



Association Luxembourgeoise
des Compliance Officers
du Secteur Financier

News Bulletin

N°9

4 DECEMBER 2006

Editorial



Dear friends and members of ALCO,

ALCO resumed business after the summer season, many of us meeting for our traditional social event at the Théâtre de l'Opéra. This gave us the opportunity to carry out an initial analysis of the responses to the questionnaire that we sent out to all our members. A more detailed analysis of the collated information is underway and, we hope, will enable us to meet ALCO members' expectations better.

There were fewer of us, on the other hand, for the two visits ALCO organised: one to the Luxembourg Stock Exchange and one to the European Parliament in Strasbourg. Both of these visits were, however, fascinating in their own way. At the Stock Exchange we learnt many aspects of its history and how it operates, as well as the impending impact of MiFID regulation on the way it is organised. At the European Parliament we were given detailed explanations of its role within the European institutions, its influence, and its methods and had the opportunity to attend a lively plenary session. I would like to thank the Secretary General of the Luxembourg

Stock Exchange and Mrs Lydie Polfer, who was our host at the European Parliament respectively.

In recent months an important event in ALCO's history has taken place: establishment of a partnership with the IFBL for the purpose of training Compliance Officers. The four-module programme has already been a great success.

In the near future we are planning a conference organised jointly with the IRE for the first quarter of next year, which will focus on a topic which concerns all Compliance Officers (and they are not the only ones...): adoption of the MiFID Directive in Luxembourg.

Financial sector compliance officers will have their work cut out. They have to play an active role in implementing MiFID in their institutions, whilst many of them are still in the process of working on the surveillance measures ensuing from the law of 9 May 2006 on market abuses.

This issue of the News Bulletin contains three articles connected with these significant legislative and regulatory developments:

- Marie-France de Pover answers the main questions that arise for a better understanding of MiFID;
- then Nancy Carabin takes stock of obligations arising from the law on market abuses;
- and Sophie Rase's article highlights a certain number of questions raised by banking secrecy legislation.

Finally, as always, the Bulletin provides information and comments on current legislation and aspects of Association life.

Can I remind you that we meet with Marco Zwick on 7 December next at the Hôtel Le Royal to present the joint report by the working group, ABBL and ALFI on "AML Guidelines for Fund Industry".

Looking forward to seeing you soon,

Jean-Marie Legendre
President

Legislative news

Actualités luxembourgeoises

Dépôt le 26 octobre 2006 du projet de loi n°5627 relative aux marchés d'instruments financiers (MIF) et portant transposition de la directive d2004/39/CE du Parlement européen et du Conseil du 21 avril 2004 concernant les marchés d'instruments financiers ;

Actualités européennes

DIRECTIVE 2006/70/CE DE LA COMMISSION du 1er août 2006 portant mesures de mise en oeuvre de la directive 2005/60/CE du Parlement européen et du Conseil pour ce qui concerne la définition des «personnes politiquement exposées» et les conditions techniques de l'application d'obligations simplifiées de vigilance à l'égard de la clientèle ainsi que de l'exemption au motif d'une activité financière exercée à titre occasionnel ou à une échelle très limitée.

Luxembourg News

The bill n°5627 regarding markets in financial instruments and implementing Directive 2004/39/CE of the European Parliament and of the Council of 21 April 2004 as regards markets in financial instruments was introduced on October 26th, 2006.

European News

COMMISSION DIRECTIVE 2006/70/EC of 1 August 2006 laying down implementing measures for Directive 2005/60/EC of the European Parliament and of the Council as regards the definition of 'politically exposed person' and the technical criteria for simplified customer due diligence procedures and for exemption on grounds of a financial activity conducted on an occasional or very limited basis.

MiFID

I. How is MiFID defined?

MiFID is a European framework directive dating from April 2004, which concerns the markets in financial instruments. It replaces the 1993 Directive on Investment Services (ISD), which introduced the concept of the European passport for investment firms. MiFID, the English term widely used to refer to this text, is short for Markets in Financial Instruments Directive. The directive is supported by another directive and a regulation containing more detailed measures for application according to the Lamfalussy process. The latter documents were published on 2 September 2006 in the Official Journal. These provisions are expected to come into force on 1 November 2007.

II. What are MiFID's innovations compared with the ISD?

MiFID introduces a harmonised regulatory framework for financial instruments within the European Union.

By recognising and regulating order execution platforms other than the regulated markets, such as Multilateral Trading Facilities (MTF) and Systematic Internalizers (SI), MiFID intends to increase competition between these. The consequence is the risk of dividing liquidity, which has necessitated the adoption of additional measures such as pre- and post-trade publications with a view to ensuring greater transparency and thus protecting investors' interests and market integrity.

Furthermore, the scope of financial instruments and services covered is extended to commodities derivatives in particular, but above all to investment consulting.

III. What are MiFID's objectives?

Essentially MiFID pursues four objectives.

These primary objectives are:

1. Increasing competition between places of execution and intermediaries by establishing rules relating to places of execution other than the regulated markets, such as MTFs (formerly Electronic Communication Networks) and SIs, i.e. investment firms that execute orders from customers against their own book.

2. Ensuring market integrity by increasing transparency through pre- and post-order execution measures for publication imposed on those executing orders.

3. Strengthening investor protection. In fact MiFID has markedly developed the rules of conduct, which are applied differently depending on the category of customer (retail, professional or eligible counterparty), especially with regard to the information to be furnished by the latter. MiFID thus reinforces the provisions relating to order processing and requires establishment and circulation of a "best execution" policy. By the same token a policy relating to conflicts of interest must be drawn up and notified to customers. The private banking sector in particular is

Bulletin

affected by the requirement for a "suitability" test, which must be carried out for all customers who benefit from advice or whose assets are subject to discretionary management. This third objective may have a potentially significant impact on Private Banking business in particular.

