



Association Luxembourgeoise  
des Compliance Officers  
du Secteur Financier

# Le Bulletin d'informations

N°20

OCTOBRE 2010

## Editorial



Chers membres de l'ALCO, chers amis lecteurs,

De par son métier le Compliance Officer est amené à s'intéresser à de nombreux sujets, aussi diversifiés que l'est l'activité financière ou para-financière de la place. Le bulletin de l'ALCO dont la rédaction est coordonnée par le GT 16 devient de plus en plus représentatif de cet élargissement de vos centres d'intérêt.

Les articles consacrés au secret bancaire et à sa levée pour défendre les intérêts patrimoniaux de la Banque, à la lutte contre le blanchiment dans les casinos ainsi qu'à la Directive, encore à finaliser, sur les fonds d'investissements alternatifs (AIFMD) portent sur des thèmes représentatifs de cette diversité.

Les tables rondes organisées avec succès depuis un an par le GT 34 démontrent également votre demande de partager votre expérience, vos questions et vos idées. Celles consacrées aux abus de marché et aux produits d'assurance-vie liés à des fonds d'investissements ont une fois de plus montré à quel point les solutions en matière de Compliance sont variées selon le métier et la dimension des entités appelées à intervenir.

# Le Bulletin

Le GT 33 reçoit beaucoup de questions encore plus diverses. Les réponses sont transmises directement et les plus générales sont reprises dans le bulletin. C'est cette fois le cas des conditions d'équivalence des « Appointed Representatives » établis au royaume Uni et au traitement des opérations de la journée par le back office.

Bonne lecture à toutes et tous.

Jean Noël Lequeue  
Président de l'ALCO

\* \*

## Articles

### **LA DEFENSE DES INTERETS PATRIMONIAUX DE LA BANQUE et LE SECRET BANCAIRE**

Quels que soient les débats politiques dont il fait l'objet, le secret bancaire constitue dans un pays à système libéral une préservation nécessaire de la sphère privée et une non-ingérence de l'Etat dans les affaires privées.

Le secret bancaire est, du point de vue juridique, - en dépit des attaques et contestations dont il fait l'objet - un des fondamentaux de la place financière luxembourgeoise. A tel point que les professionnels concernés lui confèrent un caractère absolu (1), et dont les conditions de levée restent d'interprétation stricte par les tribunaux nationaux, ne manquant pas de protéger, le cas échéant, les Intérêts privés concernés (2).

#### 1. Le secret bancaire : Pierre angulaire de la place financière

L'article 41 de la loi modifiée du 5 avril 1993 relative au secteur financier définit le secret bancaire comme suit:

« Les administrateurs, les membres des organes directeurs et de surveillance, les dirigeants, les employés et les autres personnes qui sont au service des établissements de crédit, des autres professionnels du secteur financier, des organes de règlement, des contreparties centrales, des chambres de compensation et des opérateurs étrangers de systèmes agréés au Luxembourg visés à la partie I de la présente loi, sont obligés de garder secrets les renseignements confiés à eux dans le cadre de leur activité professionnelle. La révélation de tels renseignements est punie des peines prévues à l'article 458 du Code pénal.

L'obligation au secret cesse lorsque la révélation d'un renseignement est autorisée ou imposée par ou en vertu d'une disposition législative, même antérieure à la présente loi. »

En d'autres termes, le secret bancaire luxembourgeois impose notamment aux mandataires sociaux, aux dirigeants et employés de(s) banque(s) luxembourgeoise(s) une obligation de non divulgation des informations relatives aux clients de ceux-ci, y compris en cas de rupture des relations contractuelles entre les clients et la banque ou encore à l'égard de personnes rencontrées dans le cadre de l'exercice des activités des professionnels concernés.

La législation et la jurisprudence luxembourgeoises ne permettent pas, en l'état actuel du droit, de qualifier avec certitude la nature du secret : d'ordre privé, d'ordre public, voire relevant de l'intérêt général.

Tant que le droit positif n'aura pas tranché cette question, les courants doctrinaux de conception stricte ou libérale continueront de se confronter sur la portée exacte du secret bancaire.

# Le Bulletin

En revanche, le point sur lequel les auteurs semblent s'accorder est que si le secret bancaire constitue une des pierres angulaires de la place financière luxembourgeoise, il ne saurait être absolu.

## 2. Le secret bancaire luxembourgeois n'est pas absolu

Comme l'indique l'article 41 de la loi modifiée du 5 avril 1993 mentionné ci-avant, l'obligation au secret cesse lorsque la révélation d'un renseignement est autorisée ou imposée par ou en vertu d'une disposition législative ; dans ces cas, le secret bancaire peut être légitimement levé.

Outre les cas légaux permettant la levée du secret bancaire, l'étude de la jurisprudence permet de cerner des cas de levée du secret bancaire non expressément visés par la loi, permettant de délier le banquier de son obligation au secret.

### ▪ Si l'on se place du côté du client du banquier :

La Jurisprudence a confirmé une pratique de place qui permet au client d'une banque de délier cette dernière de ses secrets dès lors qu'elle en reçoit l'instruction spécifique, sous réserve de conditions très strictes posées par la CSSF<sup>1</sup>. L'idée sous-jacente étant que le client est « *maître de son secret* »<sup>2</sup>, sans autre justification qui serait fondée sur une disposition législative. En effet une telle renonciation du client au secret ne se justifie ni par l'effet de la loi, ni par l'état de nécessité ; il ne l'est que de la volonté expresse de ce client dans le cadre de son intérêt privé. Ceci est, par exemple, d'application pour les situations fréquentes auxquelles sont confrontées les banques intervenant sur le marché de la Norvège et du Brésil, où la banque - agissant comme nommée/détentrice des titres pour compte de clients - est amenée à dévoiler l'identité du détenteur réel afin de ne pas subir un traitement fiscal discriminatoire, voire des pénalités. Dans ce cas, le client est amené à délier la banque de son secret.

### ▪ Se plaçant maintenant du côté de la banque :

Si la banque est en situation de conflit, alors la question peut se poser de la possibilité pour le banquier de lever le secret bancaire en dehors de l'autorisation expresse de son client.

Si le banquier est assigné devant les tribunaux, dans le cadre d'un contentieux l'opposant à un client, dans ce cas, la défense des intérêts patrimoniaux d'une banque ne constitue-t-elle pas un intérêt légitime pouvant justifier la levée du secret ?

La jurisprudence luxembourgeoise s'est prononcée, dans de rares décisions, sur cette question.

La réponse est apportée dans une ancienne décision du Tribunal d'Arrondissement de Luxembourg en date du 26 juin 1981, n° 552/81. En l'espèce, le Tribunal s'est prononcé, dans le cadre d'un différend opposant une banque à un de ses clients, en faveur de la légalité de la levée du secret bancaire par un établissement de crédit dès lors que ses intérêts patrimoniaux sont menacés, sous réserve du respect du principe de proportionnalité selon lequel les informations révélées doivent se limiter à ce qui est strictement indispensable pour la défense des intérêts dudit établissement de crédit.

L'attendu de principe Indique que « *La doctrine est unanime à admettre que l'intérêt légitime du banquier lui permet de dévoiler certaines informations. Que la jurisprudence suit cette opinion*

---

<sup>1</sup> Voir rapport annuel de la CSSF 2003

<sup>2</sup> Trib.Lux. 24 avril 1991 P. 28, 173

# Le Bulletin

*en admettant la révélation de certaines informations si les intérêts de la banque l'exigent » (arrêt Tournier/National Provincial and Unionbank) ».*

La condition essentielle posée par le juge est l'intérêt légitime de la banque : il est « l'intérêt qu'il a à se défendre en cas de conflit qui l'oppose à son client »; « Dans ce cas le banquier peut dévoiler le secret auquel il est normalement lié. »

Le juge explique expressis verbis : « Refuser la possibilité au banquier de révéler des secrets en cas de conflit l'opposant à son client serait le priver des moyens de sa propre défense et l'exposer à de graves préjudices ».

En substance, la levée du secret dans un contexte contentieux est légalement admissible des lors que les conditions suivantes sont cumulativement réunies :

- Il faut une mise en cause des intérêts patrimoniaux du banquier (la possibilité d'un dommage moral ne suffit pas) ;
- la divulgation du secret ne peut se faire que dans le cadre d'une procédure contentieuse ;
- la divulgation doit se limiter aux nécessités de la défense des intérêts patrimoniaux en application du principe de proportionnalité.

Cette jurisprudence de 1981 a été récemment reprise. En effet, de récentes affaires se sont plaidées devant les tribunaux luxembourgeois<sup>3</sup> portant notamment sur l'opposabilité du secret bancaire par les prestataires de services (tels que les agents teneurs de registre des Investisseurs) agissant pour le compte d'organismes de placement financiers (OPC) permettant ainsi à ces derniers de pouvoir s'opposer à diverses communications de pièces et documents contractuels.

Bien qu'il s'agisse de décisions de référé, et que leur enseignement doive en être mesuré, il y a quand même lieu de noter que le Président du Tribunal d'arrondissement a repris les termes de cette jurisprudence de 1981 en rappelant le principe selon lequel la levée du secret bancaire peut s'avérer nécessaire à l'exercice par les établissements de crédit et les professionnels du secteur financier de leurs droits de la défense en observant le principe de la proportionnalité par rapport à leur intérêt, à celui du client et au respect du caractère absolu du secret.

