CONSULTATION CESR 08-274

Market Abuse Directive
Level 3 – Third set of CESR guidance and information on the common operation of the Directive to the market

Response of the AMAFI

1. AMAFI thanks CESR for providing it with the opportunity to discuss the third set of guidance it is putting together to help the harmonised implementation of the Market Abuse Directive with respect to insiders' lists and Suspicious Transactions Reporting (STRs).

2. AMAFI is the new name adopted on 19 June 2008 by the French Association of Investment Firms (AFEI). It represents financial market professionals in France (i.e. investment firms, credit institutions and market infrastructures) and has more than 120 members representing over 10,000 professionals who operate in the cash and derivative markets for equities, fixed-income products and commodities. Nearly one-third of the members are subsidiaries or branches of non-French institutions.

3. As we have often stressed, preventing market abuse is a major concern for AMAFI members; it is also vital for achieving an integrated financial market in Europe. From the outset, AMAFI has closely participated in and supported the implementation of the Market Abuse Directive ("the Directive")[1]. In particular, AMAFI has always been keen both in promoting harmonisation of implementation measures and in setting practical guidelines to its members to ease implementation[2]. In this respect, we regard CESR's first and second guidance and information on the common operation of the Directive to the market as useful means for achieving these goals.

4. We therefore examined with great interest the paper CESR put out for consultation on 20 May 2008 and wish to make the following observations. Please note that the title numbers used throughout this document refer to the corresponding paragraphs of the consultation paper.

[1] Directive 2003/6/EC and its implementing Directive 2004/72/EC
[2] "*AMAFI – FBF Implementation Guide: procedure for reporting suspicions of market abuse*", *April 2006.*

AMAFI ■ 13, rue Auber ■ 75009 Paris ■ France
Phone : +33 1 53 83 00 70 ■ Fax : +33 1 53 83 00 83 ■ http://www.amafi.fr ■ E-mail : info@amafi.fr

➢ ***General comments***

5. As a general matter, AMAFI is pleased to note that STRs are useful to regulators in their investigations and have come to constitute a powerful tool to counter market abuse attempts.

However, the guidance tends to grant an importance to STRs that could somewhat alter the original objective of the Directive. Although useful, these only constitute alerts, i.e. one of the various tools available to regulators to identify potential cases of market abuse and decide possibly to launch investigations. Neither are they substitute for active monitoring by regulators, nor a record of data that an authority would be entitled to collect if the suspicion was considered founded and an investigation launched.

As a consequence, it appears unfounded to us to require the provision of additional information within the STRs, which are actually data that the authority would enquire upon in the context of an investigation (such as banker name and conversation tapes). Investment firms put their commercial relationships at risk when they submit STRs (in some cases, the number of people involved in a transaction is so low that the origin of the notification is obvious) and should not be asked to perform, additionally, some of the investigation tasks that are the remit of authorities. As a result, the provision of additional information should only be limited to elements that gave rise to the suspicion (see our comments on §31 of the draft guidance).

6. As far as the draft guidance on insiders' lists is concerned, the Association believes it could be useful to separate guidance destined to issuers from the one destined to their advisers. Some questions regarding the implementation of market abuse are indeed specific to one or the other and therefore some recommendations may not apply to both. As an example, it may be of interest to distinguish between the issuers' responsibilities in establishing insiders' lists and the intermediaries' in §11. Similarly, examples of categories of persons having regular access to inside information in §15 might differ slightly for issuers and intermediaries (see our comments on §15 hereafter).

➢ ***Insiders' lists***

✓ **§ 11**

7. CESR starts by recalling that the requirement to keep, maintain and provide the competent authority with insiders' lists only apply to issuers -or persons acting on their behalf or for their account- who have requested or approved admission of their financial instruments to trading on a regulated market in a Member State. Then, CESR specifies that "*the issuer should make these third persons aware that all persons who might be expected to have access to inside information are to be included in the insiders' lists, which are sent to the competent authorities*".

8. AMAFI agrees with the view that persons who have access to inside information relating directly or indirectly to the issuer must be included in insiders' lists. Consequently, investment firms that draw up insiders' lists should also include the names of third parties or entities within the group the investment firm belongs to. However, in practical terms, these insiders may not be subject to the Directive (because of their legal status or location).