The professionals in question must obtain adequate information in order to draw up a risk profile that fulfils MiFID's provisions. The provision of services may not continue otherwise.

4. Improving cooperation between regulators, in particular by clarifying the features to be considered in the light of the "Home Country Control" principle, and by harmonising the terms for reporting to authorities.

IV. Which are the institutions concerned?

Investment firms, regulated markets and credit institutions offering investment services.

V. What's the situation regarding insurance companies and OPCs?

Insurance companies are firmly outside the scope of MiFID. As far as OPCs, which are clearly financial instruments, are concerned, the matter is governed by MiFID, which specifically excludes OPCs and management companies from its scope. All the same, let's qualify that by stating that this exclusion applies only in the event that the management company does not offer any discretionary management service and does not provide advice.

ALFI is reviewing the question of whether MiFID applies to transfer agents when they carry out transactions for receipt and transmission of orders only.

VI. Does MiFID address other important subjects apart from the above topics: customer categorisation and information, "best execution", transparency, order processing, conflicts of interest, and "suitability"?

Yes, organisation of control functions, including Compliance, and Governance, including outsourcing, retention of customer assets, transaction recording, reporting to the authorities (Stock Exchange and CSSF), and especially "inducements", whose practical applications are difficult to define. According to MiFID, if the latter are not given or received by the customer or one of his representatives, they must be divulged if it can be established that they are designed to improve the quality of service provided. Here we will touch on the impact that a far-reaching interpretation of such norms could have on fund issuers and external managers, in particular.

VII. What are the peculiarities and, specifically, the consequences of customer categorisation? What is meant by "eligible counterparty"?

MiFID makes a distinction between the professional customers listed in Annex II to MiFID (credit institutions, investment firms, OPCs, etc.), which include the big companies if they meet certain criteria, and the retail customers who, by default, are those to whom the greatest protection is accorded. The eligible counterparty, which receives the least protection, constitutes a category of professional to which the investment firm offers reception/transmission and order execution services only. Apart from professionals per se, it is also possible for a retail customer to be recognised as a professional on request, if the size of his portfolio, the number of

Bulletin

transactions carried out by him and his expertise are sufficient. When the Member States have defined certain criteria, it may also be envisaged that a professional describes himself as an eligible counterparty in order to be considered as one on request.

The difficulty lies in the fact that MiFID specifies that customers may change category per service, product, transaction and per financial instrument (opt-in, opt-out options). The change towards less protected status is subject to various formalities.

Referring to the annex to MiFID, we nevertheless understand that banks are at liberty to refuse these changes. In practice, a pragmatic approach will thus be possible, taking into account the nature of the majority of the customers and possible commercial stakes, on pain of having to implement lengthy and costly IT developments. If a change of category is accepted, it would be viewed as a general preference.

VIII. What is the difference between the "suitability" test and that for "appropriateness"?

The suitability test must be used for managed customers or those using consultancy services only. It is based on three broad lines: establishment of the customer's investment aims (risk aversion, risk profile, investment horizon, etc.), his financial circumstances (assets and debts enabling evaluation of the customer's ability to bear the financial risk inherent in the investment) and his knowledge/experience of financial products (degree of familiarity with the instruments in question, frequency and volume of transactions, education, whether or not employed in the financial sector, etc.).

If one is not in possession of these facts, which must be obtained from the customer by 01.11.07, MiFID stipulates that the service may no longer be provided. In theory there is no provision for "grandfathering". It is thus a good

opportunity to quickly put the finishing touches to the risk profiles drawn up on the basis of Circular 2000/15, if need be, taking historical data as a base, as appears to be accepted by the CSSF.

As for the "appropriateness" test, it must be used for customers passing orders (execution only) on complex products (derivatives). We should note that apart from the features listed by the directive, it is not always easy to determine precisely what is a complex product and what isn't. If one acknowledges that a derivative product is complex, what is it if it is chosen for the purposes of hedging and not for speculative purposes? Then again, what about structured products with guaranteed returns?

Whatever it is, the banker must try to obtain all the required information on the customer's knowledge and experience and warn him, either in the event of mismatching between this experience and the choice of product or financial instrument, or because he does not have sufficient knowledge to judge this suitability. Even with these conditions the customer is nevertheless at liberty to continue the transaction if he wishes.

The customer who carries out transactions in non-complex products on his own initiative is not tested, for all that the policy on conflict of interests has to be observed where he is concerned and he has to be informed of the fact that he need not be subjected to a test. The latter control concerns retail customers only, whilst the "suitability" test must be carried out for both retail and professional customers.

If certain aspects of "suitability" (knowledge/experience of markets allowing a personal judgement with regard to the investment and financial capacity to assume risks) may be presumed to have been acquired where a professional per se is concerned, there is wide debate on the question of whether the investment

Bulletin

objectives should be verified. Although literal interpretation dictates a reply in the affirmative, practitioners would like to abandon a requirement which seems to them disproportionate in relation to its aim. According to the ABBL and ALFI the CSSF does not seem to be opposed to this.

IX. On what principles must the best execution of orders policy be based? How must customers be notified of it?

"Best execution" policy must be designed so that it is possible to prove to the customer that within the scope of execution of his orders the policy has consistently enabled him to obtain the best result depending on preselected criteria to which a weighting has been attached (price, costs, probability of execution and settlement, etc.), according to the type of financial instrument in question.

It must be possible to establish compliance with the policy, but it may effectively indicate that any instructions given by the customer are privileged whatever the circumstances.

Where stocks are concerned, so far as good many players agree that the market which achieves this result is usually the most liquid market. Offer and demand being more abundant there, it is the place of execution which generally gives the best price for the least cost. At any rate this is the opinion which seems to be borne out by the AMF and FSA on the basis of considerations issued by the CESR (Committee of European Securities Regulators). If MiFID achieves its objective and the MTFs (Multilateral Trading Facilities) and SIs (Systematic Internalizers) increase, the best place of execution for stock transactions could change in future, hence the importance of regularly updating such a policy and systematically following the results of MTFs and other systematic internalizers in the future.