Ces solutions de bon sens permettent ainsi aux banques, dans le respect des secrets confiés par leurs clients d'une part, et l'intérêt légitime de ces dernières d'autre part, de pouvoir exercer leurs droits de la défense préservant ainsi la sphère privée.

Karine Vilret-Huot  
Avocat aux Barreaux de Paris et de Luxembourg  
Vilret-avocats

---

<sup>3</sup> Ordonnance de référé du président du Tribunal d'Arrondissement de Luxembourg en date du 4 mars 2009 AFORGE –Sicav Luxalpha

## ***La lutte contre blanchiment dans les casinos.***

L'histoire et les fondements des jeux de hasard sont très différents à travers le monde. Les racines criminelles des casinos de Las Vegas, de Russie, des pays de l'Est, de l'Asie notamment avec Macao, Amérique du sud et Europe n'ont pas favorisé leur réputation et ont conduit à une évolution très variée de ce secteur d'activité, de son fonctionnement et de sa réglementation.

En Europe, l'industrie des casinos est sans doute aujourd'hui une des plus régularisées et contrôlées. Les recommandations du GAFI transposées en lois européennes et nationales essaient de couvrir toutes les situations et tous les dangers qui peuvent se trouver dans les casinos du monde entier.

En effet, les casinos sont par définition des institutions non financières mais qui offrent néanmoins des services similaires les rendant vulnérables face à des risques de blanchiment. Lors de sa visite, un client du casino peut effectuer plusieurs opérations financières que ce soit au moment de l'achat de jetons, pendant le jeu ou au moment de l'encaissement de ses gains. Il peut échanger des devises ou effectuer un achat de jetons ou de plaques de jeu en utilisant une carte bancaire. Il est possible également de se faire établir un chèque, de demander un transfert électronique depuis ou vers un compte de dépôt d'un autre casino du même groupe et ce, en dehors du circuit financier traditionnel ce qui en fait des cibles potentielles idéales pour les blanchisseurs.

Les casinos peuvent également être perçus par les criminels comme des lieux de rencontres privilégiés compte-tenu de leur environnement de haute sécurité bénéficiant de systèmes de surveillance très performants, ces derniers n'ont aucune crainte à avoir quant à leur propre sécurité. De plus, certains réseaux criminels voient les casinos comme un lieu de commerce idéal puisque certains clients peuvent avoir des besoins d'argent immédiats et dès lors, n'hésitent pas à avoir recours à un crédit à un taux exorbitant.

La majorité des transactions financières citées précédemment sont d'office exclues par la législation européenne et luxembourgeoise du fait de leur législation et réglementation très strictes mais aussi du contrôle quasi permanent de l'autorité de contrôle des jeux.

Par rapport aux autres secteurs privés, l'application des obligations en matière de prévention du blanchiment et du financement du terrorisme est reflétée par un suivi très proche des autorités de vigilance, puisque les casinos sont souvent eux-mêmes très proches des Etats et du contrôle étatique.

Le plus grand danger proviendrait du fait que des réseaux criminels parviennent à se procurer le droit d'exploiter un casino par le biais d'une licence ou de l'acquisition de parts. Les tentatives pour contrôler un casino ou au moins une partie de ses activités vont dans la même direction. En effet, l'argent sale serait tout simplement rajouté à la caisse chaque jour et déclaré comme gain pour le casino, et provenant donc de pertes des clients. En Europe, ce montage paraît très difficile si l'on se réfère à la 3<sup>ème</sup> directive anti-blanchiment :

*« Lorsqu'elles accordent, sur le plan national, l'immatriculation ou l'agrément à un bureau de change, à un prestataire de services aux sociétés et fiducies ou à un casino, les autorités compétentes devraient s'assurer de l'aptitude et de l'honorabilité des personnes qui dirigent ou dirigeront effectivement ces entreprises et de leurs bénéficiaires effectifs. Les critères d'aptitude et d'honorabilité devraient être définis, conformément au droit national. Ils devraient à tout le moins répondre à la nécessité de protéger ces entités contre tout détournement par leurs gestionnaires ou bénéficiaires effectifs à des fins criminelles.*

*(...) Les États membres prévoient que les bureaux de change et les prestataires de services aux sociétés et fiducies sont agréés ou immatriculés et que les **casinos** doivent obtenir une licence pour pouvoir exercer légalement leur activité. Sans préjudice de la future législation communautaire, les États membres prévoient que les sociétés de transfert de fonds sont agréées ou immatriculées pour pouvoir exercer légalement leur activité. Les États membres exigent des autorités compétentes qu'elles refusent l'agrément ou l'immatriculation des entreprises mentionnées au paragraphe 1 lorsqu'elles ne sont pas convaincues de l'aptitude et de l'honorabilité des personnes qui dirigent ou dirigeront effectivement ces entreprises ou de leurs bénéficiaires effectifs ».*

L'article 10 (1) de la même directive donne une obligation supplémentaire aux casinos: « *Les États membres imposent l'identification et la vérification de l'identité de tous les clients de casinos qui achètent ou vendent des plaques ou des jetons pour un montant de 2.000 EUR au moins* ». Par ailleurs, il faut rappeler qu'au Luxembourg les casinos sont soumis à la loi modifiée du 12 novembre 2004 ainsi qu'au Règlement Grand-ducal du 1er février 2010 sans oublier la circulaire 20/08 de la CRF.

Afin de limiter le nombre des opérateurs qui risqueraient d'être impliqués dans des affaires criminelles, le Ministère compétent au Luxembourg, mène également des enquêtes administratives minutieuses et drastiques exigeant une éthique et une intégrité parfaite des concessionnaires de casino. Les licences ne sont délivrées qu'à des candidats dotés d'un casier judiciaire vierge et jouissant d'une fiabilité assurée dans le domaine de la gestion d'entreprise. Ces conditions d'agrément sont aussi valables pour tous les actionnaires sachant que ces exigences sont les mêmes partout en Europe.

Le Casino 2000 situé à Mondorf est le seul casino de Luxembourg et il est régi par le règlement Grand-ducal du 12 février 1979 pris en exécution des articles 6 et 12 de la loi du 20 avril 1977 relative à l'exploitation des jeux de hasard et des paris relatifs aux épreuves sportives. Au Luxembourg, comme dans beaucoup d'autres pays, tous les employés du secteur des jeux doivent être agréés par le Ministère de la Justice, pour pouvoir exercer leur profession.

Trois autres dangers majeurs de blanchiment d'argent peuvent être trouvés dans certains casinos:

- les chèques,
- les dépôts,
- les transferts.

Les chèques émis par un casino sont présentés au Ministère des Finances comme preuve de gain et peuvent dès lors être présentés comme étant une preuve d'obtention d'un revenu légal. Cependant, le Ministère des Finances luxembourgeois n'accepte pas les chèques émis par le casino comme preuve de revenu. En revanche, aux États-Unis, il existe des documents similaires, établis par les casinos qui sont eux acceptés par leurs autorités. Il est important de noter qu'au Luxembourg, un chèque émanant du casino ne prouve pas du tout que le montant perçu provienne d'un gain du client.

Certains casinos dans le monde fonctionnent comme des banques et permettent aux clients l'ouverture d'un compte de dépôt. Parfois, ces comptes de dépôt sont utilisés pour « garer » de l'argent pendant un temps déterminé ou non. Le risque de blanchiment est encore plus grand pour les groupes de casinos internationaux qui acceptent les transferts d'argent (parfois de sommes mises en dépôt) vers d'autres pays où ils exploitent des casinos. Ces sommes sont alors transférées en dehors du circuit financier habituel. Ces transferts de sommes d'argent sur les comptes de joueurs pourraient également dans le cadre d'un réseau criminel être déclarés comme gain de jeux et donc, comme constituant un revenu légal.



# Le Bulletin

Comme pour la majorité des pays en Europe, l'actionnariat du Casino de Luxembourg est scrupuleusement contrôlé. Les transactions qui faciliteraient le blanchiment d'argent ne sont pas acceptées. Le casino n'autorise pas l'ouverture de compte de dépôt, ni les transferts sur un compte de dépôt d'un autre casino et n'effectue pas de transfert sur des comptes de clients. L'utilisation de chèques est également très réduite.

Conformément à loi modifiée du 12 novembre 2004 et au règlement grand-ducal du 12 février 1979, le casino a des obligations d'identification et de vigilance. L'identification et l'enregistrement des données se fait systématiquement pour tous les clients qui accèdent à la salle des jeux de tables. Pour la salle des machines à sous, l'identification a lieu lors de l'encaissement de gains ou d'échanges de jetons et, en cas d'établissement de chèques ou de retrait par carte bancaire.

En général, les casinos ont eux-mêmes un intérêt de connaître les flux d'argent pour se protéger de manipulations et disposent de nombreuses informations financières. Dans cette autre partie du secteur non financier, les exemples d'affaires de blanchiment ne manquent pas. On peut citer l'achat et le remboursement de jetons en de multiples montants inférieurs à environ EUR 6.700, la réception par les clients de casinos de chèques gagnants établis au nom de tiers et l'utilisation de jetons pour l'achat de biens et services, ou comme forme monétaire pour l'achat de drogue.

Il existe différents cas de blanchiment dans le monde impliquant des casinos, des sociétés de jeux et loteries diverses, mais aussi l'univers des courses de chevaux. Ces entités constituent autant de lieux propices au blanchiment, compte tenu de la manipulation de l'argent liquide qui y est pratiquée.