Consequently, although the investment firm may add to its insiders' lists the name of these firms, it may be the case that these firms will not draw up their own lists of employees who have gained access to inside information because they have no legal or regulatory requirement to do so (even though some third parties may choose to do so because of a contractual commitment with the investment firm, or some group entities may do so because of the group's policy applicable to them). Additionally, it is doubtful that a European regulator will be a competent authority to carry out an investigation on such entities and/or impose penalties on them.

⇨ AMAFI therefore calls on CESR to provide some clarity on what is expected from European investment firms in terms of recording on insiders' lists other legal entities that are not subject to the Directive.

✓ **§ 13 : Permanent and occasional insiders**

9. CESR considers that "*the emphasis should rather be given to the access (regular/occasional) of persons to inside information related directly or indirectly to issuers than to the existence of a legal distinction between regular and occasional insiders*".

In AMAFI's view, this paragraph requires clarification. We are uncertain what the differences are between a "*regular or occasional access to inside information" and "a legal distinction between regular and occasional insiders*".

Generally speaking, the Association agrees with the need to keep insiders' lists as short and meaningful as possible (as stated in §11 of the draft guidance), meaning that these should not include individuals who could only have access to inside information by chance, but rather those whose role or activities imply that they have such access.

However, AMAFI considers that the distinction between occasional and regular insiders is useful and consistent with a well established practice in the industry, even though harmonisation at the European level may be needed.

10. As an example, in response to practical queries from practitioners in France, the French securities regulator (AMF) has published on 18 January 2006 (updated on 14 November 2007[3]) a position regarding the drawing up of insiders' lists.

This position distinguishes between permanent insiders -people who, by virtue of their function, have regular access to insider information about the issuer, such as compliance officers- and temporary insiders (also known as transaction team insiders) -people who have access to information about the issuer from time to time, e.g. because they are involved in preparing a financial transaction.The AMF recommends that issuers and third parties acting on their behalf draw either an insiders' list aggregating both types of insiders or two different lists, one for each type.

To our knowledge, this practice is also common in the UK, where the FSA distinguishes between regular and occasional access to inside information (*DTR 2.8.1, Full Handbook*[4]).

[3] http://www.amf-france.org/styles/default/documents/general/6446_1.pdf

[4] "An *issuer* must ensure that it and *persons* acting on its behalf or on its account draw up a list of those *persons* working for them, under a contract of employment or otherwise, who have access to *inside information* relating directly or indirectly to the *issuer*, whether on a regular or occasional basis."

11. In our view, this distinction is crucial to ensure that insiders' lists are properly kept up-to-date and therefore the circulation of inside information is managed as effectively as possible. Additionally, because the definition of permanent and occasional insiders is not different to the one provided by CESR (§12 of the consultation paper "*To be included by a company on its insiders' list, the concept of having access to inside information means that the person concerned must have access to information as a result of his activities or duties within the issuer or persons acting on their behalf…*"), such practice does not result in longer lists or in the inclusion of people who are not actual insiders. On the opposite, people who may not be permanent insiders are included on the lists only when they gain access to inside information, which is a practical way of maintaining lists that are relevant and current.

⇨ AMAFI therefore calls on CESR to recognise that the distinction between temporary and permanent insiders is of practical use with regard to drawing up insiders' lists.

✓ **§ 15 : IT people and people having access to databases on budgetary control or balance sheet analyses**

12. CESR lists examples of people who are to be included on insiders' lists because they have regular access to inside information, such as IT people.

AMAFI recognises that there exist risks of leakage of information towards the IT population. However, as previously stated by CESR in §12, insiders' lists should not include those people who come to obtain inside information by accident, which may well be the case with a number of IT people whose initial duty does not involve accessing inside information but who may be able to access it while carrying their duty (for example, a person in charge of the maintenance of servers). It would therefore be extremely difficult to determine which IT function is likely to provide access to inside information, a difficulty that could result in lengthy insiders' lists, which is not a desirable result.

To this conceptual hindrance, one should add that, by nature, the IT population is somewhat exceptional because it is largely made of external contractors and turnover is high. There is therefore a practical difficulty in maintaining an up-to-date list.