MiFID allows for the customer agreeing to the order execution policy and for his agreement being express as far as orders relating to stocks admitted for trading on a regulated market are concerned; the bank would execute them outside a regulated market or an MTF (ex. OTC or internalisation).

Under the terms of a document produced jointly with ABBL and ALFI following a meeting with the supervisory authority, it seems opportune to inform customers of this policy between 3 months and 1 month before MiFID comes into force, such that they are able to react to it. Their consent may otherwise be considered to have been obtained tacitly.

X. How can conflicts of interest be managed, a policy established and a list of potential conflicts drawn up?

The list is shaped by the nature of the institution's business. An investment bank and a private bank do not necessarily experience the same problems. Having identified sources of potential conflict, it is doubtless a good idea to consider the probability of risk occurrence, the detriment to the customer of such a conflict and especially the extent to which the corrective action intended to remedy it makes up for the deficiencies identified. Customers will be notified of residual conflicts that have not been resolved before the Directive comes into force, as well as a summary of the policy drawn up in the case in question (context, business, existing measures, efforts made, etc.).

XI. What information is to be supplied to customers, when and how?

The information must be appropriate in all circumstances and must enable the customer to understand the risks relating to his investment. The type of information and method of communicating the latter depend on the type of customer. Distinctions are made depending on whether the customer has to be informed, give his consent or express consent, receive notification of the information or simply obtain it on request. In principle general information will be provided to the retail customer on the company, its services, its strategies, its costs, its policies, the risks inherent in the products, accumulation of funds, etc. before provision of the services. Management services demand additional information on performance, the possible benchmark, reporting terms and frequency. A posteriori the customer will receive reports which will obey different rules according to whether the customer is under management or not.

XII. What can we expect of CESR's work?

CESR has drawn up its programme and plans to address subjects which must be dealt with prior to MiFID coming into force as a priority, to enable consistent adaptation of level 1 and 2 provisions. Thus the transaction reporting requirements must be adopted and harmonised. The aim is still to achieve a common standard, whilst avoiding Member States introducing supplementary provisions that are more restrictive (non-gold plating principle). CESR will then address matters on which the European Commission wishes it to rule, what is known as Level 3 "by cascade", such as the question of whether the pre-and post-transaction transparency obligation should be extended to bonds, for example. It will then be up to CESR, in the company of CEBS (Commission of European Banking

Supervisors) and CEIOPS (Committee of European Insurance and Occupational Pensions Supervisors) to concentrate on greater inter-sectoral convergence. Outsourcing and governance, in particular, will appear on the agenda for these measures, known as "3Level3". Other, more technical or operational subjects, are yet to be defined.

The banking world is hoping and praying for further interpretation of certain aspects which it hopes to see given priority, such as "inducements" or "best execution". It is pleasing to note that CESR's latest agenda has been adapted as a result.

XIII. Taking into account that MiFID is due to come into force in the near future, what are the next steps for adoption of the Directive into national law?

The Member States are called to adopt MiFID in national law by 31st January 2007 at the latest. We already have a draft law intend to adopt MiFID's general measures (Level 1) and are awaiting the Grand Ducal ruling which will adopt the Directive's complementary Level 2 measures, the European regulation being applicable directly as far as Level 2 is concerned. At the same time CESR has commenced work and has proposed a timetable for examining several aspects of MiFID, which stretches to 2009.

XIV. What's the best way to prepare for being MIFID-compliant in November 2007?

There isn't a universal method but, as Jean de la Fontaine said, "No need to run if you start on time". Let's not forget that operating from an offshore centre means it is not always easy to have frequent customer

Bulletin

contact. MiFID represents 200 articles to be adopted in 12 months, so it might be useful to concentrate on the existing situation, to examine the gaps in relation to future requirements, by linking the professions concerned to establishment of "gap analysis" and suitable action plans. As a priority the IT impact must be evaluated. It is, however, possible to avoid a huge, labyrinthine system, at the risk of it all seeming a bit of an anticlimax.

XV. More specifically, what is the Compliance Officer's role before, during and after MiFID?

Before it would be useful to alert management and staff to the forthcoming changes. During, Compliance Officers can help with studying the text and practical implementation of the latter, ensuring that procedures, risk profiles, customer documentation etc. is adapted. He or she should ensure that the scenarios used always match the regulatory developments and CESR interpretation. After, the Compliance Officer should check that controls are implemented and appropriately expedited at the level of the entities directly concerned with MiFID, and he or she will put in place the testing necessary as part of his or her monitoring programme.

XVI. MiFID: a development or a revolution?

A favourable development for the investor totally in keeping with existing principles, whilst further increasing transparency. A possible future revolution where certain major markets are concerned, bearing in mind the competition that has developed between execution platforms, where systematic internalizers could do better than the Stock Exchanges.

It is difficult to predict what the post-MiFID era will have in store for us, taking into account uncertainty that persists to this day on several levels: only the future will tell, but until then we have several matters to prioritise...

M.-F. de Pover

Author's note: the next issue of Bulletin will contain an article on application of MiFID to third party countries.

How should the law of 9 May 2006 on market abuses be applied?

Introduction

The subject of market abuse is of great interest to Compliance Officers if it falls within the scope of topics to be addressed by the Compliance department under the terms of Circular 04/155.

Even before adoption of the European Directive of 28th January 2003 on the subject into Luxembourg law ALCO, having sensed the importance of the topic, published Maitre Schummer's excellent study on the draft Luxembourg law in issue 5 of this Bulletin.

