salami slicing / penny shaving This involves taking advantage of rounding to the nearest pence (or other currency) in financial transactions. These roundings are placed in another account and, due to the insignificant size, go undetected.	Monitor accounts and conduct periodic checks of transactions to ensure no money is diverted into a separate account.
Target Manipulation Falsifying performance results to hit targets.	Check performance results against verifiable data.
Payroll Fraud This may involve 'ghost employees' (entries on a payroll register which do not relate to employees of Makor), false or inflated expenses and false timesheets.	Monitor payroll entries on a regular basis to ensure only actual staff members are listed. Ensure receipts are obtained for any expenses and timesheets are completed on a regular basis.
Money Laundering This involves concealing the true origin and ownership of the proceeds of crime.	Staff members should certify that they have read, understood and will comply with Makor's anti-money laundering policy and have received annual training.
Kickbacks This may involve directing trades to a particular broker for a percentage of the brokerage commission (a "kickback").	Makor should review transactions and ensure Best Execution is obtained on every transaction and the commission on brokerage accounts.