13. Finally, it should be asked if the inclusion of IT people in insiders' lists would serve a purpose since they are generally tied contractually by confidentiality provisions and a duty of abstention if they become aware of inside information. If it is considered that the purpose still holds true, it may be better served by inserting a provision within the firm's set of policies that each department using a system is responsible for identifying regular IT insiders and communicating these names for addition to the firm's insiders' lists. Of course, this will give rise to regular training sessions designed specifically for these systems' owners to help them identify IT people who could be considered as insiders.

⇨ AMAFI therefore asks CESR to either remove IT people from the list of examples of "*categories of persons who have regular access to inside information*" or to adapt its statement to allow for a risk-based approach to this issue.

14. The draft guidance provides another example of professionals having regular access to inside information, i.e. people having access to databases on budgetary control or balance sheet analyses. AMAFI is strongly against listing these functions as examples. Such professionals, by virtue of their function, do not have regular access to insider information. They may gain access to information on a deal but only after it is public (to book fees for example). Similarly, they may have regular access to financial data about an issuer but based on its financial reports that, by nature, are a reflection of past events. If they were to obtain pro-forma financial data, computed in relation to a contemplated transaction, these individuals would be brought across the wall on a case-by-case basis. This does not constitute regular access to inside information.

⇨ AMAFI therefore asks CESR to remove people having access to databases on budgetary control or balance sheet analyses from the list of examples of "*categories of persons who have regular access to inside information*".

➢ ***Suspicious Transactions Reports (STRs)***

✓ **§ 26 : Competent authority**

15. In this paragraph, CESR points out that there are uncertainties in the market to determine which CESR members would be the competent authority to receive suspicious transactions notifications, but does not provide guidance as such. Addressing this issue is however a task that CESR could help undertake.

In AMAFI's experience, it is indeed not always easy for firms to determine which authority is competent to receive their suspicious transaction reports. For example, this is the case when a security is listed on several markets or a company executing a transaction is a remote member of an exchange, as well as its subsidiary located in another country, from which it receives orders.

⇨ AMAFI asks CESR to consider ways to help determine the authority competent for receiving suspicion reports.

✓ **§ 27 : unexecuted order**

16. CESR indicates that "*an unexecuted order for a transaction that gives rise to a suspicion of market abuse shall be reported to the competent authority*".

AMAFI agrees with CESR's view that when a firm has determined that a planned transaction was an attempt of market abuse and has declined to proceed with the transaction for that reason, it should report it to the competent authority.

However, using the terms "*unexecuted order for a transaction*" creates confusion because it could refer to other circumstances, which the firm may not be able to spot. An unexecuted order could either be an order that has never met an opposite interest or an order that was cancelled. In the first instance in particular, it is very unlikely that such an order would have raised suspicion only because it was not executed.

The triggering point of the reporting is not the fact that the order was unexecuted but rather that the firm had a suspicion in the first place and did not proceed with the transaction. What should be clearly stated here is that not proceeding with the transaction is not a reason not to report the suspicion to the competent authority.

⇨ AMAFI therefore calls on CESR to remove the terms "unexecuted order" from this paragraph of its guidance.

✓ **§ 31 : information included in the notification / confidentiality of the notification**

17. The implementing Directive specifies the minimum content of an STR. And it indicates that it should include "*any information and documents which may have significance in reviewing the case*". CESR's proposed guidance provides more detail, listing information that should be included or attached to the STR when they are readily accessible for the firms and can be easily attached to the notification.

AMAFI supports this attempt to identify more precisely which information may be concerned. This information rests on two fundamental principles (besides its significance to the case): accessibility and ease of communication. Although important, we believe that these two principles are insufficient. Additional information should be related only to the elements that gave rise to the suspicion and not to data that only further investigation would need to consider.

As a result, we must stress that we strongly oppose providing the name of the person having direct contact with the client and the tapes of conversations between the firm and its client, despite their being potentially readily available.

18. Although we agree that this information could be delivered, it should be within the context of an official investigation by the competent authority, as we consider that it is too sensitive to be transmitted in the first stage of the procedure, because it touches upon the confidentiality duty of an intermediary towards its clients and of an employer towards its employees.

