Chapter 8

Insider dealing and market manipulation

8.2 Themes

Governance

8.2.1 G The guidance in ■ FCG 2.2.1G above on governance in relation to financial crime also applies to insider dealing and market manipulation.

We expect senior management to take responsibility for the firm's measures in relation to insider dealing and market manipulation. This includes:

- Understanding the risks of insider dealing or market manipulation that their firm is exposed to (both through employee and client activity).

- Establishing adequate policies and procedures to counter the risk that their firm is used to further these offences in accordance with ■ SYSC 6.1.1R.

Senior management should also be aware and manage the potential conflict of interest which may arise from the firm's focus on revenue generation versus its obligation to counter the risk of the firm being used to further financial crime.

Self-assessment questions:

- Does the firm's senior management team understand the legal definitions of insider dealing and market manipulation, and the ways in which the firm may be exposed to the risk of these crimes?

- Does the firm's senior management team regularly receive management information in relation to suspected insider dealing or market manipulation?

- How does senior management make sure that the firm's systems and controls for detecting insider dealing and market manipulation are robust? How do they set the tone from the top?

- How does the firm's MLRO interact with the individual/departments responsible for order and trade surveillance/monitoring?

- How does senior management make decisions in relation to concerns about potential insider dealing or market manipulation raised to them by Compliance or another function? Do they act appropriately to mitigate these risks?

- How does senior management make sure that its employees have the appropriate training to identify potential insider dealing and market manipulation?

Examples of good practice	Examples of poor practice
• Senior management are able to recognise and articulate the warning signs that insider dealing and market manipulation might be taking place.	• There is little evidence that possible insider dealing or market manipulation is taken seriously by senior management. Addressing these risks is seen as a legal or regulatory necessity rather than a matter of true concern for the business.
• Senior management regularly receive management information in relation to any possible insider dealing or market manipulation that occurs.	• Senior management considers revenue above obligations to counter financial crime.
• The individual(s) responsible for overseeing the firm's monitoring for suspected insider dealing and market manipulation has regular interaction and shares relevant information with the MLRO.	• Senior management considers the firm's financial crime obligations are fulfilled solely by submitting a STOR and/or SAR.
• Senior management appropriately supports decisions proposed by Compliance.	• The Compliance function has limited independence and the first line can block concerns from being escalated.

Risk assessment

8.2.2 G The guidance in ■ FCG 2.2.4G above on risk assessment in relation to financial crime also applies to insider dealing and market manipulation.

Firms should assess and regularly review the risk that they may be used to facilitate insider dealing or market manipulation. A number of factors should be incorporated into this assessment, including the client types, products, instruments and services offered/ provided by the firm. Firms' assessments should also consider the risk which employees may pose too.

Firms should consider how their policies and procedures seek to mitigate the financial crime risks they have identified. This could include, but is not limited to:

- undertaking enhanced order and transaction monitoring on clients or employees,
- setting client specific pre-trade limits, and
- ultimately declining business or terminating client or employee relationships if appropriate (see ■ FCG 8.2.3 for more detail).

Self-assessment questions:

- Has the firm considered whether any of the products/services it offers, or the clients it has, pose a greater risk that the firm might be used to facilitate insider dealing or market manipulation? How has the firm determined this?

•Who is responsible for carrying out the risk assessment and keeping it up to date? Do they have sufficient levels of expertise (including markets and financial crime knowledge) and seniority?

What framework does the firm have in place for assessing the risk of insider dealing and market manipulation being committed by its employees?

•How does the firm use its risk assessment when deciding which business to accept?

•How often is the risk framework reviewed and who approves it? • How does the firm's risk framework for countering the risk of insider dealing and market manipulation interact with the firm's AML risk framework? Are the risk assessments aligned?

Examples of good practice	Examples of poor practice
• Insider dealing and market manipulation risks are assessed across every asset class to which the criminal regimes of insider dealing and market manipulation apply, and across all client types with which the firm operates.	• Risk assessments are generic, and not based upon the firm's own observations.
• There is evidence that the firm's risk assessment informs the design of its surveillance controls.	• An inappropriate risk classification system makes it almost impossible for a client relationship to be considered 'high risk'.
• The firm identifies and uses all information at its disposal to make informed judgments about the level of financial crime risk posed to its business.	• The firm fails to consider the risks associated with employees using discretionary accounts to commit insider trading or market manipulation.
• The firm's risk framework is regularly tested and reviewed.	• Risk assessments are inappropriately influenced by profitability of new or existing relationships.
• Where a firm identifies a risk that it may be used to facilitate insider dealing or market manipulation, it takes appropriate steps to mitigate that risk.	• The firm submits a significant number of SARs and/or STORs on a particular client, but continues to service that client without considering its obligation to counter the risk of furthering financial crime.
• The firm considers where relationship managers might become too close to customers to take an objective view of risk, and manages that risk effectively.	• The firm fails to consider additional account information it has access to, such as Power of Attorney arrangements, when designing its surveillance controls.

