Z E N T R A L E R K R E D I T A U S S C H U S S

MITGLIEDER: BUNDESVERBAND DER DEUTSCHEN VOLKSBANKEN UND RAIFFEISENBANKEN E.V. BERLIN · BUNDESVERBAND DEUTSCHER BANKEN E. V. BERLIN
BUNDESVERBAND ÖFFENTLICHER BANKEN DEUTSCHLANDS E. V. BERLIN · DEUTSCHER SPARKASSEN- UND GIROVERBAND E. V. BERLIN-BONN ·
VERBAND DEUTSCHER PFANDBRIEFBANKEN E.V. BERLIN

Comments of the Zentraler Kreditausschuss on the draft third set of CESR guidance and information on the common operation of the Market Abuse Directive to the market

Ref.: CESR/08-274

23 September 2008

In the eyes of the German banking industry, the Market Abuse Directive has been a success since its entry into force in 2004. At the same time, it would be advisable to now review the efficiency of the rules and make corrections where necessary. We therefore welcome CESR's initiative for such a review and wish to comment on the regulatory areas addressed in the draft guidance as follows:

Insider lists

Paragraph 11: The requirement to draw up lists of insiders is now well-established in practice. German credit institutions are subject to this requirement partly as issuers themselves and partly as service providers to other issuers. Institutions also prepare lists of their own in their capacity as service providers. This possibility must be retained in the future as well, particularly as there are also data protection reasons why the personal data of the employees concerned should not be transferred to third parties. With this in mind, consideration could also be given to no longer providing the final option specified by CESR of reporting this data via the issuer.

CESR considers in this connection that the issuer should make any third persons acting on his behalf or for his account aware that all relevant persons are to be included in the insider list. No requirement of this kind follows from the existing rules, however. As current well-established practice shows, there is also no need for such special notice. In principle, the issuer must – like anyone else – be able to rely on existing legal obligations already being known.

Paragraph 12 ff.: In its guidance, CESR would like to see as small a number of employees as possible included in the insider list. While this wish is understandable, it cannot always be fulfilled, particularly in the case of intermediaries, who may have inside information with respect to a large number of issuers. Under German law, there is already an appropriate restriction in that only persons who have access to inside information *in their designated function* must be included in the insider list. This means that employees from, for example, the IT department, who obtain inside information merely by accident or even unlawfully are therefore excluded. We believe that no supervisory rules on the specific form the list should take are additionally required. Whether the list is function- or project-based is something that should be decided by taking into account the way the entity keeping the list is organised. Various solutions are conceivable, provided the persons who have access to inside information are identifiable at any time. There is therefore no recognisable need for regulation.

Paragraph 16: Supervision is increasingly taking place at group level. In the area of securities supervision, home and host country supervisors jointly conduct inspections on the premises of cross-border institutions. As the employees of supervisory authorities themselves cannot be

classified as professionals acting on behalf of the issuer, they are not in our view covered by the rules. We assume that the supervisory authorities have implemented similar internal rules within the scope of their self-organisational powers.

New: Content of the insider list

In addition to the data required to identify insiders such as name, date of birth and address, some supervisory authorities also list private telephone numbers or e-mail addresses. In our view, this practice is both questionable (for data-protection reasons) and unreasonable (because this data is not necessary for identification purposes).

Suspicious Transaction Reports

Paragraphs 27, 34: Suspicious transaction reporting may also be considered to be well-established in Germany. As the starting point for a report under Article 6 rec. 9 of Directive 2003/06/EC is a "transaction" and not simply a customer's intention to conduct one, an executed transaction must be reported in Germany. There is, on the other hand, no requirement to report suspicion beforehand, although this may be done if execution of the transaction in the marketplace is to be expected. No other interpretation is likely to be compatible with the wording of the Directive or of the German Securities Trading Act for that matter.

Paragraph 35: Within the scope of the work of the compliance unit at group level, the responsibility of the parent company's compliance officer makes it necessary to report on notice of suspicious transactions given by a subsidiary. In our view, the possibility to do so is clearly provided for under the MiFID, which allows institutions to organise compliance also at group level. In practice, clarification to this effect would, however, be helpful.

Paragraph 37: The German banking industry continues to reject the introduction of technical reporting mechanisms to detect and identify suspicious transactions. As we see it, the benefit of such mechanisms in some banks is limited, as they can be easily circumvented by a customer acting with intent to manipulate the market by involving several intermediaries. Much more relevant information can, on the other hand, be gathered centrally, e.g. at exchange offices monitoring trading or supervisory authorities themselves. This would also be a much cheaper way of ensuring efficient IT-based market supervision. We therefore welcome it that CESR continues to take the view that the decision on whether to introduce such IT systems should be left to the institutions themselves.