This article does not intend to study all of the proposals contained in the law of 9 May 2006 (hereinafter referred to as the "Law") and CSSF Circular 06/257, which rapidly followed it. It makes no claims to do other than try to spell out how the principal obligations incumbent upon issuers whose securities are admitted for trading on a regulated market located or operating in Luxembourg¹, as well as those to which the banks and PSF are subject, may be fulfilled in practice now.

At any rate this article will not touch on the obligations relating to persons who produce or circulate investment recommendations produced by third parties, or those incumbent upon

¹ Or for which a request for admission to such a market has been submitted.

regulated markets, as well as credit institutions, investment firms and market operators running an MTF.

The Commission de Surveillance du Secteur Financier (CSSF) must soon issue an additional circular on the terms for applying the Law, thus throwing greater light on the subject.

The new requirements provided for by the Law may be divided according to the operator's/contributor's status: market participants subject to specific obligations in addition to the general prohibitions and other personnel to which only the general prohibitions apply.

I. General prohibitions

Under the terms of the Law of 9 May 2006, there is a general prohibition on any person, natural or legal, holding privileged information, using this information to purchase or sell securities covered by this information, communicating this information to a third party and recommending a third party to deal in the financial information covered by this information. It is also forbidden for any person to manipulate the market².

These general prohibitions, constituting offences, apply to all and consequently to employees and directors of banks and PSFs at one and the same time, and also to their customers.

² Manipulation of rates or spreading false information. The offences of insider trading and market manipulation are covered by the generic term of market abuse.

Bulletin

Within the scope of their duty of advice and prevention, Compliance Officers may make every member of staff aware of the problem already, and managers and advisers in particular, by issuing informative memoranda and addressing these topics in internal codes of conduct and through specific training.

Apart from the signs highlighted in Article 3 of the Law, which need not necessarily be considered to constitute market manipulation per se, it may be useful to consult the documents produced by the CESR³, which set out the practices that would be regarded as market manipulation⁴ by the various European regulators on a harmonised basis⁵.

II. Market participants' obligations⁶

1. Obligations incumbent upon issuers of quoted financial instruments

These obligations apply to **issuers** whose statutory seat is established in Luxembourg or abroad, if their securities are admitted for trading on a regulated market situated or operating in Luxembourg⁷.

A. Obligation to publish privileged information

In order to ensure market transparency, issuers must publish the privileged information which concerns them directly⁸ "as soon as possible".

³ Committee of European Securities Regulators.

⁴ Contrary to permitted market practices which stem from each national regulator.

⁵ Market Abuse Directive Level 3 – first set of CESR guidance and information on the common operation of the Directive (04-505b), 11 May 2005, pp. 9 et seq. and Feedback Statement – Market Abuse Directive, Level 3 – first set of guidance and information on the common operation of the Directive (05/274).

⁶ The question of whether the obligations reiterated under point 2 apply to OPCs is not discussed here.

⁷ Or for which a request for admission to such a market has been submitted.

⁸ The aim is to ensure that the information is made available to the public quickly in order to prevent insider

The privileged information must be made public in French, German or English as a minimum, using distribution channels that ensure effective circulation to the public.

In its Circular 06/257 of 17 August 2006 the CSSF made clear that, without prejudice to the issuer's obligations in respect of the market operator, the obligation is met currently if the information is published either in one or more journals published nationally or published widely in Luxembourg, or published on the website of the market operator where the issuer's securities are admitted for trading, or published through specialist financial information agencies (Reuters, Bloomberg, etc.).

Furthermore, the information must be displayed, in French, German or English as a minimum, on the issuer's website for three months. Any significant change having a bearing on the information published previously must be rapidly divulged by the same distribution channel as that used to divulge the initial information.

More detailed publication terms may be stipulated by a Grand Ducal regulation.

It is advisable to synchronise as much as possible the divulging of privileged information to every category of investor, both in Luxembourg and in other countries where the financial instruments are admitted for trading on a regulated market.

Combining the provision of privileged information to the public and marketing of business activities in a misleading manner is prohibited.

trading. In fact insider trading or market manipulation can take place only if a restricted group of persons holds information enabling it to intervene in the financial markets by buying or selling financial instruments before all the other players and without taking risks (notes to article 14).

Bulletin

Publication may, however, be postponed to protect the issuer's legitimate interests⁹ on condition, however, that this omission does not risk damaging public interest and that effective measures ensure strict confidentiality of the privileged information.

Apart from establishing a list of insider traders, the commentary to the Law's articles provides for specific measures to be adopted to guarantee confidentiality of information: the establishment, for example, of "grey lists", of "watch lists"¹⁰ or "restricted lists", implementation of negotiation windows for categories of sensitive persons, surveillance of bank employees' transactions for their accounts, recording of telephone conversations for bank employees who work in the trading room¹¹, recourse to internal codes of conduct or even implementation of Chinese walls.

The issuer must also take the measures necessary so that anyone having access to the privileged information is aware of the legal and regulatory obligations connected with this access and is warned of the sanctions in the event of unwarranted use or dissemination of this information. The issuer must also equip himself with procedures enabling him to publish the privileged information speedily in the event of him being unable to guarantee its confidentiality.

B. Obligation to draw up a list of initiates

The issuer (which may be a bank, for example), or a person acting in the name of and for the account of the latter, draws up a list¹² of persons

⁹ See Article 3 of Directive 2003/124: non-exhaustive list.

¹⁰ A list of securities selected for special surveillance by a brokerage, exchange or regulatory organisation; firms on the list are often takeover targets, companies planning to issue new securities or stocks showing unusual activity (Vector 2000 Stock System definition).

¹¹ Recording of telephone conversations requires prior CNPD authorisation.

¹² Drawing up the list of insider traders constitutes treatment and the CNPD must be notified thereof.

working for it, whether within the scope of a contract of employment or not, and having access, whether regular or occasional, to privileged information concerning it directly or indirectly.