Les casinos permettent de réaliser la première phase du processus de blanchiment, c'est à dire de faire passer les fonds à blanchir du stade de billets (monnaie fiduciaire) à l'état de chèque (monnaie scripturale). En pratique, la méthode consiste à acheter des plaques et jetons en les payant en espèces, puis à en demander le remboursement sous forme d'un chèque que le casino va tirer sur son compte. Une autre possibilité consiste à racheter les plaques du casino à un autre joueur à un prix plus élevé ce qui évite de se faire identifier à la caisse. Le système peut être rendu plus opaque en utilisant une chaîne de casinos qui dispose d'établissements dans différents pays. Plutôt que de demander un remboursement en chèque dans le même casino que celui où les plaques et jetons ont été achetés en espèces, le joueur va prétexter un voyage dans un autre pays dans lequel la chaîne de casinos possède un établissement et demander la mise à disposition de son crédit auprès de ce dernier, où il sera à son tour retiré sous forme de chèque<sup>4</sup>.

Le casino de Luxembourg a mis en place un dispositif de contrôle allant bien au-delà des ses obligations légales afin de minimiser le risque de blanchiment autant que possible. De plus, conformément au Titre IV du Règlement grand-ducal du 12 février 1979 pris en exécution des articles 6 et 12 de la loi du 20 avril 1977 relative à l'exploitation des jeux de hasard et des paris relatifs aux épreuves sportives, le casino fait l'objet d'une surveillance et d'un contrôle permanent par des fonctionnaires du service spécial de la Gendarmerie chargé de la surveillance des casinos ainsi que les fonctionnaires et agents de l'administration des Contributions et des Accises désignés par le Directeur de cette administration ou tout autre fonctionnaire nommé par décision spéciale par le Ministre de la Justice et le Ministre des Finances.

Pour ce qui est de l'information aux employés, des formations régulières sont préparées notamment sur les principaux indices de blanchiment et destinées à certains groupes d'employés des salles de jeux afin de pouvoir identifier ou reconnaître les comportements anormaux. Depuis

---

<sup>4</sup> Vulnerabilities of Casinos and Gaming Sector, March 2009, FATF Report



# Le Bulletin

quelques années, des procédures sont en place permettant l'établissement de rapports, très majoritairement conservés et utilisés en interne, de certaines situations:

- Echange de petites coupures,
- Présentation de faux documents,
- Tentative pour éviter l'identification,
- Jackpots payés en espèces (cash),
- Établissement de chèques,
- Présentation de faux billets,
- Tentative d'échange de petites coupures en grandes, etc.

Le casino étant de petite taille, il paraît dès lors plus aisés aux employés de repérer/reconnaitre des situations de risque et des transactions douteuses.

Les sociétés de jeux et les loteries sont aussi de plus en plus utilisées par les blanchisseurs. On a pu ainsi constater récemment une multiplication d'opérations financières réalisées par une même personne et justifiées par des chèques tirés sur des organismes de jeux : loto, courses de chevaux, voire casinos. Ceci permet de constater que des circuits ont été mis en place pour organiser le rachat systématique des tickets gagnants auprès de leurs détenteurs légitimes moyennant une plus-value. On a vu apparaître ces derniers temps, une autre méthode de blanchiment dans l'univers des courses et des jeux où la personne va effectivement jouer avec l'argent à blanchir, mais de telle manière qu'elle sera raisonnablement certaine au bout du processus de récupérer plus ou moins sa mise sous forme de chèque, délivré par l'organisme de gestion des jeux ou de paris, et correspondant réellement à des gains de jeux parfaitement vérifiables. Cette méthode est beaucoup plus fiable que la précédente, car le service d'investigation policière, dès lors qu'il aura pu vérifier la réalité du jeu et du gain de la personne, aura en principe beaucoup de mal à aller au-delà, et à mettre en évidence l'origine de l'argent ayant servi aux mises de départ.

Sundhevy Goïot  
May Controls Solutions S.A.  
Sundhevy.goiot@maycoso.lu

## **Alternative Investment Fund Managers Directive: an overview**

The first draft of the Alternative Investment Fund Managers directive (AIFMD) was published by the European Commission, somehow unexpectedly, on 30 April 2009<sup>5</sup>.

Since then, we have seen several draft compromise proposals published by three consecutive Council Presidencies (Sweden, Spain, Belgium); two drafts AIFMD texts licensed, by the European Parliament's ECON Committee and by the Council's ECOFIN respectively; and countless industry comments, proposals and remarks.

Despite all this, there is still much uncertainty surrounding the final AIFMD text, and it is becoming more and more difficult for industry practitioners to isolate the (expected) contents of the directive from the white noise surrounding it.

In the April 2009 draft, as proposed by the European Commission, the directive contained rules for the authorisation, ongoing operation and transparency of managers of alternative investment funds (AIFMs)<sup>6</sup>.

However, in the AIFMD there was already much more than that, as it included provisions on funds valuation, depositary, transparency, reporting, sale and marketing, and third country (ie; non-EU) rules, for a total of 56 articles distributed on 53 pages.

The subsequent regulatory production process has failed to create a clear and straightforward text. To make a comparison, the most recent draft compromise proposal<sup>7</sup> published by the Belgian Presidency of the Council contains roughly the same number of articles but is 140 pages long, including three annexes.

Why so many complexities, when dealing with a mature product such as investment funds, and what are the implications of those complexities for the compliance function?

### **Key AIFMD provisions**

Although three official texts of the AIFMD currently exist (those licensed by the European Commission, the European Parliament and the Council respectively), for this article it is useful to refer to the last compromise proposal issued by the Belgian Presidency. This text is supposed to be reflecting the status of the recent trialogue discussions between the parties, and should constitute a solid basis for estimating how the final AIFMD text will look like.

Without entering into a full review of the AIFMD, whose text is anyway still being discussed, the following key components can be identified:

#### *1. Authorisation and operating conditions of an AIFM*

No alternative investment fund manager (AIFM) is authorised to manage one or more alternative investment funds (AIF), unless authorised. It should be noted that there is no single authorisation covering both AIFM and UCITS management company. Therefore, UCITS management companies already authorised will need apply to their home state regulator to be recognised also as AIFM.

---

<sup>5</sup> Proposal for a directive of the European Parliament and of the Council on Alternative Investment Fund Managers, COM(2009)207final.

<sup>6</sup> Article 1, subject matter.

<sup>7</sup> Ref 14265/1/10, 4 October 2010

Authorisation requirements for an AIFM include minimum capital requirements, good repute and sufficient qualifications of senior management, and appropriate professional indemnity insurance amongst other requirements.

Operating conditions will impose substantial compliance costs on smaller asset management firms and boutiques, and will be similar to operating conditions imposed on UCITS management companies. An AIFM will be required to act honestly, with due skill, care and diligence in the interest of the fund and its investors. For doing so, it will have to employ effective resources and procedures, avoid conflict of interests or manage them as they arise, comply with all applicable laws and treat the investors in the fund fairly.

In order to meet these requirements, the AIFM will be expected to put in practice particular arrangements, including the following:

- In terms of remuneration practices, the AIFM is expected to have policies and practices that are consistent with the funds managed, that are consistent with sound and effective risk management and that do not encourage unjustified risk-taking.
- Proper management of conflicts is also a fundamental requirement for AIFMs. All reasonable steps should be taken to identify conflicts of interest that arise in the course of managing funds. Identified conflicts should be managed and clearly disclosed.
- A sound risk management function is to be put in place, hierarchically separate from the portfolio management. The risk management function shall implement adequate risk management systems in order to identify and measure appropriately all risks relevant to the fund's investment strategy and to which the fund can be exposed.
- Liquidity management systems and procedures will be necessary for AIFMs managing funds that are not unleveraged closed-ended ones.
- Organisational requirements for AIFMs include an obligation to use at all times adequate and appropriate human and technical resources.

The AIFMD introduces also the role of "external valuer", i.e. an entity performing the valuation of assets and the calculation of the net asset value per share/unit. The concept is widely recognised in the industry and usually referred to as "fund administrator", "central administration" or similar.

According to the AIFMD, the valuation function can be carried out either by the AIFM or by the external valuer, which should be subject to professional or regulatory registration and be able to perform the role effectively, for the concerned fund.

The role and definition of external valuer, as well as the organisation of the valuation function, has been one of the most debated elements of the AIFMD since its initial April 2009 draft, and it has been subject to a number of amendments and redrafting. One of the last compromise proposals (27 August 2010) included also a prohibition for the depositary of a fund to act as external valuer for the same fund. This prohibition has been removed in more recent texts.

- The AIFMD introduces rules on the delegation of functions from the AIFM to third parties. The functions of portfolio management and risk management cannot be delegated but to professional parties, registered and subject to supervision. Stricter requirements apply in case of delegation to entities established in non-EU jurisdictions.

- Operating conditions refer also to the role of the depositary. Along with third country rules, this has been the most debated item of the AIFMD, and would deserve an article on its own.

In a nutshell, the AIFMD introduces a liability regime on AIF depositaries, which goes far beyond what is currently applied to UCITS depositaries. In its April 2009 wording, AIFMD introduced a completely unworkable depositary regime, whose strict reading would also have implied the impossibility for a European fund to invest into non-European securities.

