Financial Conduct Authority

Flows of Confidential and Inside Information

December 2015

Thematic Review

TR15/13

Contents

1. Executive Summary

1.1 Financial services firms regularly receive, handle and generate large amounts of confidential and inside information as a result of the business they conduct.[1]

1.2 As well as complying with our rules, robust controls by firms around flows of information deliver better outcomes for market participants, improve trust in the professional financial services industry as a fair place to do business and ensure a clean market place.[2] These outcomes support our operational objectives of consumer protection, market integrity and effective competition.

1.3 This paper presents the findings of a process review into how a sample of investment banking firms manage the confidential and inside information they receive and generate. We found standards of control varied. Some of the practices observed result in heightened risks for market participants and firms. These include conduct and conflict of interest failings as well as FCA regulatory and legal breaches.[3] Furthermore if the information qualifies as inside information, then insider dealing and improper disclosure of information can result. Both are serious civil, as well as criminal, offences and the penalties are correspondingly severe.

1.4 Our review focused mainly on the Debt Capital Markets (DCM) and Mergers and Acquisitions (M&A) departments of small to medium sized investment banks. Controlling flows of information is crucial, whatever a firm's size and business model. The relevance of our findings, examples of good and poor practice and the practical questions for firms outlined in this paper can therefore be interpreted usefully across business areas.

1.5 All UK-based and FCA-regulated financial services firms should read and review this paper and consider whether their systems and controls, as well as processes and procedures, in respect of both confidential and inside information, are fit for purpose.

1.6 We did not test for market abuse including insider dealing/improper disclosure, whether civil or criminal, as part of this review. However, it is intrinsically linked to the subject of controlling information and continues to attract significant regulatory attention because of the regulatory and conduct risks associated with it.

1 Definitions of the terms confidential and inside information are provided below.
2 See, for example, SYSC 10.2.2R. The Appendix provides details of the regulatory requirements for firms in relation to managing information.
3 PRIN under Principle 8 requires firms to manage conflicts of interest fairly, both between itself and its customers and between a customer and another client. Please also refer to SYSC 10.

Overview of Key Terms

Some respondents found it difficult to define the difference between 'confidential' and 'inside' information. We have given some definitions below.

"Confidential information" *here means any information not in the public domain received or created by a firm, commonly understood as being information which should be treated as private, and not confidential information as defined within s348 of the Financial Services and Markets Act (FSMA).*

"Inside information" *as defined by s118C FSMA is information of a precise nature, which is not generally available, which relates, directly or indirectly, to one or more issuers of qualifying investments, or to one or more of the qualifying investments themselves, and would, if generally available, be likely to have a significant effect on the price of the qualifying investments or related investments. Please also note the other associated definition of inside information in s118C FSMA, in relation to commodity derivatives. The Criminal Justice Act (CJA) describes inside information as information which is specific or precise, not made public, likely to have a significant effect on the price of any securities if it were to be made public and relating to particular securities or issuers of securities.*

Several distinct pieces of information that do not in themselves constitute inside information, when taken together, can also constitute inside information. Firms and individuals should give proper consideration to the management of information received from external parties as well as to the collective information they hold and decisions they make themselves. Firms can receive, as well as generate, inside information and individual pieces of information which, by themselves, may not be inside information, may nonetheless collectively and/or where overlaid with the firm's decision, become inside information.

"Market abuse" *can result where inside information is improperly disclosed and/or used, other than in the proper course of the exercise of employment, profession or duties, for example to commit insider dealing.[4] Market abuse is punishable as a criminal or civil offence and may result in serious penalties (up to seven years imprisonment or an unlimited fine) and other enforcement action for both the firm and the individual.[5] Firms need to have in place an effective process for identifying inside information. Once identified, access to such information needs to be tightly controlled, with the number and identity of 'insiders' as defined by section 118B FSMA carefully monitored. Firms must be able to keep track of who has access to which pieces of inside information and all insiders should be recorded on an insider list.[6]*

4 There are seven civil market abuse offences including improper disclosure and insider dealing.

5 Insider dealing is a criminal offence under section 52 of the Criminal Justice Act (CJA) 1993. For details of the different civil market abuse offences under FSMA please refer to the Code of Market Conduct sourcebook (MAR 1) in the FCA Handbook

6 The rules on the maintenance of insider lists are outlined in the Disclosure and Transparency Rules (DTR) at DTR 2.8. Under DTR 2.8.6G the issuer is ultimately responsible for the maintenance of insider lists. However, in practice this responsibility is often carried out by those acting on behalf of the issuer. The Market Abuse Directive under Article 6(3) also requires that '[…]issuers, or persons acting on behalf or for their account, draw up a list of those working for them, under a contract of employment or otherwise, who have access to inside information.' Under the Market Abuse Regulation insider lists will need to follow a specified format and be kept for a period of five years following their last update. Firms may want to consider keeping a list of deal team members with access to the information ('deal team list') even where they are not required to maintain a formal insider list.