The Law itself can be referred to for determining regular initiates and thus bear in mind that members of the Board of Directors, the Management Committee, members of the Audit and Compliance Committees, as applicable, even the Mixed Enterprise Committee and/or Employees' representatives if they are represented on the Board of Directors, are primary initiates¹³.

Where persons to be regarded as initiates as a result of exercise of their profession or their role are concerned, it is necessary to first ask oneself about the nature of the privileged information itself. Which persons have non-public information of a specific nature regarding the issuer that would be likely to have a significant influence on the security's price, assuming that it were to be published?

It is likely that members of Management, people having access to the issuer's results before publication (accounting, management control), as well as Management secretaries, for example, will be deemed to be initiates because of the position they occupy.

Furthermore, persons called to work on specific files or a confidential project, like an IPO, may be included on an ad-hoc list of occasional initiates.

Provision of services by third parties who are not encompassed by a contract of employment with the issuer (lawyers, auditors, notaries, etc.) must also be noted. It is not enough to give the name of the issuer's

¹³ In the terms of Article 8, §1, para. 1 the members of the issuer's executive bodies, management or supervisory bodies in particular are initiates.

Bulletin

audit firm or lawyer's practice. The names of the employees who possess information concerning the latter must be stipulated.

Once the persons to be listed have been determined, they must be informed that they are included on the list by letter addressed to them personally.

They will be made duly aware of the new applicable legal and regulatory obligations as well as criminal, administrative or disciplinary sanctions provided for in the event of illicit use or illegal circulation of the privileged information to which they have access.

The list will include the initiates' identities (surname, first name, address, date and place of birth, nationality, etc.) as well as the reason for their registration (position, department) and the date the list was created and updated. Taking into account this update requirement, it may be useful if the list is retained by the Compliance Officer of a quoted bank, for example, in order to plan a regulation with the Human Resources Department, under the terms of which the Compliance Officer is notified of any change of address or secondment of personnel in question.

This list must be held for five years at least after creation or updating and must be available to CSSF. It will be transmitted to it by request only.

2. Obligation incumbent on directors/managers

The directors/managers¹⁴ of issuers established in Luxembourg, as well as persons having a close link with them¹⁵ must declare any

¹⁴ Persons exercising managerial responsibilities are members of the issuer's administrative, management or supervisory bodies, and high level officers who have regular access to privileged information directly or indirectly concerning the issuer, and have the power to take management decisions concerning this issuer's future development and corporate strategy.

¹⁵ By person having a close link with the director, the law means the spouse (or similar), dependent children, any other relative sharing the same domicile for at least a year, and any moral person, trust estate or other trust [...]

transactions¹⁶ effected for their own account and relating to the issuer's shares¹⁷ admitted for trading on a Luxembourg or foreign market to the CSSF and the issuer.

Board members, members of various Committees (Management Committee, Audit Committee, etc.) as well as persons having regular access to privileged information concerning the issuer and the power to take management decisions concerning the issuer's future development and corporate strategy all fall within the scope of this new obligation.

Issuers, which may be quoted banks, coming within the text's scope will on the one hand take care to make their directors aware of the significance of this new obligation and, on the other, to implement a system for publishing declarations, more often than not via their website (in French, German or English).

The declarations are to be made within five working days following the transaction and must include the following information: the issuer's name, the name of the natural or legal person conducting the transaction or that of the person having a close link with the director/manager whose name is stated as applicable; the grounds for the compulsory notification, description of the financial instrument, the nature of the transaction (purchase or sale), the date and place of the transaction, the price per security and the total value of the transaction.

whose directorial responsibilities are exercised by a director, or which is directly or indirectly controlled by him, or which is constituted for his benefit [...]

¹⁶ It seems that the definition of the term "transaction" is subject to interpretation.

¹⁷ Or to derivatives or other financial instruments linked to these shares such as options, warrants, convertible bonds, etc.

Bulletin

To date the CBFA and AMF¹⁸ have issued standard forms for reference.

3. Obligation to notify suspicious transactions

Henceforth, following investigation on a case-by-case basis, banks and financial sector professionals established in Luxembourg¹⁹ will be obliged to notify transactions that they reasonably suspect of representing a market abuse immediately.

It ensues from European texts²⁰ that the period only starts to run once the professional has acquired information substantiating the existence of a market abuse, suspicion alone is not enough. It is necessary to be able to put forward serious motives.

The notification requirement does not entail the obligation for professionals to check every transaction, but they should have at their disposal methods enabling them to determine which transaction may be regarded as suspect. According to the CESR²¹ "investment firms and credit institutions should not only notify transactions they consider as suspicious at the time the transaction is carried out but also any transactions which might become suspicious in the light of subsequent events. However, this does not mean that they are required to go back and retroactively review transactions in the run up to that event or development."

If it is thus recognised that systematic verification of transactions is not required, the fact remains that in the interests of professionals there is a duty of surveillance. It will be

¹⁸ Forms available from www.cbfa.be and www.amf-france.org

¹⁹ This declaration obligation also exists for regulated markets, credit institutions, investment firms and operators running an MTF in Luxembourg; (article 27, §3).

²⁰ Preamble 9 of the Directive 2004/72.

²¹ See document quoted below, pp. 14 et seq.

essential for the outcome of analyses to be retained, as with any Compliance matter.

It is important to draw the attention of entities at risk (trading room, dealers etc.) to the fact that it is essential they report their suspicions to Compliance for investigation, in order to enable the latter to declare the suspicions to the CSSF as applicable. With this in mind it may be opportune to provide personnel with specific training and to stipulate the information to provide in the event of suspicions, with the help of a suitable form, for example.

The professional in question may avail himself of the declaration forms offered by the Belgian or French supervisory authorities or that prepared by CESR²² directly before notifying the CSSF and before he has more detailed information at his disposal.