Conversation tapes could contain information that may touch on other matters than the ones relating to the suspicious transactions. The banking secrecy principle should not be infringed upon more than absolutely necessary in order to preserve clients' confidence in their intermediary. A balance needs to be sought between preserving the confidentiality of client's information as a matter of principle and fostering market integrity. There is also a risk that the investment firm's reputation could be harmed as a result.

19. In addition, the need for competent authorities to have a contact person at the investment firm to discuss market abuse suspicions is not arguable. However, this contact person should not be the one in charge of the client relationship, but rather the person who generally deals with regulatory authorities.

For example, in France, the AMF recognises the advantages of having the compliance officer as their first contact for control and investigation matters[5]. Although the authority has the right to communicate with any employee of the intermediary, it has proved more efficient to be able to rely on a point person who organises the gathering of information within the intermediary. AMAFI believes that this set-up should not be jeopardized by providing, at the very first stage of the process, direct access to bank employees.

[5] See "*Charte de conduite d'une mission de contrôle sur place*', AMF, February 2008 update.

Furthermore, with respect to STRs, there is an added risk to contacting the investment firm's personnel, since they may not be aware of the notification. It is therefore unlikely that they would be able to provide further explanation on the case and, on the contrary, such contact would create an additional risk of a leak of information of a sensitive nature.

20. Finally, it is doubtful that providing the conversation tapes can be done within a delay that is unlikely to jeopardize the requirement to "*notify the competent authority without delay*" (*Article 6[9] of the Directive 2003/6*).

⇨ AMAFI therefore calls on CESR to exclude from the list of additional information that should be included in an STR, the identity of the person who has direct contact with the client and the tapes of relevant conversations between the firm and its client.

21. More generally on the subject of confidentiality, AMAFI would welcome some guidance from CESR.

The Directive states (*Directive 2004/72/EC, art. 11*) that "*the person notifying the competent authority (…) shall not inform any other person, in particular the persons on behalf of whom the transactions have been carried out or parties related to those persons, of this notification (…)*". In practice, a firm with operations in several countries faces issues when requesting to one of its remote locations information to assess a suspicion case related to a client of the location. These requests from the Compliance department, which are infrequent for this location, may give some hints that an STR is being prepared to employees who do not need to know about it. The Association would be interested to obtain guidance from CESR as to how to deal with such situations and ensure that the confidentiality of the notification is safeguarded within the notifying party's organisation.

22. As an additional comment, the Association would welcome a common set-up among CESR members that would ensure the anonymity of the institution that declared the STR, when it is used in a prosecution. In France, when an STR is attached to a case, the identity of the reporting entity is not made available.

This set-up is however absent in the case where an STR is transmitted to another competent authority whose judiciary authorities may require its details.

⇨ Due to the commercial risk banks take when reporting suspicions to authorities, AMAFI calls for CESR to ensure that confidentiality of reporting entities is preserved by all Member States, in all cases.

✓ **§ 34 : record keeping**

23. AMAFI is sceptical about the usefulness of recording information gathered by a firm over a suspected case of market abuse that has not been reported to the competent authority. Besides the fact that the Directive does not impose such requirement, there are issues in doing so. This would create yet another record containing personal data, whereas the rationale for doing so is not set in laws and the sensitive nature of this information does not combine well with clients' rights with regard to this information (right to access, amend or oppose to such records).

24. Furthermore, from a practical point of view, such a recommendation is likely to create discrepancies in the way it is implemented among Member States. For example, it is unclear which retention period should apply[6]. As a result, different retention prescriptions would apply depending on the Member State. Similarly, there is no guidance over which elements should be recorded.

⇨ AMAFI therefore calls on CESR to withdraw its proposal to recommend the recording of a suspected case of market abuse that is not notified to the competent authority. If it decides nevertheless to do so, guidance on data that should be retained and applicable retention period should be provided and harmonization at European level should be sought.

[6] For example, in France, one could consider that art. L 621-15 of the Code Monétaire et Financier apply to such records, which states that "*acts older than three years cannot be referred to the Sanctions Commission if, during this period, no action was taken to search for, ascertain or sanction them*." However, one could argue that the retention period applicable to data related to cases of potentially suspicious transactions that have not been reported should be consistent with the one applicable to insider lists, which is of five years (art. 5.4 of the Directive).