Key messages

1. Employees at all levels should understand their role in controlling flows of confidential and inside information and make it an integral part of how they carry out their work.

2. While firms and senior management had identified and considered the main risks that flows of confidential and inside information posed to clients, firms themselves and the financial markets, they were not doing enough to manage these risks.

3. We expect to see business heads acting in a supervisory capacity taking responsibility for controlling flows of information, with appropriate challenge and monitoring from the second and third lines of defence.[7]

4. Firms should place the assessment of circumstances that could present heightened regulatory and conduct risks at the centre of their ongoing risk assessment. These circumstances could also give rise to misuse of confidential and inside information.

Key Findings

1. We have summarised the findings of our review under three main headings below. These should be read in conjunction with the summary of our regulatory requirements in section 2, Scope of the Review. Further details of our findings are provided in section 3, including examples of good and poor practice, as well as practical questions for firms to consider.

A. Circumstances Posing Heightened Risk

2. Firms should regularly assess the conduct risks that affect their activities and services. As part of this, they should consider which circumstances pose heightened levels of risk for misuse of confidential and inside information and whether these have been considered and mitigated appropriately.

   - Changes to a firm's business model or rapid growth will likely pose new conduct risks, including around managing flows of information. Firms would benefit from considering and to the extent possible, mitigating these from the outset.

   - We found that several firms had not thought sufficiently about these types of circumstances. For example, where deal trees[8] are set up, the firm must consider how to control flows of information and manage its conflicts of interest.

7 The first line of defence includes management, front office and support functions that are responsible and accountable for its day-to-day activities, management of risks and controls to mitigate the risks of the business with senior management taking overall accountability across the firm. The second line of defence includes the global functions such as Risk and Compliance and is responsible for providing assurance, challenge and oversight of the activities of the first line of defence. The third line of defence is Internal Audit which provides independent assurance over the first and second lines of defence.

8 'Treeing' refers to the practice of providing services to more than one bidder in a competitive M&A transaction.

What does 'need to know' mean?

'Need to know' is a frequently used principle within the financial services industry. To appreciate how to best apply it, firms may want to consider only sharing confidential and inside information where certain criteria are met. Employees disclosing information should always ensure that they take into account the best interests of the client, and identify and manage any potential conflicts of interest that may arise either between (i) the firm and a client of the firm or (II) one client of the firm and another client.[9]

For inside information, firms must consider whether the disclosure is made in the proper course of the exercise of employment, profession or duties. In this context firms should have regard to Market Conduct Sourcebook section 1.4.5E of the FCA Handbook. This outlines (non-exhaustive) considerations to determine whether inside information is disclosed in the proper course of employment, profession or duties. While the Market Conduct Sourcebook[12] *relates to inside information, the considerations described are nonetheless indicative of the kinds of factors that determine if there is a 'need to know' and firms may find it helpful to consider these when deciding if confidential information should be shared. These include whether the disclosure is:*

- *Accompanied by the imposition of confidentiality requirements on the person to whom the disclosure is made and is:*
- *Reasonable and to enable a person to perform the proper functions of his employment, profession or duties; or*
- *Reasonable, including for the purposes of facilitating any commercial, financial or investment transaction.*[10]

When disclosing information, whether externally or to other parts of the business, the firm should be able to explain why the particular recipient needs to know this information.[11]

Firms would further find it advantageous to always keep the number of people privy to the information, confidential or inside, to the minimum necessary to perform a particular role or task to the appropriate standard.

9 In this context please review the current consultation on market abuse which can be found http://www.fca.org.uk/news/cp15-35-implementing-market-abuse-regulation.

10 Refer to MAR 1.4.5E for the full list of factors to be taken into account to ascertain whether or not behaviour amounts to improper disclosure.

11 Firms may find it useful to record individuals with access to confidential information on a deal team list. Where inside information is concerned, it is the obligation of the issuer under DTR 2.8.1R to keep an insider list of those individuals with access to the information. This obligation is in practice often delegated to the issuer's advisors.

B. Conduct, Culture and Responsibility

3. All staff members across the three lines of defence have a role to play in ensuring that flows of confidential and inside information are adequately controlled, though ultimate responsibility sits with senior management.[12]

- We noted that senior management responsibility and accountability in managing flows of information was not always clear and understood.
- The Compliance function in some firms was remote, while in others it took on too much of the first line's responsibilities.
- Employees at some firms shared information without adequate deliberation.

C. Firm Systems, Procedures and Infrastructure

4. Robust systems, procedures and infrastructure underpin the effective management of flows of confidential and inside information in firms.