The depositary liability regime has been subject to a number of amendments during the last few months – sometimes for the better, sometimes for the worse. Without entering into a too detailed analysis of the issue, it should be noted that the final regime should imply a substantially increased liability regime, including a reversal of the burden of proof (the depositary becomes responsible for assets lost, unless it can prove it has complied with the directive) with limited carve-outs and enhanced due diligence obligations in the case of appointment of subcustodians and prime brokers.

It should be noted that the European Commission is expected to amend the UCITS regime for depositaries and align it to the AIFMD regime.

## 2. *Transparency requirements*

Transparency requirements for AIFMs consist of: an annual report including not only the financial statements but also details on remuneration paid to senior management and staff; pre-investment detailed investor disclosures (including, for instance, the circumstances under which a fund may use leverage, the types and sources of leverage permitted and the associated risks, any restrictions to use of leverage and of any collateral and asset re-use arrangements); and finally, detailed regulatory reporting.

## 3. *Rules applicable to specific types of AIFs*

The AIFMD provides for additional obligations for managers of leveraged funds and for managers of private equity funds.

In the case of leveraged funds, the AIFMD imposes additional vigilance obligations on competent regulatory authorities, as well as on the ESMA<sup>8</sup>, which have to assess the extent to which the use of leverage contributes to the build-up of systemic risk. As far as AIFMs are concerned, those must demonstrate that the leverage limits for each fund they manage are reasonable and that they comply at all times with the limits imposed by law or fund's rules.

Rules applicable to private equity funds are still a matter of debate. Although older versions of the AIFMD included rules in terms of acquisition of non-listed companies, the latest drafts are incomplete and refer to ongoing dialogue discussions. We may need some more time to have more clarity on the matter.

## 4. *Passporting rights*

One of the key features of the AIFMD is undoubtedly that it establishes passporting rights for AIFMs and for the funds they manage. Those passporting rights are not so different from those currently applicable under the UCITS IV regime. It should be noted however, that unlike UCITS, passporting rights for AIFs apply only in the case of marketing to professional investors.

---

<sup>8</sup> The newly established European Securities Market Authority

This does not mean that AIFs cannot be sold to retail investors. EU Member States may allow the sale of an AIF also to retail investors, but can impose additional or stricter requirements on the AIFM or on the product.

### 5. *Third country rules*

Third country rules have been, along with depositary rules, the most debated part of the AIFMD and probably the only reason why no final text has yet been licensed.

In a nutshell, the key issue with third country rules is how to reconcile the Council's view with the view of the European Parliament, as expressed in their respective official proposals.

The most obvious difference between the European Parliament's text and the Council's text is that according to the former, non-EU-domiciled funds may, under certain conditions, be granted a European marketing passport while according to the latter, no passport is made available and the decision to allow marketing rests on each Member State, separately.

More specifically, the European Parliament's approach is that funds that are non-EU-domiciled may market their units or shares in any Member State, as long as they are domiciled in a qualifying country (specific criteria are established, focusing mainly on exchange of information and cooperation mechanisms with Member States).

If the non-EU fund is managed by a non-EU AIFM, enhanced criteria apply and the country where the AIFM is domiciled must also qualify. Additionally, it introduces rules for investment into non-EU-domiciled funds (in addition to marketing rules) to avoid circumventing marketing rules via private placement arrangements. Substantially, institutional investors that are EU-domiciled cannot invest into non-EU funds unless those funds are established in qualifying countries.

The Council's text instead makes a clear distinction between those funds managed by an EU-domiciled AIFM and those that are not.

If the fund is managed by an EU-domiciled AIFM, marketing may be granted under the conditions that the AIFM complies with the requirements of the AIFMD (with the exception of depositary rules) and that cooperation arrangements exist between the Member State where the AIFM is domiciled and the supervisory authority of the third country where the fund is domiciled.

If the fund is managed by a non-EU-domiciled AIFM, the AIFM must comply with transparency, reporting and disclosure rules. Cooperation arrangements between the Member State where the fund is marketed and the supervisory authority where the AIFM is domiciled must include rules for the oversight of systemic risk in line with international standards.

In terms of delegation of service provisions to providers established outside the EU, the Council's and the European Parliament's text differ greatly. While the Council's text is silent (or better, deletes any relevant provisions as contained in the original EC AIFMD draft), the European Parliament's text contains provisions that apply to the delegation of activities such as administrative tasks and valuation of assets to a non-EU entity.

The 4 October compromise proposal is the latest attempt to make clarity on the matter. But there is little point in providing here a detailed analysis – this is definitely work in progress, still being discussed in trialogue.

## 6. *Competent authorities*

AIFMD is naturally aligned to the new EU supervisory framework, therefore requiring increased cooperation and coordination between national regulatory authorities and ESMA – including processes for imposing administrative penalties, right of appeal against those, and dispute settlement procedures.

### **New challenges for the compliance function?**

The challenges introduced by the AIFMD for the compliance function can be seen from three angles: from a rule-making process angle, from a product design/management angle, and from a pure compliance oversight function angle.

In terms of rule-making process, the most challenging activity for the past two years has been to keep up to date with regulatory discussions at European level, trying to make clarity out of the several, and most often contradictory, AIFMD texts.

One can only hope that the recently approved financial supervision reform, with the establishment of ESMA, will substantially improve and streamline the fund regulatory production process.

As the regulatory making process becomes more and more centralised at European level (a trend which we have seen increasing in the last 5-6 years), the compliance function will be required to stretch outside of its national borders, to ensure that it is aware of regulatory initiatives well before they are implemented in national laws. From this point of view, national industry associations, such as for Luxembourg ALFI, ABBL and the same ALCO, will play a key role and will need making additional efforts to ensure their voice reaches out to Paris (in the case of ESMA).

In terms of product design and management, from a Luxembourg point of view, challenges should be limited. The legal and regulatory framework of the Grand-Duchy is broadly in line with most of the AIFMD requirements, although fine tuning will be required. The SIF law provides for a very solid basis to build upon.

However, attention will have to be paid to depositary provisions (in particular, with reference to the depositary-prime broker relationship) and on the external valuer provisions, in particular should the final AIFMD text impose a legal (and not only functional) segregation with the depositary.

Enhanced due diligence obligations will impose additional efforts also on the compliance function, that will be called upon either to perform reviews of sub-custodians and prime brokers, or to ensure that appropriate due diligence is employed by the business when selecting them.

In terms of compliance oversight, again for a mature regulatory environment such as Luxembourg organisational requirements imposed on AIFMs should not provide particular concerns. However areas such as remuneration practices and transparency and reporting requirements, in particular for private equity business, could be demanding at least in the initial stage, before a solid business practice is established.

### **Conclusions**

The final word on the AIFMD has still to be written. Since the beginning of the Belgian Presidency (but also before) a number of revised compromise proposals have been circulated to the industry, including sometimes significant changes – although the basis structure of the directive has remained pretty much the same since August 2010.

The last official position, at the date of writing, is that the AIFMD should be licensed by the European Parliament in plenary vote on 18 October, even if rumours are that a vote is more likely to happen in November. As the vote will be held only on the basis that trialogue discussions have finally reached an agreement, the vote would imply green light for the AIFMD. Level 2 measures will then be produced.

## Le Bulletin

Almost at the same time, we should also see the much rumoured UCITS V directive (or UCITS IV ½ as some European Commission officers informally name it), that will introduce almost surely depositary liability standard comparable to (or even stricter than) those included in the AIFMD.

Stefano Pierantozzi  
Head of EMEA Fiduciary Oversight & Research  
Citibank International



## Résumé des Tables Rondes

One year ago the round table lunch meetings were launched. Already 80 participants have accepted to share their experience, their questions and their feelings on 5 different topics<sup>9</sup>. Although it is not easy to go through tricky issues in only 100 minutes, most of the participants agreed to take the opportunity to start interesting peer to peer discussions around the table.

### MARKET ABUSE - prevention & detection

For this first meeting of 2010 we decided to focus on the prevention and the detection of market abuse. More than 30 members showed interest, but only 16 of them were available to attend on the 24th.

14 completed questionnaires have been collected. Their summary is hereto attached.

This time, we were glad of having Cyril Mathieu as expert to enhance the discussions.

Cyril Mathieu is Assistant Manager Fund Compliance at HSBC. He has participated to ABBL working groups and, subject to ALCO members' interest he is willing to re-launch the ALCO Market Abuse working group 29 he is chairing to discuss further this interesting matter and share practice. Don't hesitate to join this working group, if you are interested in the subject.



- He introduced the meeting by commenting some slides<sup>10</sup> explaining the specificities & evolutions of the subject. He also questioned how the Market Abuse Directive might be reviewed soon as there is an obvious hardening of public and regulators attitudes to improve market cleanliness and integrity. Finally, he highlighted some best practices expected to reinforce the prevention of market abuse.
- A few slides showed a sample of the market abuse cases that have been commented in the newspapers:
  - The GBP 1,7 million FSA fine levied against Shell Petroleum in 2004 and the USD 120 million settlement agreed by the company with the SEC.

---

<sup>9</sup> (a) expectations of new members towards ALCO ; (b) MIFID – suitability ; (c) Compliance & Risk Management – links in the fund industry ; (d) AML Filtering (e) Market Abuse –detection & prevention

<sup>10</sup> The PowerPoint presentation is available upon request.

