FINANCIAL CONDUCT AUTHORITY

Market Watch

Newsletter on market conduct and transaction reporting issues

August 2019

Contents

If you wish to join our email list to receive future editions, please contact us at market.watch@fca.org.uk

You can also find issues on our website at: www.fca.org.uk/firms/markets/market-abuse

Introduction

In this edition, we share our concerns and findings about control of access to inside information. This follows the conviction of Fabiana Abdel-Malek, a former Compliance officer in the London branch of a major investment bank. We also highlight our recent thematic review of money laundering risks in capital markets.

Controlling access to inside information

Ms Abdel-Malek was found guilty of 5 counts of insider dealing under Section 52(2)(b) of the Criminal Justice Act 1993.

While Ms Abdel-Malek was named on the relevant insider lists, she had no business need to access the information concerned.

Under Section 52(2)(b) of the Criminal Justice Act 1993:

> *An individual who has information as an insider is also guilty of insider dealing if –*
>
> *he discloses the information, otherwise than in the proper performance of the functions of his employment, office or profession, to another person.*

That such behaviour amounts to unlawful disclosure is echoed at Article 10 (1) of the Market Abuse Regulation.

Ms Abdel-Malek abused her position of trust by repeatedly accessing electronic compliance systems containing inside information about several, as then non-public, price-sensitive corporate transactions. She then passed that information to a private individual and not an employee of the bank, who used it to trade CFDs on the relevant securities.

Why this matters to firms

By allowing widespread and unchallenged access to individuals who do not require the inside information to do their job, firms increase the risk of that information being disclosed unlawfully. Firms also risk being caught up in unlawful disclosure and insider dealing investigations. They may expose themselves to regulatory action and significant reputational risk.

In a speech in February 2019, we highlighted the importance of firms being able to identify conduct risks to ensure they have effective market abuse controls in place. We also emphasised that systems and controls to manage how inside information is communicated outside a firm are as important as having in place effective controls to manage that information within the firm.

This sits within Questions 1 and 3 of our 5 Conduct Questions, which ask:

> *What proactive steps do you take as a firm to identify the conduct risks inherent within your business?*

and

> *What support (broadly defined) does the firm put in place to enable those who work for it to improve the conduct of their business or function?*

Insider lists and access to inside information

The Market Abuse Regulation (MAR) states:

> *1. Issuers or any person acting on their behalf or on their account, shall:*
>
> *(a) draw up a list of all persons who have access to inside information and who are working for them under a contract of employment, or otherwise performing tasks through which they have access to inside information, such as advisers, accountants or credit rating agencies (insider list); (Article 18.1.a)*

When investigating suspected insider dealing, it is crucial that we establish who had access to inside information at particular points in time. However, when conducting investigations and reviews we frequently encounter:

- Insider lists omitting the names of people who were provided with or who had access to inside information.
- Evidence of individuals not named on relevant insider lists accessing inside information.

These issues hinder our investigations.

Findings of FCA review

We published the results of a Thematic Review of the processes investment banks have in place to control flows of confidential and inside information (TR15/13) in December 2015. Market Watch 58 describes the results of our high-level review of the industry's implementation of MAR.

Recently we reviewed the systems and controls used by a sample of investment banks, legal advisers and other consultancies to manage access to inside information. Our findings included:

- Instances of large numbers of support staff having access to documents containing inside information. One insider list suggested that only 12 deal team members worked on the transaction, but that over 600 members of Compliance, Risk and other support functions also had full access to inside information about the deal. Similarly, some insiders at some firms are being classified as 'permanent insiders' and have routine access to all inside information without obvious reason.
- Failures to restrict access to inside information to those who need it for the proper fulfilment of their role. For example, support staff having the same access rights to inside information as the deal team, regardless of the differing needs of those roles. However, some firms took reasonable steps, such as granting IT staff access only to anonymised or code-named folders for maintenance or permission purposes, (so not to files within those folders).
- An absence of regular reviews of access rights. This resulted in access not being terminated after staff changed roles or transferred from projects.
- Insider lists containing very generic descriptions of the functions of non-deal team staff, for example 'Support Function', or 'Other Support Function'. We question whether non-descriptive titles provide enough information for firms to track and control how inside information is communicated, and whether a valid business 'need to know' is being imposed. Firms should consider whether such descriptions meet the MAR requirement that insider lists should include 'the reason for including that person in the insider list' (Article 18 (3) (b)).
- Insider lists including individuals who did not have access to inside information, rendering them not fit for purpose.
- Electronic files containing deal specific inside information stored in general team folders, accessible by (and in some cases, accessed by) front-office staff not working on the deal and not on the insider list.
- Non-deal team staff in multiple jurisdictions having access to inside information, where some of those jurisdictions had no connection to the transaction. We have not explored control requirements within these jurisdictions. Firms may wish to consider the degree to which such access meets their risk appetites and whether there is a 'need to know'.
- We observed differing levels and methods of monitoring by firms:
  - In some firms, there was a complete absence of any monitoring.
  - Some firms' monitoring did not give enough detail on who had accessed inside information.
  - Some firms monitored for repeated access to large numbers of documents, or access outside normal working hours by permissioned individuals, as well as attempted access by non-permissioned staff and from non-permissioned devices.
  - In some firms, responsibility for monitoring rested with dedicated staff within

Compliance, who had a clear understanding of the need to control access to inside information. In others, monitoring was conducted by more generalised support staff.

- Some firms were able to provide comprehensive audit trails of access, including instances of 'read only' access. Others were able to evidence only when documents had been created, edited or deleted. A small number of firms were unable to provide any logs of access to inside information at all.
- In compiling responses to our questions, some firms identified inaccuracies in several insider lists previously supplied in response to regulatory requests. These included discrepancies between those lists and records of who was actually given permission to access the relevant inside information. This suggests that the accuracy of insider lists offers significant room for improvement.

Summary and key recommendations

We view an inability to respond to a regulatory request with accurate records of who had access to inside information, as an indication of underlying weaknesses in systems, procedures and policies. By allowing widespread and unchallenged access to inside information to individuals who do not require it to perform the proper functions of their employment, firms increase the risk of that information being disclosed unlawfully. In addition, if firms cannot respond appropriately to FCA requests, they may be subject to further regulatory scrutiny.

We expect firms to take reasonable steps to ensure that the risks of handling inside information are identified and appropriately mitigated. The Abdel-Malek case is an example of the risks of non-deal team staff being granted access to inside information not being identified and appropriately mitigated, leading to criminal activity.

Understanding the money laundering risks in the capital markets – thematic review publication

In June, we published our thematic review 'Understanding the money laundering risks in the capital markets' (TR19/4). The report concludes that capital markets firms need to do more to fully understand their exposure to money laundering risk. It notes that participants had often not considered that some market abuse suspicions could also indicate money laundering.

The report contains an Annex of typologies, demonstrating how money might be laundered through the capital markets. We expect firms to consider their approaches to identifying and assessing money laundering risk in light of the report and Annex.