- Our review found some firms had not adequately considered the risks of locating employees with conflicting roles or responsibilities in close physical proximity to each other.
- While firms used both manual and automated surveillance mechanisms around flows of information, these were not always fit for purpose.
- We found that both policies and procedures at some firms were not user-friendly and training was at times inadequately tailored to the needs of employees.

12 Refer to, for example, SYSC 3. Please also consider the new Senior Managers and Certified Persons Regime in this context.

Next Steps

1.7 This review is relevant to senior management, front office staff and all staff comprising the first, second and third lines of defence at UK-based and FCA-regulated financial services firms.

1.8 All UK-based and FCA-regulated firms should consider whether their own arrangements are fit for purpose and meet the standards set out in this report. If firms are not effectively managing the risks associated with flows of confidential and inside information, then they should make improvements to their practices. This is not a one-off exercise. All firms in the industry should have arrangements in place to continually review their practices and procedures for handling confidential and inside information both from a market abuse and conduct of business perspective. Firms should also keep themselves informed about their external environment and be aware of any changes in the conduct risks they face that may arise due to external factors. Examples of this include regulatory measures affecting the firm, changed market practices or other macroeconomic factors.[13]

1.9 We will provide individual feedback to the firms that participated in this review and will expect them to address any issues we raise with them.

13 Firms should also take into account other relevant publications such as The Fair and Effective Markets Review (FEMR) as well as remain apprised of future regulatory developments, in particular the Market Abuse Regulation (MAR), MiFID Regulation and Directives as well as any changes to the FCA Handbook.

2. Scope of the Review

2.1 This review focused on the processes investment banks have in place to control flows of confidential and inside information.[14]

2.2 The review sample consisted of sixteen mostly small- to medium-sized wholesale firms and contained both integrated firms and purely private side advisory houses. The sample firms were asked for policies and related documentation. We made full-day visits to 10 of the participating firms. These visits included transaction walk-throughs of a sample of DCM and M&A deals in which the firms had acted for clients, to illustrate how these firms handled information on a day-to-day basis. These reviews were conducted through staff interviews and a limited review of transaction documentation. We did not perform systematic testing or front-to-back transaction reviews.

2.3 The review also considered how senior management disseminated messages through the organisation, management oversight, employee understanding of key concepts and the role of the Compliance function, all in the context of controlling confidential and inside information. We met with CEOs and other senior management, junior staff, the business unit heads for DCM and M&A and Compliance staff.

The FCA's Approach to Flows of Confidential and Inside Information

2.4 The FCA Handbook outlines our regulatory expectations around management of risks, including in relation to flows of information (see Appendix for details). Our approach to regulation is defined by our strategic objective of ensuring that relevant markets work well. We also have three operational objectives: securing an appropriate degree of protection for consumers; protecting and enhancing the integrity of the UK financial system; and promoting effective competition in the interests of consumers in the markets.

2.5 If confidential or inside information is used or disseminated inappropriately, this has an impact on our achievement of our operational objectives.

2.6 **Market integrity:** If any type of inappropriate sharing of information is perceived to be tolerated, this represents a risk to the integrity of the UK market and its reputation as a clean and fair place to do business.

2.7 **Consumer protection:** A client may suffer detriment if any type of information about them or their business is shared or used inappropriately. Financial services firms often provide a range of different services to different clients, often within the same industry. Information about a competitor could be valuable to all of the respective teams working for these different clients.

14 Financial Conduct Authority, Our Business Plan 2014/15, http://www.fca.org.uk/news/business-plan-2014-15.

This scenario creates a potential conflict of interest for the firm which can harm the clients, the business and the firm's reputation. It needs to be managed properly.[15]

2.8 **Competition:** Inappropriate use of information by firms may also give them an unfair competitive advantage in the market and restrict the advantages of competition to the consumer. This is especially true when firms are inappropriately using clients' information to gain an unfair advantage in financial markets, as opposed to acting in their clients' best interests. This would occur if, for example, bank employees across different firms were agreeing on the price to charge a client, or clients and effectively creating a cartel. Inappropriate sharing of information about transactions and fee structures results in collusion and inefficient competition.

15 PRIN under Principle 8 requires firms to manage conflicts of interest fairly, both between itself and its customers and between a customer and another client. These are underpinned by the detailed requirements in SYSC 10.

3. Detailed Findings

3.1 While smaller firms often did not have, or necessarily need, extensive automation or systems-based controls, there was no clear difference in the quality of standards based on the size of the firm. We also found no notable systematic difference in the quality of controls between the different types of firms that formed part of the review (i.e. DCM/M&A/integrated).

3.2 We outline our findings in three sections: Circumstances Posing Heightened Risk, Culture, Conduct and Responsibility and the broader topic of Systems, Procedures and Infrastructure.