# Le Bulletin

- The GBP 25K FSA fine against the director of Cambian Mining in 2005 and the GBP 59K fined by the FSA against the director of Byron Holdings in 2009.
- The sentenced use of insider information by a dentist who had been informed by his son who could get insider information during a student job with a broker (2009).
- Several persons sentenced to jail for insider trading in Hong Kong in 2009; several criminal prosecutions by the FSA since 2008.

The discussions were moderated (& stimulated!) by Pierre Hennericy and Charles van Doorslaer was in charge of summarizing the discussions.



Once again the questionnaires showed a wide range of practices<sup>11</sup>. The diversity of the answers can be explained partially by the kind of business (banking, insurance, asset management...) as well as by the size of the companies. Belonging or not to an international group, being listed or not on a stock exchange is even more determining for the prevention & controls put in place and for the level of awareness.

It is important to keep in mind that the ideas expressed in the questionnaire, the discussions and this summary are not reflecting any position, nor from the ALCO, nor from any institution of which a member has participated. Although it is difficult to reflect all the details of the discussions in a written summary, this document aims at reflecting the extent of the talks we had during the session.

## Prevention:

---

There isn't one single way to organise prevention. Different complementary ways might be used.

A compliance officer might organise trainings. These trainings can be given through e-learning or face to face sessions or a combination of both. Some companies benefit from training materials made available by a foreign parent company, some organise it themselves. External trainers can be hired and exposed employees can also participate to seminars & conferences.

Some banks train all employees upon their arrival. Others launch specific training sessions focused on certain departments. Most of the participants have already tested e-learning or expect to start e-learning sessions in a close future.

---

<sup>11</sup> It has to be noted that 14 completed questionnaires cannot be considered as a representative number compared to the hundreds of financial companies that are present in Luxembourg.

# Le Bulletin

Everybody agrees training should be as close as possible to the daily activities of the trainees. It is a big advantage when a trainer has gained experience in the same business and can illustrate concepts with his own experience and anecdotes.

Awareness can also be improved when compliance officers participate to business meetings, especially when these take place on a regular basis. And if they don't get invited to these meetings, they invite themselves!

Quite some documents are issued to inform employees about their responsibilities & duties.

- An internal **code of conduct** applies to all employees.
- When the company is listed, a **dealing code** has to be agreed by any potential insider within the company. Blocking periods and specific procedures need to be respected strictly.
- All employees linked to asset management activities need to comply with specific rules on employees **personal transactions**.
  - o Some companies are asking all concerned employees to notify immediately all their transactions in securities handled through another bank. Results are mitigated. Depending on the way the rules have been implemented<sup>12</sup> and the level of awareness of the employees, few or many operations are reported. It is almost impossible to control the exhaustiveness. An employee may report a lot of transactions, but it might be that he will not report a transaction that he might consider himself as a forbidden insider deal.
  - o Some banks request from their employees to buy & sell securities exclusively through their account at the bank. Success may be depending on the tariffs that are offered to employees. There again, it doesn't prevent an employee to also execute some insider trades in a different institution. A pre-trade clearing by compliance might offer a solution.
  - o Specific constraints can be issued about a minimum delay between acquisition and sales (E.g. minimum 3 days, 10 days...), a maximum number of transactions per month etc.
  - o To avoid conflicts of interests or difficulties in monitoring, investment in 'own' products might be forbidden.
  - o In certain countries (E.g. France, UK) bank statements are sent in copy to the employer.
  - o It also happens that employees are asked not to invest in any securities, unless it is through discretionary management or in UCITS. Sometimes they are asked to invest only through a dedicated investment company or to have each investment decision first validated by the compliance officer before being executed.

Are awareness messages helpful? It's important to target the right persons and to have very short texts. It might be interesting to check, through a acknowledgment of receipt, how many messages are opened and to have some statistics about the received feed back. When people are asked to do something (e.g. print a form that they have to sign & return), this will encourage them to have a closer look to keep in mind what it is about.

Are Chinese walls helpful? Avoiding employees getting access to certain data, certain files, certain departments is essential in a lot of companies. Especially when one is offering investment banking, corporate finance as well as private banking or retail services, one needs to make sure that information is not circulating easily from one place to the other within the organisation.

---

<sup>12</sup> Through e-mail or handed over personally, requesting or not a duly signed notice of receipt, combined or not with a training session....

# Le Bulletin

Should compliance officers have permanent access to all the activities? Not necessarily a permanent access, but they need to have the possibility to obtain access on request. If access is refused, the compliance officer should escalate the issue to the board, who will then determine how the access will be organised.

Commitment of senior management is probably the main key to success.

64% feel senior management have a sufficient understanding of the Market Abuse risks. A way to check awareness of Senior Management is observing how they react when they are notified of an information request from the Authorities. The question of the awareness should not be measured through the level of *understanding* but rather through the level of *support* senior management grants to prevent and to fight against market abuse. Can one compare the level of support against M.A. with the level of support for A.M.L.?

Commitment significantly depends on the manager's experience and working environment. It seems that managers who are linked to UK, USA, France, and Far East ... have often a much higher level of awareness than those who are linked to Belgium, Switzerland or Eastern Europe ... The influence of the mother company is of course determinant as well.

How to draft a Market Abuse Policy, a code of conduct? Most of the participating companies have drafted their Policy on their own or have received a standard text from their parent company. Most of them include examples of information, circumstances, events that should be considered as inside information, a procedure for escalation, an obligation to report any inside information leak and rules to handle such leak and even rules about trading in clients' financial instruments...

Most of participants have a list of permanent insiders. Some of them (36%) have also had specific insiders' lists related to certain projects

64 % confirm that they already have mapped sources and typical flows of inside information. Same number is trying to identify all clients that are to be flagged. Flagging potential insiders (or potential market manipulators) needs to be done through the client due diligence as from the entry into relationship.

## Detection

---

Which are our main obligations concerning detection? Identify persons closely related to listed companies - identify them among clients & employees, detect suspicious transactions (insider trading and market abuse) and monitor employee transactions.

Flagged clients and employees are often gathered together on a watch list used for specific controls.

A few participants (29%) have developed a proactive system to get alerts on transactions or market events enabling a priori detection. Half of the participants have a posteriori detection systems.

Among all the transactions that are expected to be detected by the systems, insider trading and fictive orders are the most inclined to be highlighted (46 %). They are followed by 'pump & dump - trash & cash' transactions (29%) and then by front running and market timing (both 21%).

When one cannot reckon on a performing automated tool that helps to detect insider trading or market manipulation, is it efficient to focus the controls on traders? Often traders know the rules very well.

# Le Bulletin

Sometimes they contact compliance in a proactive way. Most alerts on transactions from traders require deep analysis, but the outcome of the analysis is rarely positive.

It is possible to perform ex post detection in an efficient way through queries built with general software like Business Object, Access or even Excel, generating automated daily reports. Here consideration should be given to the accuracy and efficiency of the whole detection process with regard to external auditors and prudential authorities.

In 71% of the answers, there is a group policy regarding market abuse, but in only 57% of the cases detection and monitoring of market abuse is coordinated within the group, with some controls delegated to the company.

Another issue is about the difficult balance between the need of escalating the suspicious transactions to a parent company on the one hand and the bank secrecy & no tipping off principles on the other hand.

## Expectations from the authorities

---

Only one participant seems to have received feed back from the authorities on the reporting of a suspicious transaction. Does this mean that CSSF or FIU require discretion that is even higher than for AML issues? Or do enquiries take a lot of time to conclude? Or that there is no feed-back from the investigating foreign authorities? It's difficult to determine. Prevention and detection of market abuse is not an obligation of results but of means. The risk of having an authority blaming you that "you should have known" or "you should have detected earlier" is not easy to evaluate.

Consequently, it might be a good suggestion to document as much as possible why the bank decides, on a risk-based approach, not to monitor certain categories of transactions or of accounts.



## Conclusion

---

We feel that most of the participants have appreciated the opportunity of asking their questions, sharing experience and exchanging thoughts. Some of them have showed interest in reactivating and joining the Working Group on Market Abuse to continue the brainstorming and some other to join the Working Group organising the Round Table discussions.

## Summary of the answers received to the questionnaire

O Bank O Asset Management Company O Fund administration Company O Insurance Company O Other

Bank	AM	Fund	Insurance	Other	Total
11	1	0	1	1	14
79%	7%	0%	7%	7%	100%

**ALCO Round Table nr 4**  
**Prevention & Detection of Market Abuse - Preliminary questionnaire**
**Prevention – Training – awareness: what's included in your company prevention?**

- code of conduct, dealing code, policies - to all/to exposed employees only

- training: internal - to all/to exposed only

- training: external - to all/to exposed employees only

- awareness messages (by e-mail...) - to all/to exposed employees only.....

- chinese walls: on physical access?

and ..... on IT access?

**Commitment of senior management**

- Do you feel your senior management has a sufficient understanding of the risks they face?

- Have responsibilities, duties &amp; ownership been determined at all levels?

**Prevention of (external & internal Insider) trading -**

- Have you mapped sources and typical flows of inside information?

- Does your insider policy include:

- *examples of information, circumstances, events... that should be considered as inside information*- *a procedure for escalation of information about events that may constitute inside information*- *an obligation to report any inside information leak & rules to handle such leak*- *rules re: trading in clients' financial instruments to all or certain members of the staff*

- Have you got, at some stage, some external support from law firms/consultants?

