



### 1) Principles of good practice for handling inside information

In Market Watch 21 we signalled our desire to consider ways to share the good practice points with firms we do not regulate. The development of a set of Principles of Good Practice ('the Principles') was a major part of the work during this phase of the project. An industry Working Group was formed to address the subject and was comprised of market practitioners and relevant representative bodies - namely the CBI, PRCA, LIBA, ICAEW, Imprima Group, Bowne International, RR Donnelley, Merrill Corporation and the CLLS. FSA acted as facilitator for the Working Group. The Working Group was asked to consider how best to heighten awareness with the non regulated community, with a particular focus on the areas that had been identified in Market Watch 21 as requiring most attention.

The Working Group considered that the following framework was important for the work:

- 1) The purpose of any published material should be clear:
  - a. It is not a replacement for existing rules and regulations, e.g. The Criminal Justice Act 1993, the takeover Code, The Listing Rules or the Code of Market Conduct.
  - b. The principles were not drafted with a view to becoming adopted as legally binding terms in contracts.
  - c. It is not FSA regulation of firms outside its regime.
  - d. It should be voluntary.
  - e. Its one main objective is that any published material helps contribute to an overall heightened awareness by non regulated firms of the ways to protect sensitive information.
- 2) Published material should not be prescriptive but principles based, with firms able to adapt it to their particular circumstances (where detailed good practice points are highlighted it should be clear that these are simply examples in place at some firms and are not necessarily suitable for all firms).
- 3) Firms should only be responsible for their own systems and controls.

The Working Group has produced a document, which is attached to this article. Some of the Working Group will also host the document on their websites. While we fully support it, the document is not an FSA document and we will not be assessing firms' compliance against it. The main aim is that the work contributes to an overall heightened awareness of the ways to protect sensitive information.

The document contains six principles covering the following:

- policies and procedures;
- awareness and training;
- 'need to know' and other information controls;
- passing price sensitive information to third parties;
- Information Technology security; and
- personal dealing policies.

Practical examples of good practice are then provided in the annex to the Principles.

The Principles are voluntary to adopt and are broad based. While they are aimed at the unregulated community, aspects of them could also provide assistance to other market participants.

In addition to those directly involved in the drafting, a wide range of other stakeholders have also voiced their support for the work. These entities are listed in the Principles document. We are extremely pleased with the high quality output from the Working Group and are delighted that so many market participants have pledged their support to assist in the work to reduce leaks of sensitive M&A information.

As signalled in Market Watch 21, we envisage that the firms we regulate which are appointed as advisers to M&A deals will play a role as facilitators of the Principles, seeking to bring them to the attention of those that engage them and other third parties then engaged in that deal who are not regulated by their own professional bodies. We, of course, recognise that making firms aware of the Principles is just one way of helping to educate market participants about their responsibilities.

The Working Group will consider whether any review of the Principles of Good Practice is necessary in 18 months time.

### **Contact Details**

This newsletter is produced regularly by the Market Conduct and Transaction Monitoring teams in our Markets Division. If you would like to receive this newsletter by email, or have any comments on it, please contact [market.watch@fsa.gov.uk](mailto:market.watch@fsa.gov.uk)

**Market Abuse Helpline:** 020 7066 4900 & [market.abuse@fsa.gov.uk](mailto:market.abuse@fsa.gov.uk)

**Transaction Monitoring Helpline:** 020 7066 6040 & [tmu@fsa.gov.uk](mailto:tmu@fsa.gov.uk)

## **PRINCIPLES OF GOOD PRACTICE FOR THE HANDLING OF INSIDE INFORMATION**

There is a widespread desire amongst those involved in capital markets to support efforts to eliminate misuse of inside information. Concerns remain that inside information from time to time leaks into the market, whether accidentally or intentionally, and may be misused: this is a particular issue in relation to inside information about mergers and acquisitions. Misuse of inside information is a financial crime carrying significant penalties, including imprisonment.

Those organisations involved in capital markets which are subject to direct regulation by FSA or other regulators, or are subject to the Disclosure and Transparency Rules (DTRs), should already have in place policies and procedures on dealing with inside information. However others, such as unregulated service providers and some other market participants, may not.

In light of this it was thought timely to highlight the need for unregulated participants to consider policies and procedures for handling inside information. Accordingly, to raise awareness of the importance of combating market abuse and to assist the market with developing and maintaining good practices in the handling and control of inside information, the FSA has sponsored an industry led working party made up of representatives of regulated and unregulated participants including the CBI, PRCA, LIBA, ICAEW, Imprima Group, Bowne International, RR Donnelley, Merrill Corporation and the CLLS.