A. Circumstances Posing Heightened Risk

3.3 The specific regulatory and conduct risks a firm faces, including in relation to flows of information, depend on the business it conducts. Certain circumstances will create heightened risks of confidential and inside information being passed on or used inappropriately. These will vary from firm to firm and may depend on, amongst other factors, business model, product offering, types of clients and complexity of the firm. Firms must ensure that their systems keep pace with any growth in their size, business complexity or changes in the market place.[16]

3.4 Smaller or less complex firms may have less comprehensive or sophisticated infrastructure, but they still have to meet the same standards of complying with rules and regulations. These include the following:

- Are systems and controls as well as targeted monitoring arrangements around flows of information suitable for the firm's specific conduct risks and structured with them in mind?
- Are these risks reviewed regularly in light of market changes and developments?
- What circumstances present heightened risk and require higher levels of manual and/or automated surveillance?

Good practice

One firm reported that members of different deal trees would, as far as logistically possible, be located in different offices, or different rooms or floors, with adequate surveillance put in place.

The Fair and Effective Markets Review (FEMR) observes that 'reviews of the use of confidential information and increased scrutiny of trades' are useful practices for firms to consider. It also highlights that this type of supervision is 'likely to be most effective when backed up with direct oversight by front office managers and when high quality on-site Compliance staff are available to advise in cases of uncertainty'.[17]

16 See, for example, SYSC 3.1.1R and SYSC 10.1.7R in conjunction with SYSC 10.1.3R. Also refer to PRIN 2, 3, 6 and 8 as well as COBS 11.7.

17 www.bankofengland.co.uk/markets/Documents/femrjun15.pdf, p. 76.

Poor practice

Several firms did not put in place adequate systems and controls, including enhanced surveillance, in the context of debt issuances in relation to which the firm would be entering into a swap/derivative (e.g. interest rate/currency swap). The trader executing the swap would often be made aware of their role before the swap needed to be executed (normally once the debt issuance, but not necessarily the intention to swap, is in the public domain). Aware that they will have to execute a potentially large swap at a later date, the trader may start building a position in advance, in order to minimise market impact. This may be prudent but knowledge of the impending swap (and the debt issuance where that is not already public) could also be used to trade on inside information and this might constitute insider dealing[18], as well as breach our conflicts of interest[19] and client order handling rules.[20]

A small number of firms did not have in place adequate arrangements for sovereign debt issuers and did not require sovereign issuances to be logged, even where potentially sensitive issuances, e.g. by lower rated sovereigns, were concerned. All types of information about upcoming debt issues potentially represent inside and in any case confidential information.[21]

B. Conduct, Culture and Responsibility

3.5 A strong, positive firm culture which is acutely aware of the risks around flows of information is crucial to ensure that these risks are adequately managed. If employees take responsibility for their conduct and escalate any concerns, the risk of inappropriate flows of information can be greatly reduced. A conduct culture that is embedded through all levels of the firm is beneficial in managing both flows of information but also to the management of risks at the firm more widely.

3.6 Senior management at all of the firms confidently reaffirmed the importance they placed on controlling flows of confidential and inside information. However, some senior management were unable to adequately explain the difference between confidential and inside information.

• Senior management responsibility

3.7 The FCA requires senior management to be aware of the risks of inappropriately handling inside and confidential information.[22]

- Is senior management able to identify inside information and aware of their obligations in relation to controlling flows of information?
- Does senior management visibly champion adherence to firm principles about controlling flows of information, both formally and on a day-to-day basis?
- Are lines of accountability for managing flows of information clearly defined, both overall and in relation to day-to-day deal management?
- Does senior management take an active interest and role, as appropriate, in training staff to practically apply regulatory requirements, including rules around improper disclosure, the circumstances under which confidential and inside information may be shared, as well as the associated controls?

18 Please refer to MAR 1.3.2 in this context.
19 See SYSC 10.1.7R.
20 See, for example, SYSC 10 and COBS 11.3.5R.
21 Please refer to SYSC 10.1.3R as well as SYSC 1.1.7R in this context.
22 See, for example, SYSC 2 and SYSC 6, as well as SYSC 5.1.12R and SYSC 4.3.1R.

Good practice
At one firm, senior management at CEO level would stand alongside Compliance at 'townhalls' to discuss compliance-related matters. This demonstrates in a visible way the importance placed on compliance-related matters by senior management.

One senior manager described an example of stopping a junior about to inappropriately dispose of documents. This demonstrates the kind of everyday attention to detail and leading by example that is essential in senior staff.

Poor practice
In some instances, the first line appeared lax in relation to its responsibilities in managing flows of information.[23] At times, there was both a misunderstanding of policies and a lack of clarity on procedure. At some firms, senior management repeatedly stated that 'Compliance did this' task, rather than demonstrating ownership and proper understanding of the risks.