- Are your clients identified or screened in some way in order to be flagged as potential insiders?

**About (internal) insiders lists (re: employees, management)**

- Have you a list of permanent insiders (structured by functional responsibility/exposure)?

- Have you ever had a „project-specific“ ? insiders list structured by inside information item or project?

**If your bank is member of an (international) banking group:**

- Is there a Group policy regarding market abuse

- Is detection /monitoring coordinated within the group

- Are control processes delegated to your entity

**Personal account dealing regime / policy on personal employee transactions**

- Are certain managers/employees to obtain prior permission to trade (pre-trade clearance)?

- Have managers/employees to respect trading black-out periods?

permanent trading prohibition?

- Are employees required to report a posteriori security transactions made on external accounts?

- Do your employees and managers ask for clearance as a matter of practice on their own initiative?

- Do you restrict trading “channels” (e.g. dedicated investment firms) of managers/employees/?

- Are certain managers/employees required to declare certain of their holdings?

**Detection: what kind of systems do you use?**

- a proactive system to get alerts on transactions or market events or a priori detection?

- a passive database of transactions to be analysed or a posteriori detection?

- a transaction monitoring system that has been developed internally?

- a transaction monitoring system that has been developed by an external service provider?

**Examples of transactions that you expect to be detected by your institution:**

- insider trading

- front running

- market timing

- late trading

- pump &amp; dump / trash &amp; cash

- concentrations of unusual operations

- fictive orders

**Which kind of market abuse has your institution already detected?**

None: 6

Insider dealing: 5

Front running: 2

Other: 1

YES	%	NO	%	All	%	Exposed	%				
14	100%		0%	12	86%	1	7%				
9	64%	5	36%	4	29%	4	29%				
3	21%	6	43%		0%	1	7%				
8	57%	6	43%	3	21%	3	21%				
12	86%	2	14%		0%		0%				
13	93%	1	7%		0%		0%				
YES	%	NO	%	No opinion	%						
9	64%	1	7%	4	29%						
9	64%	3	21%	2	14%						
YES	%	NO	%	N/A	%						
9	64%	4	29%	1	7%						
11	79%	2	14%	1	7%						
11	79%	2	14%	1	7%						
10	71%	3	21%	1	7%						
9	64%	4	29%	1	7%						
1	7%	12	86%	1	7%						
9	64%	4	29%	1	7%						
YES	%	NO	%	N/A	%						
10	71%	3	21%	1	7%						
5	36%	8	57%	1	7%						
YES	%	NO	%								
10	71%	4	29%								
8	57%	6	43%								
8	57%	6	43%								
YES	%	NO	%								
6	43%	8	57%								
9	64%	5	36%								
8	57%	6	43%								
9	64%	5	36%								
7	50%	7	50%								
4	29%	10	71%								
9	64%	5	36%								
YES	%	NO	%								
4	29%	10	71%								
7	50%	7	50%								
5	36%	9	64%								
1	7%	13	93%								
manual	%	semi-automatic	%	N.A.	%	no answer	%	Sample	%	selection	%
6	43%	2	14%	2	14%	4	29%	2	14%	4	29%
3	21%	2	14%	5	36%	4	29%		0%	1	7%
3	21%	2	14%	5	36%	4	29%		0%	2	14%
2	14%	4	29%	4	29%	4	29%		0%	2	14%
4	29%	3	21%	5	36%	2	14%	1	7%	1	7%
6	43%	0	0%	2	14%	6	43%	1	7%	2	14%
6	43%	0	0%	4	29%	4	29%	1	7%	1	7%

<sup>13</sup> Charles van Doorslaer, Pierre Hennericy, Xavier Leydier, Vincent Salzinger, Mike Sommer, Eef Liesens, Jean-Michel Righi



## **Assurances: La lettre Circulaire 08/1 du CAA relative aux règles d'investissements pour les produits d'assurance-vie liés à des fonds 'investissements**

Présents : 16 membres de l'ALCO

Référents :

- Nicolas Limbourg, VITIS LIFE SA
- Thierry Flamand, PwC

Pour le WG 34 :

- Pierre Hennericy, Banque Pictet & Cie, Modérateur
- Xavier Leydier, Banque Havilland SA, Secrétaire
- Eef Liesens, VITIS LIFE SA, Initiatrice de la table ronde
- Charles van Doorslaer, KBL EPB, organisateur

### **Introduction**

---

Cette Table Ronde 'assurances' s'est tenue à un moment propice. En effet, suite à la crise financière, il y a une prise de conscience certaine au sein de la profession quant à certains risques jusqu'alors mésestimés. Ces risques concernent tant la Banque dépositaire que les actifs sous-jacents. Des avancées ont été faites en 2009 mais surtout en 2010 dans la mesure où de plus en plus de compagnies d'assurances mettent en place des outils pour mieux contrôler les risques sous-jacents à la gestion des actifs investis. Nous remercions particulièrement Eef Liesens, qui est à l'initiative de cette table ronde, ainsi que Nicolas Limbourg et Thierry Flamand pour leur expertise et leurs apports aux débats, en tant que référents techniques.

### **Tour de table et discussions**

---

Un tour de table est organisé sur la base d'une série de sept questions remise aux participants avant la Table Ronde (en annexe).

Les participants sont unanimes pour reconnaître que les processus d'ouvertures et de gestion de comptes des banques ne sont pas suffisamment adaptés aux fonds sous-jacents aux contrats d'assurance-vie.

La plupart des sociétés représentées ont mis en place, ou ont le projet de mettre en place, une base de données regroupant toutes les données financières des banques dépositaires. Elles se reconnaissent le même problème majeur, à savoir celui de l'alimentation de cette base, pour plusieurs raisons :

- Le manque de moyens télématiques ayant pour conséquence le besoin d'input manuel ;
- Les mêmes actifs dans différentes banques dépositaires peuvent être repris avec des valeurs différentes ou une classification différente ;
- Le niveau de la VNI en fonction du « side-pocketing » qui reste du domaine du choix pour la société d'assurance.

Les participants regrettent un manque de communication de la part du Commissariat Aux Assurances (CAA) notamment lors des dernières crises (Madoff, 2009 – Grèce & Portugal avril 2010).



# Le Bulletin

Il ressort du tour de table que :

- Certains participants n'ont pas (encore) de base de données.  
Dès lors, le contrôle est réalisé, manuellement, ligne à ligne et a posteriori. Peu de sociétés ont développé (ou finalisé) un contrôle on-line. En général, il existe une séparation nette entre les activités de banque dépositaire et celles de sociétés d'assurance.  
Le contrôle a priori est effectué pour chaque transaction et un contrôle a posteriori est effectué sur une base mensuelle.
- Pour le reporting, certains outils sont disponibles dans le commerce mais certains ont aussi opté pour un développement personnalisé en interne d'une base de données.
  - Les participants sont confrontés à un problème constant que constitue la valorisation des titres non cotés.
  - Le reporting peut être effectué sur la base d'un reporting transmis par la banque dépositaire.
  - Le reporting de la banque dépositaire peut être aussi corroboré avec les valorisations reçues par l'intermédiaire d'un système de valorisation internationalement reconnu tel que Bloomberg, Reuters ou Telekurz, par exemple.
  - Tous les participants ne sont pas aussi avancés en matière de contrôle de restrictions d'investissement que les autres.

On constate que :

- Peu de banques dépositaires contrôlent la gestion et la répartition des Actifs dans le portefeuille d'assurance.
- Les sociétés d'assurances sont confrontées aux problèmes de la mise en place des normes IFRS.
- Elles sont, en outre, confrontées au fait de gérer des actifs soumis à trois circulaires différents datant de 1995, 2006 et 2008 et ayant une certaine redondance, créant ainsi un problème 'd'éducation' des partenaires.
- Le contrôle est centralisé, même s'il existe différents sous-dépositaires ou gestionnaires dans différents pays.
- Certaines sociétés d'assurances travaillent avec plusieurs gestionnaires externes et une seule banque dépositaire centralisée. Dans ces cas-là, les « breaches » sont rapportés directement aux gestionnaires externes. Certaines entreprises préconisent de faire certifier dans le mandat de gestion la connaissance des règles du CAA. Cependant, il est admis que le gestionnaire a une obligation contractuelle de moyens, et non pas de résultats.
- Il existe une zone grise sur la place en matière de passation d'ordre pour la banque dépositaire : de qui doit-elle recevoir les instructions ? Les gestionnaires peuvent avoir le choix pour passer leurs ordres : soit directement auprès de la Banque dépositaire soit via la société d'assurance.
- De même, il se pose le problème de l'intervention du client dans le changement de la stratégie globale ou pour un investissement spécifique, que ce soit auprès de la société d'assurance mais aussi directement auprès de la banque dépositaire. Dans le but d'éviter la requalification du contrat d'assurance, certains participants mettent en avant le fait qu'ils interdisent aux « Asset Managers » de passer des ordres en fonction des ordres des clients. Les gestionnaires d'actifs doivent en effet se conformer aux règles d'une gestion discrétionnaire.
- Les participants reconnaissent la pauvreté des conventions sur l'attitude à avoir en cas de « breach ». En règle générale, les participants reconnaissent que les conventions de gestion font la loi entre les parties et confèrent à chacune des parties une obligation de moyens. Les participants reconnaissent qu'ils sont souvent confrontés à une traduction par la banque dépositaire des grilles d'investissement produites par la société d'assurance, afin de les

adapter à leur grille interne. Il s'en suit dès lors des difficultés d'analyse pour la société d'assurance.