Conclusion

This subject, some aspects of which are new, raises numerous questions which the present article does not address. The forthcoming CSSF circular will be especially valuable as a result. The only purpose of these reflections is to provide Compliance Officers who are confronted now with complying with these obligations pertaining to issuers and banks/PSFs, which came into force several months ago, with temporary assistance.

There is no doubt that further experience likely to be gained in future and subsequent questions that will arise will fuel the debate and, perhaps, to give rise to jurisprudence which will make it easier to detect the limits of the new constraints.

Nancy Carabin

06.11.06

²² www.cesr.org

Refreshing Memory on Banking Secrecy

In this article, we will detail the current legislation regulating the banking secrecy specific to Luxembourg. We will also try to cast some light on the practical application of banking secrecy for professionals of the financial sector in Luxembourg.

The Rules of the Game in a Nutshell

Credit institutions and other Professionals of the Financial Sector (“PSF”) are bound to professional secrecy as detailed under article 41 of the law of 5 April 1993 on the financial sector as modified (“the Law”).

The information these entities hold on their clients is generally available to all directors (whether in Luxembourg or not), managers, employees and supervisory bodies.

General, non-nominative, information is also available to shareholders or partners for the purpose of sound and prudent management (the information may not provide detailed information on specific client relationships).

All information may be accessed by the group internal audit body for the overall management of legal or reputational risks connected to money laundering or the financing of terrorism.

Article 41 also provides that information

- may be revealed where the law requires or authorises it, or
- may be revealed to national or foreign supervisory authorities when acting within their competency and under their own professional secrecy, or
- may be revealed to professionals listed under articles 29-1,29-2,29-3 of the Law (communication agents,

administrative agents, IT systems operators) under a service agreement.

Any information held by credit institutions or PSF on their clients if passed on to individuals or entities other than those listed above is a breach of banking secrecy and is subject to article 458 of the Penal Code. This may entail 8 days to 6 months imprisonment sentence and a fine of between 500 Eur to 5000 Eur fine.

Where does Client Consent Start and Banking Secrecy Stops?

The Commission de Surveillance du Secteur Financier (“CSSF”) issued a note on 1 March 2004 prepared by its legal expert committee analysing the banking secrecy requirements for PSF, the public order character of banking secrecy and specifically to what extent, information provided to a professional may be transferred to a third party with the client’s consent or at the client’s request.²³

Public Order?

The CSSF stated that all obligations where a criminal sanction is prescribed for non compliance, are by their nature of public order²⁴ (regardless of whether the protected interests are of public or private nature) and that according to article 6 of the civil code, no private agreement may depart from laws effecting public order.

Client Consent or Client Request?

A professional must ensure that when a client requests that information be communicated to third parties, it does not infringe article 41 of the Law and does not renounce to the protection of the Law.

According to the CSSF, it is sometimes difficult to distinguish between “permissive consent” and “agreed renunciation”.

²³ CSSF annual report 2003, Appendices pages 195-209- Accessible on CSSF website www.cssf.lu

²⁴ This reflects the doctrinal position of the CSSF- This position is not always agreed with by other doctrines in Luxembourg. The public order status of banking secrecy is a highly controversial subject.

Bulletin

Because of the public order characteristic of banking secrecy, an agreement by which the

protected person would renounce, in advance and in general to the protection of the law would be void.

The CSSF adds that the request from the client to communicate information to a third party (allowed under certain conditions) is very different from the consent from the client to transfer information to a third party at the third party's request (which is not allowed as it would mean renouncing the very principle of secrecy).

The protected person's request to the transfer of information should fulfil two conditions:

- The transfer of information should always be **in the interest of the protected person only** (not in the interest of the professional). The protected person is the "Master of the Secret" and the protection of his/her information should not be a constraint or impediment for a client to do business. Transfer of information must always be requested by the client.
- The client request must be **specific** (vs. general).

It must be specific as regards to the content of the information (what information exactly the client allows the transfer of). A general consent allowing the transfer of "all and any information" would be void.

It must be specific as regards to the intended addressee of the information (to whom exactly may the information be transferred). A general consent to "whoever requests" the information would be void.

It must be specific as regards the purpose for which the client wishes the information to be transferred. The professional must know the reason why the client requests that his information be transferred to a third party.

It must be specific in time: The consent to transfer information should not be for an indeterminate period.

Not all of those conditions have to be met (non cumulative). The professional must make its own opinion as to whether the consent is in the interest of the client and sufficiently specified.

But Surely, Information May Freely be Transferred Intra Group?

Many financial institutions wish that information could be more freely transferable within their group for proper group management of client databases, accountancy, IT, or even the fight against money laundering.

According to the CSSF the only practical way to deal with this is to use the outsourcing possibility organized by the law of 2 August 2003, whereby a professional may outsource certain administrative services under a service agreement to other professionals (which must be CSSF licensed) and which are themselves subject to banking secrecy. In practice, where professionals have several entities **within Luxembourg**, the CSSF appears to accept that a client, who would be client of more than one of those entities, renounces the benefit of the secret between such entities, as it is in the best interests of the client who would otherwise suffer from lack of communication between the entities. This does not extend to cross border group entities, although the result (client suffering from lack of internal communication) would be the same.

Holding the Secrets under a Mandate Agreement?

In 2005, two authors have looked at banking secrecy in relation to a mandate contract.²⁵

²⁵ Le secret bancaire luxembourgeois face au mandat dans la perspective du banquier, Christophe Liebertz et Carole Schmidt, Arendt & Medernach, ALJB-Bulletin Droit et Banque, Hors Série-Juin 2005, pages 37-56.

Bulletin

They seem to agree that a client may give instruction to a professional to transfer information the professional holds on the client to a third party, but it is essential that the request comes from the protected person directly.