- **Role of Compliance**

3.8 Firms can set up their second line of defence in different ways to meet our rules and manage their conduct risks. In practice, it appeared that the first line benefitted from the physical proximity of select members of Compliance on a day-to-day basis.[24]

3.9 We considered two questions:

- Does the role of Compliance include both concurrent challenge and retrospective monitoring of flows of confidential and inside information?[25]

- Do Compliance in their role as second line of defence staff adequately understand the activities of the business they oversee and the risks around flows of confidential and inside information arising from them?

Good practice
At several firms, a member of the Compliance function was part of the 'conflict and new business approval' committees and also contributed to policies and procedures. At many firms, the Compliance function's importance was underscored by a physical presence within the business lines, both public and private.

Compliance should challenge the business where required, and provide insight and oversight at the appropriate times. This includes assisting the first line in ensuring inside information is identified and logged. This shows a balance between the two very different examples of poor practice below.

23 This is part of the FCA's expectations under SYSC 3.1.1R.
24 Market Watch 49 on Commodities Trading notes 'the best results were achieved by those firms where Compliance was integrated with the front office and had a permanent physical presence on the trading floor; at these firms we observed proactive risk identification with Compliance participating in the flow of information and traders able to receive guidance on acceptable market conduct.' Market Watch No. 49, Commodities Trading Thematic (CT) Review, September 2015. http://fca.org.uk/static/documents/newsletters/market-watch-49.pdf.
25 See SYSC 6.1 for details of the regulatory rules and expectations around Compliance.

Poor practice

At some firms, Compliance appeared to be seen as a quasi-administrative function, removed from the business both in terms of location and the quality and level of interaction. At one firm, the Compliance function was located in a different building to the business, while in another it was based in another city.

There were other cases of Compliance being strong and constantly present at all stages of transactions. This can lead to the first line relying too much on Compliance, when the business itself should be taking responsibility. Over time, this could result in the degree of challenge provided by Compliance growing weaker and it effectively operating as part of the first line. This also creates the risk that the second line will be monitoring its own work, rather than the work of the first line.

- **Information sharing**

3.10 Information should only be shared where strictly necessary. Senior management should think about how to implement this principle on a day-to-day basis, including appropriate oversight arrangements as well as considering electronic sharing and access.[26] All employees should take responsibility for adherence to the principle of only sharing confidential and inside information where permissible.

- Can senior management and staff always explain the reason for deciding to share confidential information?
- Inside information may only ever be shared in the proper course of the exercise of employment, profession or duties. Has the firm put adequate monitoring arrangements in place, including defined wall-crossing procedures, to ensure information is appropriately disseminated?
- Does internal supervision of flows of information include both manual and automated monitoring, as well as related management information (MI) and auditing?
- Have the risks associated with the use of code words as well as electronic access rights been considered by the firm and is their use within the firm's risk appetite?
- Have firms considered their processes in relation to the sharing of information:
  - Between public and private side employees?
  - Between employees on the same side of the information barrier?
  - Where the information concerned is confidential, rather than inside information?
  - Electronically and via, for example, distribution lists?

Good practice

Some firms stated they would only share information on live transactions with senior management and people on the deal team to the extent needed and always considered whether this was necessary and permitted. They shared transactional lessons learned more widely when the transaction had been completed and was in the public domain.

26 Refer to the section on Surveillance found at 3.16-17 of this report in this context.

Poor practice

At some firms, ongoing transactions were discussed in general meetings with teams of up to 25 private side employees, including those who were not part of the deal team and did not need to know the information.

At one firm, team meetings sometimes included both public side employees and private side groups, i.e. DCM team meetings included the public side MTN (medium term note) desk. While they took great care to restrict the discussion to market trends seen by the MTN desk and not potential DCM transactions, this still creates a risk of updates straying into the non-public domain and inside, or at least confidential, information being passed on by accident and potentially misused.[27]

All firms reported using code names for certain types of transactions to help control flows of information and some firms provided updates on deals at team meetings using code names. Employees frequently reported that they may be able to work out the underlying transaction if they so wanted, putting into question the effectiveness of code words as a mitigant.

One firm we visited gave electronic access to deal-related information on a sector team basis. It has changed its approach following our feedback.

C. Firm Systems, Procedures and Infrastructure

3.11 Whatever its size or business model, a firm must take care to establish and maintain systems and controls which are appropriate to its business.[28]

3.12 All firms had defined procedures around personal account (PA) dealing, insider or deal team lists and wall crossings. Other useful practices include monitoring and enforcing a clear desk policy, restricting IT access and marking sensitive calendar entries as private.