The publication of this document is also supported by the QCA, ABI, BBA, the LSE and the Executive of the Takeover Panel, which in March 2008 published Practice Statement No.201 which contains more information about the need for secrecy in takeovers and the specific rules of the Takeover Code relating to secrecy and announcements. The SRA has also issued a statement expressing its support for the objectives behind the publication of the Principles and reminding solicitors of their relevant professional duties in respect of confidential information and managing risk.

This document has been developed for those in the unregulated community involved in handling inside information, in order to set out general principles on which they can then develop their own policies and practices, as best suits their particular businesses. It is intended that this approach should support the idea that each organisation accepts responsibility for its own conduct rather than relying on others. The annex includes examples that give a practical context to the principles and highlight good practice points. Whilst the principles and good practice points are aimed at the unregulated community, aspects of them could also provide assistance to other market participants.

### **The Principles**

#### **1. Policies and procedures**

Policies and procedures for the use and control of inside information should be established and reviewed from time to time. These should recognise the responsibility to control access to inside information and reduce risk of misuse. There should be clear responsibility within organisations for overseeing controls and procedures in relation to inside information.

#### **2. Awareness and training**

Appropriate measures should be taken, including training, to assist staff in understanding the importance of keeping information secret and the implications of improper disclosure – including the

potential civil and criminal liabilities for the firm and the individual. Ensuring policies are capable of being readily understood by all relevant staff is an important part of this approach.

### **3. "Need to know" and other information controls**

Reasonable steps should be taken to limit the number of those with access to inside information. Where practicable a "need to know" policy should be applied.

### **4. Passing price sensitive information to third parties**

Reasonable care should be taken to ensure that where inside information is provided to a third party, the third party is aware of its obligations in relation to the use and control of the information.

### **5. Information technology security**

Appropriate consideration should be given to the security of and access to inside information on IT systems, including the implementation of controls to limit access.

### **6. Personal dealing policies**

Reasonable consideration should be given to establishing personal account dealing policies; those policies should be made clear to staff along with the civil and criminal penalties for dealing on the basis of inside information or for enabling such dealing.

The principles and the practice suggestions in the annex are not a substitute for the relevant laws and regulations nor are they intended to have any legal effect or to be used by the FSA or other regulators: their objective is simply to help raise standards generally in relation to the use and control of inside information.

### **Annex to the "Principles of good practice"**

The Financial Services and Markets Act (s. 118 FSMA) defines inside information as "*information relating to particular securities or to a particular issuer or issuers of securities which has not been made public and which, if it were made public, would be likely to have a significant effect on the price or value of any securities*".

In effect, if a piece of information could be deemed material to the price of a share or a derivative of it, that information may be "inside information" which should in general be made public as quickly as practical.

Until the material information has been made public, a party dealing in or enabling someone else to deal in a share (or a derivative of it) that could be affected by that information is committing a criminal offence.

Inside information surrounding merger and acquisition activity is often particularly price sensitive and must remain confidential until released to the market. Other events frequently involving price sensitive information include company results statements and trading updates, board appointments and senior executive changes, contract wins and losses, changes in accounting treatment, crises affecting the ordinary course of business and suchlike.

As part of the Principles of Good Practice for the Handling of Inside Information, unregulated service providers (service providers) and participants in unregulated markets are encouraged to have in place procedures and controls to prevent the abuse of inside information.

The following are suggestions for differing organisations to consider and then refine as they think most appropriate to their businesses. Since it is anticipated that the following examples of good practice will evolve and be refined, updates to this Annex to the Principles of Good Practice will be published from time to time.

### **1. Policies and procedures**

A firm's policies and procedures for the use and control of inside information should be established and reviewed from time to time. These should recognise the responsibility to control access to inside information and reduce risk of misuse. There should be clear responsibility within organisations for overseeing controls and procedures in relation to inside information.

Good practice points to be considered include:

- Appoint a senior person with responsibility for maintaining good practice procedures, ensure they are trained and resourced and see that all members of staff know who this person is
- Maintain documented policies on price sensitive information handling that are regularly reviewed; and updated

- Conduct an internal review of the operation of policies, systems and procedures at least annually
- Ensure that insider lists are complete, accurate and regularly updated
- Have in place a policy on external contact enquiries, particularly with the media
- Staff policies:
  - Maintain procedures making it easy to report and discuss sensitive information being handled inappropriately
  - When staff who hold sensitive information leave a firm or change roles, conduct an 'exit interview' during which the leaver is reminded of the ongoing confidentiality of inside information
  - A policy on introducing temporary or contract staff to company policies regarding inside information
  - Undertake staff vetting such as criminal record checks and references from previous employers
  - Employment contracts to make staff aware of their duty of care regarding insider information together with the employer's right to access email, phone and other communication records as part of the employer's policy in regard to insider dealing

## **2. Awareness and training**

Appropriate measures should be taken, including training, to assist staff in understanding the importance of keeping information secret and the implications of improper disclosure – including the potential civil and criminal liabilities for the firm and the individual. Ensuring policies are capable of being readily understood by all relevant staff is an important part of this approach.