- La plupart des sociétés représentées ont le même problème pour se débarrasser des actifs « indésirables » lors de la reprise d'un portefeuille d'actifs. Ce problème se retrouve principalement lors du transfert de comptes gérés en produit d'assurance ou lors du transfert d'un portefeuille bancaire existant lors de la clôture d'un compte au profit d'un contrat d'assurance-vie. La société d'assurance peut se retrouver parfois avec une série d'actifs non autorisés par le CAA. Les participants reconnaissent qu'il s'agit dès lors d'un problème pour le preneur d'assurance. La société d'assurance adapte en général sa stratégie d'investissement en fonction de la liquidité des titres reçus. Elle peut, le cas échéant, faire signer une « indemnity letter » par le preneur afin de transférer les titres non éligibles ou pour détailler une stratégie pour se défaire de ces titres, au cas où ceux-ci seraient non liquides ou non vendables.
- De même, les sociétés d'assurances sont confrontées à la difficulté de certification des investissements devant la diversité des produits financiers. Dès lors, la décision quant à l'admissibilité de l'investissement est-elle de la responsabilité de la Banque dépositaire ou du gestionnaire ?
- La détermination des priorités de contrôle des portefeuilles peut se faire en fonction d'une « risk based approach » en commençant par les plus gros portefeuilles ou par les gérants externes affichant le plus de non-conformité ou encore par les gérants externes les plus importants...
- Pour les banques prestant à la fois des services « fonds » et des services « assurances », les contrôles à prester pour les services « assurances » sont généralement exercés par l'entité « Compliance Fonds ».

Dans le domaine de la domiciliation, il ressort que la plupart des participants doivent quelquefois faire face à une certaine confusion des rôles entre ceux de société domiciliataire, banque dépositaire, gestionnaire ou compagnie d'assurance. Afin de définir ces rôles d'une manière plus précise, on retrouve différentes approches :

- Le contrôle des limites d'investissement peut être du ressort du service « Fonds » de l'entreprise.
- La « VNI » du produit d'assurance reste dépendante de la VNI produite par la banque dépositaire.
- Comme les banques dépositaires sont assujetties au contrôle de la CSSF et non pas du CAA, les spécificités du CAA ne sont souvent pas assez connues des banques.
- La société d'assurance considère bien souvent son rôle comme étant une responsabilité de « second niveau » de contrôle.

Pour ce qui est de la « Due Diligence » pour la sélection des Asset Managers :

- La plupart des participants exigent que les Asset Managers disposent d'une qualification dans le pays de résidence. Cette exigence est complétée par une enquête de réputation. Pour certains participants, une décision d'un comité d'acceptation est nécessaire. Pour d'autres, il n'y a pas de formalités standards, ni de comité d'acceptation, car tout nouvel Asset Manager se doit d'être accepté, à la source, par la direction ;
- La notion de qualification pose problème aux participants car, si à Luxembourg le cadre semble verrouillé (si la supervision de l'intermédiaire n'est pas effectué par le CAA, il existe une supervision par la CSSF pour les PSF), il n'en est pas de même dans les pays étrangers où la notion de supervision par un régulateur n'existe pas toujours. De plus, il ressort des

directives du CAA qu'il y a un problème de responsabilité de la contrepartie, si la Due Diligence n'est pas effectuée.

Les participants se penchent ensuite sur la problématique des litiges en cas de disparition des actifs ou en cas de perte substantielle. Il ressort de la discussion que tous sont d'accord pour reconnaître que la responsabilité incombe aux sociétés d'assurances, la banque dépositaire n'intervenant qu'en tant que « nommée ». De plus, pour les banques dépositaires, se pose le problème de l'identité de l'actionnaire et du contact avec ce dernier ainsi que de l'accès aux informations relatives à ce dernier. En tout état de cause, les participants reconnaissent qu'une collaboration plus proactive avant tout litige est hautement recommandée :

- Pour certains, cette collaboration passe par des réunions mensuelles ou trimestrielles avec les gestionnaires, mais pas avec la banque dépositaire.
- Pour d'autres, il s'agit d'analyse au cas par cas via la banque dépositaire.
- Les contrôles effectués pour vérifier le niveau des investissements sont en général pollués à plusieurs niveaux par des problèmes inhérents au niveau d'activité tels que la multiplicité des contacts, des titres, des types de VNI, de périodicité de VNI...
- Les participants s'interrogent ensuite sur leur niveau de contrôle et reconnaissent que s'il existe des contrôles externes chez les grands acteurs, les plus petits ont plus de mal à les mettre en place ou à s'imposer dans ce domaine.
- Enfin, les participants regrettent leur dépendance vis-à-vis des informations transmises par les Banques dépositaires et se posent la question de leur possibilité d'évaluer correctement ces informations.

## Conclusion

---

Cette table ronde met en évidence une fois de plus la diversité du métier de Compliance Officer. Cette diversité est fonction de l'entité dans laquelle il s'opère. C'est d'autant plus vrai dans le domaine de l'assurance. Il touche en effet différents types d'acteurs de la Place financière. Améliorer encore la coordination entre les deux entités de supervision que sont le CAA et la CSSF, afin d'harmoniser au mieux la réglementation et donc le niveau de contrôle, serait tout bénéfique pour la Place.

Les participants peuvent se référer à l'Association des Compagnies d'Assurances (ACA) qui émet des recommandations.

La réunion a été appréciée pour avoir permis de confronter les points de vue et de mieux partager les interprétations et pistes de solutions, ce type d'exercice permettant à chacun de se « benchmarker » par rapport à la pratique professionnelle de la place.

Pour le GT 34, Xavier Leydier

## Question de Membre

Question : *Les Appointed Representatives établis aux UK peuvent-ils être considérés comme équivalents aux PSF de droit luxembourgeois vis-à-vis desquels les assujettis aux règles LAB/CFT luxembourgeoises peuvent bénéficier de l'exonération d'identification ?*

Réponse :

Cette question relative à l'*Appointed Representative* (ci-après « AR ») n'est pas tant importante au regard de son sort personnel que par rapport au traitement de ses propres clients, notamment dans le cas de la distribution de produits financiers (parts de fonds, produits d'assurance, etc...).

De manière générale, un AR est une personne physique ou morale qui est enregistrée auprès de la Financial Services Authority, et fait l'objet d'une supervision par un « Principal » qui joue un rôle de sponsor. Un lien contractuel doit exister entre l'AR et son Principal, ce dernier devant obligatoirement être une entité « autorisée » par la FSA. Le statut et les attributions des AR sont précisés dans la section 39 du Financial Services and Market Act, 2000.

Cependant, un AR n'est pas régulé et est non nécessairement soumis aux obligations en matière de prévention des activités de blanchiment de capitaux et de financement du terrorisme. Dès lors, dans le respect du principe de l'approche risque, seule la mise en œuvre d'une série de mesures de vigilance pourra permettre de distinguer les AR pouvant être considérés comme équivalents à des PSF luxembourgeois de ceux qui ne peuvent l'être.

Les points d'attention indispensables semblent être les suivants :

- s'assurer que l'AR figure bien dans le registre de la FSA (disponible sur internet) ;

- établir le lien existant entre le Principal et l'AR : il s'agit de vérifier, par la production de pièces justificatives (copie de contrat, accord, etc...), la réalité du lien contractuel et opérationnel entre les deux entités ainsi que la ventilation des obligations et responsabilités pour la matière LAB/CFT. Il conviendrait alors de s'assurer de l'existence et de la conformité du service ou produit visé au regard du périmètre des activités dédiées à l'AR par le Principal ;

- vérifier la fiabilité du Principal (statut, régulation, réputation, etc...) par tout moyen;

- matérialiser un contrôle du Principal sur l'AR : il semble notamment indispensable d'obtenir une garantie donnée par le Principal sur l'AR (AML Letter par laquelle le Principal confirme qu'il impose à l'AR l'application des obligations LAB/CFT telles que prévues par la 3<sup>ème</sup> directive UE anti-blanchiment, certifie l'absence de suspension, de retrait d'agrément, de condamnation judiciaire, de sanctions professionnelles ou d'implication dans des affaires criminelles,...de l'AR).

Il est à noter que ces éléments de vigilance sont à appliquer lors de l'entrée en relation mais également tout au long de cette dernière.

# Le Bulletin

Ainsi, le principe d'équivalence pourra n'être considéré comme acceptable qu'à la double condition suivante :

- que satisfaction soit donnée au PSF luxembourgeois une fois ces points de vigilance réalisés ;
- que les flux financiers ou assimilés (ex : ordres de souscription) transitent nécessairement par l'AR en question et ne proviennent pas directement de tiers (ex : investisseurs). Dans le cas contraire, ie si les flux atteignent directement le PSF luxembourgeois sans l'intermédiation de l'AR, il conviendrait soit d'obtenir un engagement de la part de l'AR sur la qualité du client/investisseur final, soit d'appliquer le principe d'identification complète à ce dernier.