• Policies and procedures

3.13 Firms must implement appropriate and robust processes. These should include how to identify inside information as well as how and when confidential and inside information may be shared.[29]

- Are the policies and procedures easy to find and use; are they up to date and reviewed regularly; are they meaningful and relevant for employees?
- Has the firm given adequate consideration to both confidential and inside information?
- Would employees benefit from practical examples and case studies relevant to their day-to-day work?

27 The FCA notes that many firms in the market have now moved their MTN desks along with Syndicate on to the private side to reduce this risk.
28 See, for example, SYSC 3 and SYSC 10.
29 Specifically in relation to conflicts of interest, SYSC 10.1.11R outlines our expectations for firms' conflicts of interest policies.

Good practice

Many firms' policies and procedures included a definition and examples of what constitutes confidential and inside information, as well as the requirements around identification, control, insider or deal team lists and PA dealing restrictions.

Some firms included a description of the different civil and criminal offences, including improper disclosure, insider trading and associated penalties.[30]

A small number of firms referenced relevant enforcement cases in the area of market abuse to demonstrate how UK and EU legislation applies to flows of information. Some firms had specific and bespoke conflicts of interest policies for each business area which included examples of potential conflicts of interests tailored to that specific business line and its activities.

Poor practice

A small number of non-UK headquartered firms completely failed to reference the UK regulatory regime and regulatory bodies in their policies and procedures.

Others contained overly legalistic language or excessively cross-referenced different policies and annexes, making it difficult to find the required information. This means they did not function as a practical tool for employees to support them in doing their job.

- **Physical separation, information barriers and electronic separation**

3.14 Firms should think about how to ensure that access to confidential and inside information is limited to personnel who are expressly permitted to access such information. Manual and automated surveillance is an important part of limiting risk in this area.

3.15 We found the majority of firms had already adopted the physical separation of certain functions to help control the flow of information and manage potential conflicts of interest (e.g. separate the primary syndication team and secondary market bond traders).[31]

- Is the firm exposed to unnecessary and/or inappropriate conduct and conflict of interest risks as a result of the potential co-location of different private side groups, e.g. ECM versus M&A, as well as ECM versus DCM?[32]
- Has the physical location of different teams which regularly handle inside information, including in the case of organisational 'trees', been considered? What are the associated surveillance needs?
- Is electronic separation, both routine and ad hoc, fit for purpose?
- Are the electronic access records which are kept sufficient to enable firms to effectively monitor and demonstrate control of confidential and inside information?

30 For details of the different market abuse offences please refer to the Code of Market Conduct sourcebook (MAR 1) in the FCA Handbook.

31 www.bankofengland.co.uk/markets/Documents/femrjun15.pdf

32 Please refer to SYSC 10.1.3R and SYSC 10.1.7R in this context. Any inappropriate dissemination of information may further put firms in breach of the MAD and MAR.

Good practice
Most firms in our sample had separated all of their private side functions, as well as their Prime Brokerage and Proprietary Trading desks, from public side floors.

Poor practice
In two firms, private side functions, such as the DCM and/or private side Syndicate desk, were located on the trading floor without physical barriers between them and the public side. Further, one of the firms had located the proprietary trading desk in the middle of the trading floor. Both firms have since resolved this situation following our feedback.

In another case, ECM and M&A were located in close proximity, which causes concerns that information may be inadvertently shared. This requires careful monitoring of who has access to confidential information and inside information. It also raised concerns regarding how the firm managed its conflict of interest risks.

- **Surveillance**[33]

3.16 Surveillance models can vary. Firms should consider the particular manual and automated surveillance needs in relation to flows of confidential and inside information in their businesses and implement what is expected to be an appropriate and effective surveillance model. It appeared that the most useful strategies relied on a mixture of manual and automated surveillance.

3.17 Physical separation may be difficult to achieve in practice, but is something firms should strongly consider where possible. Where this is not possible, enhanced surveillance, including automated surveillance, becomes even more important. Embedding Compliance officers with front line operations to improve manual surveillance capabilities and information management may also be useful, as observed in the FEMR Report.[34]

- Has the firm considered targeted surveillance based, for example, on key words, specific instruments, staff and ongoing transaction timings, with heightened surveillance at key stages and decision points of deals?
- Does surveillance take into account the use of multiple languages and/or colloquial language?
- Have the risks arising from the use of mobile phones, instant messaging (including e.g. Bloomberg chat rooms) and other social media, over and above those classified as relevant conversations, been sufficiently considered?[35]
- Does the firm keep up to date with the prevalence and development of other types of communication platforms in their policies and training of staff (e.g. Whatsapp, Instagram, VOIP etc.)?

33 Please refer to, for example, PRIN 2 and 6 as well as COBS 11.3.5R and COBS 11.3.6G in this context.
34 www.bankofengland.co.uk/markets/Documents/femrjun15.pdf
35 Firms are required to record relevant conversations and communications. The recording perimeter is set out in COBS 11.8.