Good practice points for consideration include:

- Foster a culture that respects the sensitivity of inside information and establishes an awareness of the penalties for its abuse
- Have a dedicated training responsibility
- Hold induction training, as well as refresher training, for all staff regardless of position (including support staff)
- As new rules come into force, maintain an 'update' system
- Test awareness and understanding from time to time
- Maintain training records and review process annually

## **3. 'Need to know' and other information controls**

Reasonable steps should be taken to limit the number of those with access to inside information. Where practicable a "need to know" policy should be applied.

Good practice points for consideration include:

- A policy for making someone an insider, including only passing inside information to colleagues if they are first alerted to their responsibilities regarding the information
- Limit the number of insiders to a practical minimum and introduce a requirement to justify adding people to the insider list ("need to know" criteria)
- Communicate to other insiders when someone is removed from an insider list
- Where practicable, separate deal teams from other parts of the business
- Security of price sensitive information:
  - Have a policy on secure disposal of confidential documents/soft copy
  - Monitor and enforce a clear desk policy to reduce the risk of non-insiders seeing papers left on desks (contract cleaning companies)
  - Maintain formal, written procedures for staff working off-site
  - Use code names disguising the identities of relevant parties that are effective and not obvious
  - Discourage staff reading or working on sensitive papers in public and discussing sensitive matters in public (eg in taxis)
  - Require staff working on deals only to discuss deals in meeting rooms
  - Control the email distribution of sensitive information, ensuring the regular use of passwords
  - on documents
  - Control the hard copy distribution of papers (e.g. numbered copies or bar codes on documents)
  - Ensure hard copy sensitive information is stored in lockable cabinets and soft copy securely stored also

- Use restricted access systems in work and IT systems areas where sensitive information is handled

#### **4. Passing price sensitive information to third parties**

Reasonable care should be taken to ensure that where inside information is provided to a third party, the third party is aware of its obligations in relation to the use and control of the information.

Good practice points for consideration include:

- Maintain formal, written procedures when adding third parties to the information chain, formally making them insiders and spelling out the responsibilities inherent in handling the information
- Obtain comfort that third parties appreciate the importance of safeguarding inside information and have appropriate procedures in place
- Consider the third party's suitability as a recipient.
- Include third parties to the information chain as late as practical in the process
- Orally explain responsibilities rather than simply exchanging standard confidentiality letters

#### **5. Information technology security**

Appropriate consideration should be given to the security and access to inside information on IT systems, including the implementation of controls to limit access. IT configurations will differ significantly between service providers and some of the following may not be applicable; however good practice points for consideration include:

- Where practical, restrict IT access only to named individuals in preference to a companywide, open IT access
- The use of a secure "data room" with robust portal restricted to named individuals
- IT and other management support considered insiders to comply with appropriate policies
- Once a member of staff leaves or changes roles, the individual's IT access be removed
- Employ 'ethical hackers' to check the robustness of IT systems and keep abreast of any new methods of data theft
- Use code names and passwords for IT files and folders, including email subject lines
- Password protect all electronic equipment
- Laptops, Blackberries etc to have automatic locking after brief periods
- Technology to generate an audit trail of access to sensitive files
- Restrict emails with sensitive information going to personal websites
- Maintain procedures for 'fat finger' errors on emails, letters or faxes (recalling emails quickly and IT check showing if emails have been opened)
- Use Virtual Private Networks for staff who need access to system when working off-site

#### **Personal dealing policies**

Reasonable consideration should be given to establishing personal account dealing policies; those policies should be made clear to staff along with the civil and criminal penalties for dealing on the basis of inside information or for enabling such dealing.

Good practice points for consideration include:

- Maintain a formal, written procedure regarding Personal Account ("PA") dealing for all members of staff, ensuring awareness of this (consider including it in employment contracts) and test compliance from time to time
- Ensure that staff are aware that insider dealing is a criminal offence
- Explicit reference in PA dealing policy to derivatives, related products, sector "knock on", etc
- Policy covers dealings under power of attorney and by immediate family
- Policy addresses approach to dealings through discretionary accounts or manager, having regard to the independence of discretionary manager dealings
- Consider restricting staff or relevant staff members from dealing without permission from their immediate manager or compliance officer. Refusal may be given without further explanation
- Restrict staff members of service providers from dealing in client companies. (This should not apply
- Where assets are managed by others for a staff member on a discretionary basis without input from the person concerned).
- Require staff to maintain updated declarations of their holdings
- Keep a written log of permission requests and their outcomes, including risk based records of staff trading against announcements