Cette dernière exigence est primordiale. En tout état de cause, des AR qui ne revêtraient que le simple statut d'intermédiaire ou d'apporteur d'affaires, sans intervenir par la suite dans l'exécution des opérations effectuées par le client/investisseur final, ne pourraient pas être considérés comme équivalents aux PSF luxembourgeois. Ils devraient dans ce cas être identifiés ainsi que les clients/investisseurs finaux. Aussi, dans un souci d'efficience opérationnelle, le régime d'identification à appliquer à un AR et/ou au client/investisseur final pourra être décidé dès la phase d'entrée en relation.

Pour plus d'information, on se réfèrera à la section 12 du « Handbook AR » de la FSA disponible sur internet.

## Vie associative

### VIE ASSOCIATIVE

#### GROUPES DE TRAVAIL ACTUELS

##### Groupe de travail 11

##### Site Internet

Responsable Olivier GILSON  
Téléphone +352 48 48 80 51 08  
[olivier.gilson@efa.eu](mailto:olivier.gilson@efa.eu)

##### Groupe de travail 16

##### Commission permanente juridique et relations publiques

Responsables Claudine FRUTSAERT  
Téléphone +352 44 24 24 43 15  
[claudine.frutsaert@axa.lu](mailto:claudine.frutsaert@axa.lu)

Jean-Marie LEGENDRE

Téléphone +352 24 67 26 07  
[Jean-Marie.LEGENDRE@ca-luxembourg.com](mailto:Jean-Marie.LEGENDRE@ca-luxembourg.com)

##### Groupe de travail 20

##### Funds practices and recommendations AML

Responsable Patrick Watelet  
Téléphone +352 45-14-14-231  
[patrick.watelet@citi.com](mailto:patrick.watelet@citi.com)

##### Groupe de travail 21

##### Interprétation pratique des restrictions d'investissements de fonds

Responsable Tim WINFIELD  
Téléphone +352 34 10 23 85  
[tim.winfield@jpmorgan.com](mailto:tim.winfield@jpmorgan.com)

##### Groupe de travail 27

##### Formations IFBL

Coordinateur Sundhevy GOÏOT  
Téléphone +352 621 30 23 63  
[sundhevy.goiot@maycoso.lu](mailto:sundhevy.goiot@maycoso.lu)

##### Groupe de travail 29

##### Abus de marché

Coordinateur Cyril MATHIEU  
Téléphone +352 40 46 46 400  
[cyrilmathieu@lu.hsbc.com](mailto:cyrilmathieu@lu.hsbc.com)

##### Groupe de travail 30

##### Domiciliation de société

Coordinateur Sophie RASE  
Téléphone +352 40 25 05 408  
[sophie.rase@maitlandgroup.com](mailto:sophie.rase@maitlandgroup.com)

Coordinateur Marie-Hélène CLAUDE

Téléphone +352 48 18 28 39 03  
[marie-helene.claude@alterdomus.lu](mailto:marie-helene.claude@alterdomus.lu)

##### Groupe de travail 33

##### Réponses aux questions des membres

### ASSOCIATION ACTIVITIES

#### CURRENT WORKING GROUPS

##### Working group 11

##### Website

Owner Olivier GILSON  
Phone +352 48 48 80 51 08  
[olivier.gilson@efa.eu](mailto:olivier.gilson@efa.eu)

##### Working group 16

##### Legal and public relations

Owners Claudine FRUTSAERT  
Phone +352 44 24 24 43 15  
[claudine.frutsaert@axa.lu](mailto:claudine.frutsaert@axa.lu)

Jean-Marie LEGENDRE

Phone +352 24 67 26 07  
[Jean-Marie.LEGENDRE@ca-luxembourg.com](mailto:Jean-Marie.LEGENDRE@ca-luxembourg.com)

##### Working group 20

##### Funds practices and recommendations AML

Owner Patrick Watelet  
Phone +352 45-14-14-231  
[patrick.watelet@citi.com](mailto:patrick.watelet@citi.com)

##### Working group 21

##### Practical interpretation of fund investment restrictions

Owner Tim WINFIELD  
Phone +352 34 10 23 85  
[tim.winfield@jpmorgan.com](mailto:tim.winfield@jpmorgan.com)

##### Working group 27

##### Training IFBL

Coordinator Sundhevy GOÏOT  
Phone +352 621 30 23 63  
[sundhevy.goiot@maycoso.lu](mailto:sundhevy.goiot@maycoso.lu)

##### Working group 29

##### Market abuse

Coordinator Cyril MATHIEU  
Phone +352 40 46 46 400  
[cyrilmathieu@lu.hsbc.com](mailto:cyrilmathieu@lu.hsbc.com)

##### Working group 30

##### Domiciliary agent

Coordinator Sophie RASE  
Phone +352 40 25 05 408  
[sophie.rase@maitlandgroup.com](mailto:sophie.rase@maitlandgroup.com)

Coordinateur Marie-Hélène CLAUDE

Téléphone +352 48 18 28 39 03  
[marie-helene.claude@alterdomus.lu](mailto:marie-helene.claude@alterdomus.lu)

##### Working group 33

##### Answers to questions of members

# Le Bulletin

Coordinateur Carine VAN MULDER  
Téléphone +352 47 97 28 15797 2815  
[CARINE.VAN-MULDER@kbl-bank.com](mailto:CARINE.VAN-MULDER@kbl-bank.com)

Coordinator Vincent WILLEM  
Phone +352 49 924 3956  
[CARINE.VAN-MULDER@kbl-bank.com](mailto:CARINE.VAN-MULDER@kbl-bank.com)

## **Groupe de travail 34**

### **Tables rondes**

Coordinateur Charles VAN DOORSLAER  
Téléphone +352 47 97 39 09  
[charles.van-doorslaer@kbl-bank.com](mailto:charles.van-doorslaer@kbl-bank.com)

## **Working group 34**

### **Round tables**

Coordinator Charles VAN DOORSLAER  
Phone +352 47 97 39 09  
[charles.van-doorslaer@kbl-bank.com](mailto:charles.van-doorslaer@kbl-bank.com)

## **Groupe de travail 35**

### **Doctrine**

Coordinateur Guillaume BEGUE  
Téléphone +352 26 96 22 31  
[guillaume.begue@bnpparibas.com](mailto:guillaume.begue@bnpparibas.com)

## **Working group 35**

### **Doctrine**

Coordinator Guillaume BEGUE  
Phone +352 26 96 22 31  
[guillaume.begue@bnpparibas.com](mailto:guillaume.begue@bnpparibas.com)

## **MEMBRES ET VIE ASSOCIATIVE**

## **MEMBERS AND ASSOCIATION ACTIVITIES**

### **Nombre de membres (au 30/09/2010):**

Banques	222
Fonds	93
Fonds / Banques	28
Assurances	58
Consultants / Réviseurs	35
Admin. et domiciliation de sociétés	17
Avocats	8
PSF	48
Gestion de fortune	22
Autres	14
<b>Effectif total:</b>	<b>545</b>

Membres effectifs	440
Membres d'honneur	105

**Effectif total: 545**

### **Réunions et activités:**

Mensuellement	Réunions du conseil d'administration
1 / 2 x par an	Réunions plénières
2 / 3 x par an	Rencontres informelles autour d'un thème

### **Number of members (as per 30/09/2010):**

Banking sector	222
Funds sector	93
Funds / Banking sector	28
Insurance sector	58
Consultants / Auditors	35
Admin. and company domiciliation	17
Law firms	8
SFP	48
Asset management	22
Other	14
<b>Total number:</b>	<b>545</b>

Active members	440
Honorary members	105

**Total number: 545**

### **Meetings and activities:**

Monthly	Board meetings
1 / 2 x per year	Plenary assemblies
2 / 3 x per year	Informal meetings on a subject



# Le Bulletin

---

## – Conseil d’administration:

Jean-Noël LEQUEUE	Président
Claudine FRUTSAERT	Vice-Président, section assurances
Patrick WATELET	Vice-Président, section fonds
Vincent SALZINGER	Vice-Président, section banques
Marie-Hélène CLAUDE	Trésorière
Guillaume BEGUE	Administrateur
Sundhevy GOÏOT	Administrateur
Jean-Marie LEGENDRE	Administrateur, Président honoraire
Custodio PORTASIO	Administrateur
Thierry GROSJEAN	Administrateur
Patrick SCHOTT	Administrateur
Olivier GILSON	Conseiller
Patrick CHILLET	Conseiller
Tim WINFIELD	Conseiller
Karine VILRET-HUOT	Conseiller
Benoît MARTIN	Conseiller
Rob Sonnenschein	Conseiller

---

## – Secrétariat de l’ALCO:

Emilie Schmitt  
[secretariat@alco.lu](mailto:secretariat@alco.lu)  
2 rue de l'Eau  
L-1449 Luxembourg  
Tél: 26-63-86-25

---

## – Secrétariat du Bulletin:

Emilie Schmitt  
[secretariat@alco.lu](mailto:secretariat@alco.lu)

---

## – Comité de rédaction:

Claudine FRUTSAERT (responsable), Patrick SCHOTT, Jean-Marie LEGENDRE, Julie BECKER, Leen BOM, Stefano PIERANTOZZI, Olivier GILSON, Jean-François PEMMERS, Sandra SIMON, Ingrid MALMEDY, Sundhevy GOÏOT, Karine VILRET-HUOT, Jean Noël LEQUEUE, les membres du GT 33 et du GT34

VISITEZ NOTRE SITE WEB : [www.alco.lu](http://www.alco.lu)