Good practice
After seeing a number of desk limit breaches, one firm ensured a constant Compliance presence on the floor, in addition to automated surveillance of trading activity. This also helped the manual monitoring of flows of information.

As our rules require, all firms confirmed that they had a policy in place for the use of mobile phones and other electronic mediums and devices in the workplace when undertaking certain activities. This included recording fixed line and mobile phones, email surveillance and the monitoring of chat rooms and instant messaging. Some firms also recorded communications and conversations that are not within the scope of our rules and did so from a legal and risk management perspective.

Poor practice
One firm with a small leveraged finance team would allocate employees to different financing teams in a competitive M&A situation ('treeing') without separating the employees, adequately limiting system access or putting in place any additional surveillance.

- **Logging of deals**

3.18 Firms would benefit from logging and conflict clearing potential deals as soon as feasible, independently of mandate status. We appreciate that firms do not always have advance notice of a deal until the mandate is awarded. This is particularly the case in DCM, as these transactions are sometimes executed at short notice.

3.19 Deals must always be logged when inside information is received or generated, at which point insider lists should also be kept.[36] It is important to note that this could be the case even for so-called 'frequent borrowers' (in the case of lower rated sovereign issuers for example).

- Is each transaction considered on its own merit, rather than using a 'one size fits all' approach?
- Is the changing nature of clients kept under review?
- Are any potential conflicts and the information received or generated considered when logging deals?
- Has the risk of not recording, or recording late, who has access to confidential information been considered?
- What prior practices for the logging of deals still in place may no longer be appropriate because of a changed market environment?

Good practice
One firm reported that each client interaction was recorded on a central system which allowed the creator to decide who was allowed to see it. Several firms stated that they set up a deal log as soon as feasible and always before attending any pitch meetings with clients.

36 Please refer to the earlier footnote number 6 on the subject. While insider lists are ultimately the issuer's responsibility, this will often be delegated to the firm's advisor(s). Firms may nonetheless benefit from keeping deal team lists in any case to track who has access to confidential and inside information held by the firm.

Poor practice
One firm's policy required conflict clearance for DCM deals only after they had received a mandate. At another firm, debt issuances for 'frequent corporate' issuers were not logged and employees reported, that for all DCM deals a log may not be set up until mandate, even if there was a formal pitch.[37,38]

- **Training**[39]

3.20 Employees must be fit and proper to carry out their functions.[40] As part of this, firms must comply with the rules in the Training and Competence Sourcebook (TC).[41]

- Have the training needs of different groups of employees been taken into account, e.g. based on business areas and levels of experience (new joiner, experienced hires)?
- Have the benefits of training targeted at the handling of client information and conflicts of interest management been considered?
- Have the advantages of different types of instruction, including internal face-to-face, online and external training been taken into account?
- Would employees benefit from senior management providing and/or supporting training, for example by drawing on their experiences and providing real-life examples?
- Would it be useful to test training effectiveness on a regular basis?
- Have the benefits of tracking attendance, and a potential impact on remuneration for non-attendance for staff at all levels, been considered?

Good practice
Several firms had training programmes targeted at different groups of employees. One firm had a specific training programme for employees who joined from other jurisdictions, to ensure they were familiar with the UK regulatory regime.

Poor practice
One firm reported doing its entire Compliance training syllabus at a single face-to-face session held once a year. Employees felt that this was too concentrated and not as useful as more bite sized training spread throughout the year.

37 Please refer to SYSC 10.1.3R in this context.
38 The FCA's expectations are set out in SYSC 10.
39 The FCA's expectations are set out in the Training and Competence sections of the FCA Handbook.
40 Please also reference the new Senior Managers and Certified Persons Regime for the responsibilities of firms in this context.
41 Please refer to the FCA Handbook for applicability.

Appendix 1
Relevant Rules and Legislation

1. We have a number of regulatory powers at our disposal to ensure firms comply with our rules. These include the power to stop firms and individuals providing regulated financial services, levying fines on firms and, where we think it is necessary, taking enforcement action.

2. Below are some of the most relevant rules and regulations that underpin our oversight of management practice related to handling confidential and inside information. This is not an exhaustive list.