Policies and procedures

8.2.3 G The guidance in ■ FCG 2.2.5G above on policies and procedures in relation to financial crime also apply.

Firms' policies and procedures should include steps designed to counter the risk of insider dealing and market manipulation occurring through the firm. Policies and procedures should be aligned and make reference to the firm's insider dealing and market manipulation risk assessment.

Firms should ensure that their policies and procedures cover both:

(1) identifying and taking steps to counter the risk of financial crime before any trade is executed, and

(2) mitigating future risks posed by clients or employees who have already been identified as having traded suspiciously.

Firms should make sure that front office employees are aware of the firm's policies and procedures with regard to countering the risk that the firm is used to further financial crime. Among other things, these should reflect the *FCA's* expectation that market participants do not knowingly or intentionally aid, abet, counsel or procure the commission of a criminal offence (insider dealing or market manipulation). Therefore, where the firm holds information which leads to the conclusion that its employee or client is seeking to trade either manipulatively or on the basis of inside information, it should refuse to execute the trade where it is able to do so.

Firms' policies and procedures should state clearly how they identify and monitor employees' trading, in addition to their clients' trading. ■ COBS 11.7 requires firms that conduct designated investment business to have a personal account dealing (PAD) policy. Appropriately designed PAD policies can:

•counter the risk that employees of the firm commit financial crime themselves,

•make sure that conflicts of interest that might result in employees not escalating suspicious activity are avoided. For example, if employees are allowed to copy clients' trades on their own accounts, they may be less inclined to escalate financial crime concerns that only become apparent post-trade, as, by reporting the client they would, by implication, be reporting their own trading as suspicious.

Policies and procedures relevant to each business area, including front office functions, should be communicated and embedded.

Self-assessment questions:

•Does the policy define how the firm will counter the risk of being used to facilitate insider dealing and market manipulation? For example, in what circumstances would the firm conduct enhanced monitoring or stop providing trading access to a particular client or employee?

•Does the firm have established procedures for following up and reviewing possibly suspicious behaviour?

•Do front office staff understand how insider dealing and market manipulation might be committed through the firm, to escalate potentially suspicious activity when appropriate, and challenge client or employee orders (where relevant), if they believe the activity will amount to financial crime? Does the firm have effective

whistleblowing arrangements in place to support appropriate financial crime detection and reporting?

Examples of good practice	Examples of poor practice
• The firm has clear and unambiguous expectations for its employees and anyone acting on its behalf, such as introducing brokers.	• The firm's policies and procedures aren't updated for legal or regulatory changes.
• Employees in dealing roles understand and are able to identify potentially illegal conduct, and their trading is regularly monitored by Compliance.	• Policies and procedures are generic and don't consider the specific processes or risks of the firm.
• The policies and procedures make adequate reference to the firm's risk assessment.	• Policies and procedures cover only post-trade identification and reporting of suspicious activity and do not cover countering the risk of financial crime.
• Policies and procedures make sure that the risk of financial crime is considered throughout the lifecycle of a security transaction, including before the order has been executed.	• The firm sets apparently robust procedures for assessing and mitigating identified financial crime risk, but sets thresholds for engaging these measures which mean that they are almost impossible to trigger.
• Where the financial intermediary is aware that a client is intending to trade on the basis of inside information or manipulate the market, the firm refuses to execute the order(s).	• The firm doesn't have policies detailing the circumstances when it will consider rejecting a prospective client or terminating an existing client relationship.
• The firm takes swift, robust action for breaches of its policies and procedures.	• The firm doesn't have appropriate policies or procedures in place regarding personal account dealing, so that staff are able to deal in a manner which creates conflict in escalating suspected market abuse.
• The firm's policies and procedures include controls designed to counter the risk of financial crime being committed by employees, for example wall crossings, restricted lists and personal account dealing restrictions.	

Ongoing monitoring

8.2.4 G We recognise that the *Market Abuse Regulation* already imposes monitoring requirements on persons professionally arranging or executing transactions, in order to detect and report suspicious orders and transactions in the form of STORs (as well as imposing similar monitoring obligations on market

operators and investment firms that operate a trading venue). It may be appropriate to use the results of this monitoring for the purpose of countering financial crime.