Two types of mandate contracts may exist: Either the client has asked a mandatary to act on his behalf in relation to the professional, or the client has asked the professional to act as mandatary in relation to a third party.

In both cases the four conditions for a mandate to be valid must be fulfilled:

- capacity of the client to enter into a mandate;
- consent which must be certain/clear and not forced (however it may be unwritten and tacit);
- the object of the mandate must be certain and possible;
- the cause or purpose must be lawful and not against public order.

In the case where the client has asked a mandatary to deal with the professional, once the professional has ensured that a proper mandate is in fact in place, it can consider the mandate to be within the “sphere of discretion” of the client and therefore information on the client may be transferred to the mandatary by the professional without breaching banking secrecy.

In the case where the client has asked the professional to act as mandatary in relation to a third party, a proper mandate must be in place with clear and defined limits where the client expressly instructs the professional to transfer information to a specific third party for specific purposes.

Specific Concerns for Domiciliation Agents

From the point of view of domiciliation agents, a category of PSF, some specific areas of concern may be identified.

Domiciliary agents provide registered addresses as well as ancillary administrative services to companies under a domiciliation agreement.

Domiciliation agents, as PSF, are covered by banking secrecy and must identify the beneficial owners but also all members of the body of the companies they domicile (directors or “gérants”, shareholders, “commissaires aux comptes”, etc) which information must remain secret.

Here are two examples of practical situations where the question of banking secrecy might arise:

-Let's take for instance a Luxembourg company domiciled with the agent, at the agent's registered address. The domiciliation agent provides in-house directors to the client's company. The domiciliation agent has identified all relevant parties in accordance with Luxembourg law. The client subsequently requests that the company opens a bank account in Luxembourg. The directors will resolve to open a bank account and appoint signatories to operate it. However the domiciliation agent is bound by professional secrecy. Can the domiciliation agent transfer the confidential information it holds on the beneficial owner of the domiciled company to the bank without breaching banking secrecy? The client himself could not open the bank account in the name of the company as he does not represent the company, only the directors are allowed to do so. No bank account will be opened without providing the bank with full due diligence on the ultimate beneficial owner so it seems unavoidable that the due diligence held by the domiciliation agent is transferred to the bank without breaching banking secrecy. Ultimately, the domiciliation agent can only protect itself by ensuring that the injunction to open the bank account was provided by such beneficial owner, whom by doing so is also requesting the domiciliation agent to transfer his confidential information to the bank.

Bulletin

-The same domiciled company has a trading activity, a VAT number and files VAT returns. The VAT authorities, while

doing an investigation, wish to verify the books of the domiciled company. However as the premises of the domiciled company are also the premises of the domiciliation agent (who is bound by banking secrecy), would the domiciliation agent be (1) obliged under article 40 of the Law (“Duty to cooperate with the authorities - Credit institutions and other professionals of the financial sector, must to the fullest extent possible, provide an answer to and cooperate with all legal requests addressed from the authorities responsible for the application of the law in the exercise of their duties”) or (2) authorised under 41 (2) of the Law (“The requirement for secrecy ceases when the disclosure of information is authorised or imposed by or because of the a legal provision, even when prior to the present law”) to give access to the VAT authorities? For any company, the VAT authorities are allowed to do so under article 70 and 71 of the law of 12 February 1979 on VAT.

What Should Professionals Do (or not Do)?

There have been many court cases in Luxembourg where even with the client request, banks have been charged with breach of professional secrecy because for instance the transfer of information was not in the client’s best interest. Also there is increasing pressure on Luxembourg from other EU member states who do not have such levels of protection, and who see banking secrecy as a conflict of law and an impediment to the proper handling of judicial procedures especially in the field of taxation.²⁶

Because of the grey areas that still remain (and where even the supervisory authority feels necessary to attempt clarifying the

situation), the conclusion is that revealing information on a client for a Luxembourg professional is a judgement call. The

professional must “make an opinion taking into account all elements, even with the client request, and ask itself *ex-ante* whether the instruction received from the client exonerates the professional from its banking secrecy obligations *ex post*”.²⁷

Finally, let’s not forget that clients are eager to do business in Luxembourg, inter alia, because of the protection of banking secrecy. Clients as well as professionals should bear in mind that banking secrecy in Luxembourg is a “package deal” with its up sides and downsides to deal with.

Sophie Rase
Compliance Officer

Maitland Luxembourg S.A.

Disclaimer: This article is for information purposes only and is not intended to constitute legal advice.

²⁶ Lemmer, Joé. - Le secret bancaire et la lutte anti-blanchiment : l'arsenal législatif luxembourgeois / par Joé Lemmer, Jérôme Bach. - In: Feuille de liaison de la Conférence Saint-Yves. - Luxembourg. - N° 105 (sept. 2003), p. 31-51.

²⁷ CSSF annual report 2003, op.cit., page 201.

Vie associative/Association activities

VIE ASSOCIATIVE

ASSOCIATION ACTIVITIES

GROUPES DE TRAVAIL ACTUELS:

CURRENT WORKING GROUPS:

A. SECTEUR TRANSVERSAL:

A. CROSS-SECTOR:

Groupe de travail 16

Commission permanente juridique et relations publiques / site internet

Responsable Karine VILRET-HUOT
Téléphone (+352) 26 44 14 13
kvilret@vilret-avocats.com

Responsable internet Olivier GILSON
Téléphone (+352) 49 49 30 888
olivier.gilson@sanpaoloam.lu

Working group 16

Legal and public relations / internet site

Owner Karine VILRET-HUOT
Telephone (+352) 26 44 14 13
kvilret@vilret-avocats.com

Internet Owner Olivier GILSON
Telephone (+352) 49 49 30 888
olivier.gilson@sanpaoloam.lu

Groupe de travail 27

Formations IFBL

Coordinateur Rob SONNENSCHNEIN
Téléphone (+352) 31 99 11 450
r.sonnenschein@vanlanschot.lu