3. When considering the requirements and expectations around the handling of confidential and inside information, firms should specifically take into account their obligation to always act in the best interests of their clients (COBS 2.1.1R) as well as the **Principles for Business (PRIN)** section of the FCA Handbook.[42] PRIN sets out the fundamental obligations of all firms under the UK regulatory system. Firms should be particularly aware of the following when considering their responsibilities for the handling of any type of information:

4. Principle 2. *A firm must conduct its business with due skill, care and diligence.*

5. Principle 3. *A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.*

6. Principle 5. *A firm must observe proper standards of market conduct.*

7. Principle 6. *A firm must pay due regard to the interests of its customers and treat them fairly.*

8. Principle 8. *A firm must manage conflicts of interest fairly, both between itself and its customers and between a customer and another client.*

9. **Senior Management Arrangements, Systems and Controls (SYSC)** sets out the responsibilities of directors and senior management. Firms should have particular regard to:

   - SYSC 3 (Systems and Controls)
   - SYSC 4 (General organisational requirements)
   - SYSC 5 (Employees, agents and other relevant persons)
   - SYSC 6 (Compliance, internal audit and financial crime)
   - SYSC 10 (Conflicts of interest)

10. The Training and Competence sourcebook (TC) sets out the commitment and requirements concerning staff competence.

42 Please check correct application of the FCA Handbook rules according to the type of entity or activities, or both, as necessary.

11. For inside information specifically, firms should be mindful of the criminal offences under Section 52 of the **Criminal Justice Act 1993 (CJA)** and the civil market abuse regime under the **Financial Services and Markets Act 2000 (FSMA)**. Section 118 FSMA describes six types of behaviour that may constitute market abuse, including improper disclosure of inside information. Note that failure to correctly classify information as 'inside' is not a defence against the charge of improper disclosure. The **Code of Market Conduct (MAR 1)** provides detailed guidance for market participants on the civil market abuse regime in s118 FSMA 2000 and describes forms of conduct that would, and would not, amount to market abuse.

12. The FCA is authorised under FSMA Section 402 to enforce the criminal offences of insider dealing and market manipulation (CJA) with a maximum penalty of seven years imprisonment or an unlimited fine. Additionally, where we find the relevant individual is not fit and proper, we may be entitled to vary or revoke the offender's regulatory permissions and could ban them from holding any FCA regulated function in future.

Forthcoming changes

The Markets in Financial Instruments Directive (MiFID) II

13. MiFID II when it comes into effect, will strengthen a number of the requirements outlined in this report. Firms should make sure they are aware of their obligations under MiFID II and the associated implementing measures and can meet them by the relevant implementation date. In the context of flows of information firms should have particular regard to the enhanced requirements around:

- **Conflicts of interest.** Under Article 23 firms will be required to take all appropriate steps to identify and prevent or manage conflicts of interest. This underlines the need for firms to identify and prevent or manage conflicts of interest. It also significantly enhances the content and quality of the disclosure to be made available to clients when firms cannot manage or prevent conflicts of interest from arising.

- **Compliance function.** MiFID II will strengthen the Compliance function. ESMA in its technical advice to the Commission stated that senior management should be ultimately responsible for establishing and maintaining an appropriate and effective Compliance function.[43]

- **Record keeping.** MiFID II will increase firms' reporting obligations and the reviews to be carried out by senior management. For example, firms will be required to periodically monitor the records of transactions and orders that fall under the new recording of telephone conversations and electronic communications requirements.

The Market Abuse Regulation (MAR)[44]

14. The Market Abuse Regulation will apply from 3rd July 2016. MAR will replace the current civil UK market abuse regime, which is based on the 2003 Market Abuse Directive (MAD).[45] It will update and strengthen the existing framework in a number of key ways, most significantly by extending its scope to cover new markets, platforms and financial instruments. MAR will extend to cover all financial instruments trading on an EU regulated market and will include instruments trading on a multilateral trading facility (MTF) and an organised trading facility (OTF).

43 EMSA, Final report. Guidelines on certain aspects of the MiFID compliance function requirement, www.esma.europa.eu/system/files/2012-388.pdf.

44 http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0596&from=EN

45 Please refer to our current consultation on market abuse which can be found www.fca.org.uk/news/cp15-35-implementing-market-abuse-regulation

15. For inside information specifically, the definition will remain largely unchanged under MAR. However, MAR will separate the definition in relation to the different types of products (including commodity derivatives) and will introduce a new definition of inside information for emission allowances and auctioned products. It also extends the insider dealing offence to instances where an order placed before receiving inside information is subsequently cancelled or amended based on the information received. Attempting to engage in insider dealing, as well as encouraging another person to do so, will also be caught under the legislation.

16. MAR maintains a prohibition of disclosure of inside information and states that unlawful disclosure occurs where a person possesses inside information and discloses that information to any other person, except where the disclosure is made in the normal exercise of an employment, a profession or duties.

17. MAR will add further detail to rules around insider lists, for example by requiring that insider lists are retained for a period of five years after their last update and specifying the precise, harmonised, format of the lists. MAR will also introduce a new framework for disclosures of inside information made in the course of a market sounding. Provided that certain requirements are met, persons will be protected from the allegation of unlawful disclosure.

Financial Conduct Authority

PUB REF: 005134

25 The North Colonnade Canary Wharf
London E14 5HS
Telephone: +44 (0)20 7066 1000
Website: www.fca.org.uk