Firms should note that the markets and instruments to which the criminal offences of insider dealing and market manipulation apply are different to those covered by the *Market Abuse Regulation*. Firms should therefore assess whether their arrangements to detect and report market abuse can be appropriately relied on to monitor for potential insider dealing and market manipulation.

For their risk assessments, firms should regularly take steps to consider whether their employees and/or clients may be conducting insider dealing or market manipulation. This could be achieved by transaction, order and communications surveillance, with consideration given to the employee's or client's usual trading behaviour and/or strategies, and in respect of clients: initial on-boarding checks and ongoing due diligence, or other methods.

Firms should consider the risks that arise in scenarios whereby their client is not the decision maker behind the activity taking place, with orders and trades being instructed by an underlying client. In this scenario, where a firm is concerned either about a particular client or trade, firms should consider the steps they could take to gain further information, or an understanding, of the client, underlying client and/or activity. The firm may wish to engage with its client to obtain further information about the trading in question and/or the nature of the underlying client(s).

If a firm is, based on their understanding of a client and monitoring of that client's transactions, suspicious that a client might have committed or attempted to commit insider dealing or market manipulation, the firm should comply with its obligations to report those suspicions via a STOR and/or SAR (where appropriate). In addition, it may be appropriate for the firm to document the options available to it to counter the risk of any ongoing financial crime posed by its ongoing relationship with that client, and when these options should be considered.

In addition, a firm must also submit a STOR where it identifies suspicious trading by an employee. The nominated officer of the firm would also be required to report any knowledge or suspicions of money laundering or terrorist financing arising from trade by submitting a SAR to the NCA. Again, the firm's policies and procedures should document the options available to it to counter the risk of any ongoing financial crime related to employee trading activity, and when these options should be considered.

Options available to firms to counter the risk of being used to further financial crime by its clients and/or employees could include:

- Carrying out enhanced due diligence on a client and enhanced monitoring of a client's or employee's trading activity.
- Restricting the client's access to particular markets or instruments.
- Restricting services provided to the client (eg direct market access).
- Restricting the amount of leverage the firm is willing to provide to the client.
- Taking disciplinary action against an employee.
- Ultimately terminating the client or employee relationship. The appropriate response will depend on the outcome of the firm's

monitoring procedures and the extent and nature of any suspicious activity identified.

Self-assessment questions:

•Does the firm consider its obligations to counter financial crime when a client's or employee's activity is determined as suspicious via surveillance systems and subsequent investigation?

•How do the firm's monitoring arrangements interact with the client-on-boarding process / AML framework?

•Does the firm undertake enhanced monitoring for high risk clients?

•Does the firm's monitoring cover the activity of any employee trading?

•In instances where a firm is concerned about a client which is not the individual or entity who is making the decision to trade, has the firm considered information it has access to, or ways it can gain information, to allow it to counter the risk of being used to further financial crime?

Examples of good practice	Examples of poor practice
• The firm's monitoring seeks to identify trends in clients' or employee's behaviour, in addition to one off events.	• The firm believes that its obligations cease when it reports the suspicious transactions and orders.
• The firm undertakes enhanced monitoring of clients it has determined are high risk.	• Suspicious transactions and orders are identified but not investigated further.
• The firm conducts regular, targeted monitoring of voice and electronic communications.	• Monitoring identifies individual suspicious events but does not attempt to identify patterns of suspicious behaviour by the same client or a group of clients, using, for example, historical assessments of potentially suspicious activity or STORs submitted.
• Front office employees escalate suspicious activity promptly to Compliance.	• The firm does not consider engaging with its clients, whether to understand their trading activity or the activity of their underlying client(s).
• The firm takes additional steps to understand and ensure it is comfortable with the rationale behind the trading strategies employed by its client(s) and/or staff.	• The firm does not use information obtained via monitoring and subsequent investigation to consider the suitability of retaining a client relationship.
• The firm conducts regular monitoring of its employee	• In instances when a client is placing orders on behalf of its

Examples of good practice	Examples of poor practice
trading activity, whether personal account dealing or trading on behalf of the firm or clients.	underlying clients, the firm fails to make use of information which could allow it to understand the nature and potential risk of their client (for example, number of underlying clients, trading strategies, the nature of their business).
• In instances when a client is placing orders on behalf of its underlying clients, the firm engages with their client to establish whether they maintain appropriate systems and controls for countering the risk of being used to further financial crime.	
• The firm considers a client or employee's ongoing risk of committing insider dealing or market manipulation following the submission of a STOR and/or SAR.	