Working group 27

Training IFBL

Coordinator Rob SONNENSCHNEIN
Telephone (+352) 31 99 11 450
r.sonnenschein@vanlanschot.lu

Groupe de travail 28

MiFID

Coordinateur Evelyn MCHALE
Téléphone (+352) 48 88 96 21
evelyn.mchale@hsbcib.com

Working group 28

MiFID

Coordinator Evelyn MCHALE
Telephone (+352) 48 88 96 21
evelyn.mchale@hsbcib.com

Groupe de travail 29

Abus de marché

Coordinateur Cyril MATTHIEU
Téléphone (+352) 40 46 46 400
cyrilmatthieu@lu.hsbc.com

Working group 29

Market abuse

Coordinator Cyril MATTHIEU
Telephone (+352) 40 46 46 400
cyrilmatthieu@lu.hsbc.com

B. SECTEUR BANCAIRE:

Groupe de travail 04

Lutte contre le blanchiment dans le secteur de la banque privée

Responsable Patrick SCHOTT
Téléphone (+352) 46 71 71 400
pschott@pictet.com

Groupe de travail 10

Contrôles de compliance

Responsable Patrick CHILLET
Téléphone (+352) 40 65 40 584
p.chillet@ing.lu

C. SECTEUR FONDS:

Groupe de travail 18

Compliance relative aux investissements alternatifs

Responsable Jean-Marie FOURQUIN
Téléphone (+352) 26 27 16 1
jmfourquin@alternativeleaders.lu

Groupe de travail 21

Interprétation pratique des restrictions d'investissements de fonds

Responsable Tim WINFIELD
Téléphone (+352) 34 10 23 85
tim.winfield@jpmorganfleming.com

D. SECTEUR ASSURANCE:

Groupe de travail 12

Lutte contre le blanchiment dans le secteur des assurances

Responsable Gérard ZOLT
Téléphone (+352) 22 51 51 342
gerard.zolt@kpmg.lu

Groupe de travail 13

Compliance et intermédiaires

Responsable Bruno GOSSART
Téléphone (+352) 24 18 58 51 60
b.gossart@fortis.lu

Groupe de travail 14

B. BANKING SECTOR:

Working group 04

Anti-money laundering in private banking

Owner Patrick SCHOTT
Telephone (+352) 46 71 71 400
pschott@pictet.com

Working group 10

Compliance controls

Owner Patrick CHILLET
Telephone (+352) 40 65 40 584
p.chillet@ing.lu

C. FUNDS SECTOR:

Working group 18

Compliance for alternative investments

Owner Jean-Marie FOURQUIN
Telephone (+352) 26 27 16 1
jmfourquin@alternativeleaders.lu

Working group 21

Practical interpretation of fund investment restrictions

Owner Tim WINFIELD
Telephone (+352) 34 10 23 85
tim.winfield@jpmorganfleming.com

D. INSURANCE SECTOR:

Working group 12

Anti-money laundering in insurance

Owner Gérard ZOLT
Telephone (+352) 22 51 51 342
gerard.zolt@kpmg.lu

Working group 13

Compliance and intermediaries

Owner Bruno GOSSART
Telephone (+352) 24 18 58 51 60
b.gossart@fortis.lu

Working group 14

Bulletin

Statut du compliance officer dans le secteur des assurances

Responsable Benoît MARTIN
Téléphone (+352) 45 67 30 49 54
benoit.martin@paneurolife.com

Status of the compliance officer in insurance

Owner Benoît MARTIN
Telephone (+352) 45 67 30 49 54
benoit.martin@paneurolife.com

Coordinateur groupes de travail / Working groups coordinator:

Rob Sonnenschein
Téléphone (+352) 31 99 11 450
E-mail r.sonnenschein@vanlanschot.lu

MEMBRES ET VIE ASSOCIATIVE:

Nombre de membres (au 30/09/2006):

Banques	128
Fonds	79
Fonds / Banques	36
Assurances	40
Consultants / Réviseurs	27
Admin. et domiciliation de sociétés	10
Avocats	6
PSF	9
Gestion de fortune	3
Autres	9
Effectif total:	347
Membres effectifs	283
Membres d'honneur	64
Effectif total:	347

MEMBERS AND ASSOCIATION ACTIVITIES:

Number of members (as per 30/09/2006):

Banking sector	128
Funds sector	79
Funds / Banking sector	36
Insurance sector	40
Consultants / Auditors	27
Admin. and company domiciliation	10
Law firms	6
SFP	9
Asset management	3
Other	9
Total number:	347
Active members	283
Honorary members	64
Total number:	347

Réunions et activités:

Mensuellement	Réunions du conseil d'administration
7/12/2006	Déjeuner conférence de Marco Zwick "AML Guidelines for Fund Industry"

Meetings and activities:

Monthly	Board meetings
12/7/2006	Lunch- Conference Marco Zwick "AML Guidelines for Fund Industry"



Association Luxembourgeoise
des Compliance Officers
du Secteur Financier

Secrétariat de l'ALCO:

Johanny LICK
Téléphone (+352) 47 67 26 12
Fax (+352) 47 67 36 12
E-mail Johanny.lick@ca-luxembourg.com
Adresse B.P. 1104
L-1011 Luxembourg

Secrétariat du bulletin:

Coralie CZERWINSKI
Téléphone (+352) 26 44 14 13
Fax (+352) 26 44 15 14
E-mail cczerwinski@vilret-avocats.com

Comité de rédaction / Drafting committee:

Karine VILRET-HUOT, Marie-France DE POVER, Leen BOM, Olivier GILSON, Jean-Marie LEGENDRE, Philippe SCHNEIDER, Patrick SCHOTT

Visitez notre site / Visit our website: www.alco.lu
