

# COMMISSION de SURVEILLANCE du SECTEUR FINANCIER

Luxembourg, le 19 décembre 2008

A tous les professionnels du secteur financier soumis à la surveillance de la CSSF et qui sont visés par la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme

## CIRCULAIRE CSSF 08/387

**Concerne :** Lutte contre le blanchiment et le financement du terrorisme et prévention de l'utilisation du secteur financier à des fins de blanchiment et de financement du terrorisme

à lire conjointement avec les circulaires CSSF 10/476 et CSSF 11/528

### S O M M A I R E

#### **Introduction** (1-5)

- I Evolution du cadre législatif et réglementaire (1-2)
- II Personnes responsables en matière de lutte contre le blanchiment et le financement du terrorisme (3)
- III Approche basée sur le risque (4-5)

#### **Partie I Les infractions de blanchiment et de financement du terrorisme** (6-12)

##### **Titre 1 L'infraction de blanchiment** (7-10)

- Chapitre 1 Les infractions primaires (8)
- Chapitre 2 L'élément matériel (9)
- Chapitre 3 L'élément intentionnel (10)

##### **Titre 2 L'infraction de financement du terrorisme** (11)

##### **Titre 3 Les sanctions pénales** (12)

**Partie II Volet préventif du dispositif de lutte contre le blanchiment et le financement du terrorisme: les obligations professionnelles** (13-153)

**Titre 1 Le champ d'application des obligations professionnelles** (13-20)

Chapitre 1 Le champ d'application matériel (13)

Chapitre 2 Le champ d'application personnel (14-20)

Section 1 Les professionnels du secteur financier exerçant au Luxembourg (14-16)

Section 2 Les succursales et filiales à l'étranger des professionnels du secteur financier visés exerçant au Luxembourg (article (2)) (17-20)

Sous-section 1 Principe général (17-18)

Sous-section 2 Filiales et succursales établies dans des pays tiers dont la réglementation ne permet pas d'appliquer les mesures équivalentes (19)

Sous-section 3 Contrôle du respect des obligations professionnelles auprès des filiales et succursales (20)

**Titre 2 Le contenu des obligations professionnelles** (21-145)

Chapitre 1 Les obligations de vigilance à l'égard de la clientèle (23-79)

Section 1 Mesures de vigilance à l'égard de la clientèle (23-66)

Sous-section 1 Identification des clients et vérification de leur identité (25- 46)

A. Clients en relation d'affaires (26-43)

Paragraphe 1

Notions de relation d'affaires et de client (26-28)

Paragraphe 2

Caractère préalable de l'identification et de la vérification de l'identité (29-34)

a. Principe général (29-31)

    Clients de tiers introducteurs (31)

b. Exception (32)

    Sociétés en voie de formation

c. Autorisation écrite nécessaire (33-34)

### Paragraphe 3

Identification et vérification de l'identité du client sur base de documents, de données ou d'informations de source fiable et indépendante (35-43)

- a. Client personne physique (36-38)
- b. Client personne morale (39-42)
  - I. Identification et vérification de l'identité de la personne morale (40-41)
  - II. Identification et vérification de l'identité des représentants (mandataires) de la personne morale (42)
- c. Vérification par rapport aux situations exigeant l'application de mesures de vigilance renforcées (43)

### B. Clients occasionnels (44-46)

#### Sous-section 2 Identification des bénéficiaires effectifs (47-59)

Paragraphe 1 Définition du bénéficiaire effectif (47-48)

Paragraphe 2 Règles générales (49-51)

Paragraphe 3 Client personne physique (52-56)  
Cas particulier : Clients dont l'activité professionnelle implique la conservation de fonds de tiers (p.ex. avocats, notaires, ...) (54-55)

Paragraphe 4 Client personne morale (57-59)

Paragraphe 5 Sociétés domiciliées (60)

#### Sous-section 3 Obtention d'informations sur l'objet et la nature envisagée de la relation d'affaires (61-62)

#### Sous-section 4 Exercice d'une vigilance constante de la relation d'affaires et tenue à jour des documents donnés ou informations détenues (63-66)

Paragraphe 1 La vigilance constante de la relation d'affaires (64-65)

Paragraphe 2 La tenue à jour des documents et informations (66)

### Section 2 Obligation d'accorder une attention particulière à certaines activités et transactions (67-75)

- Sous-section 1 Transactions particulièrement susceptibles d'être liées au blanchiment ou au financement du terrorisme (67-72)
  - Sous-section 2 Procédures, systèmes et mécanismes à mettre en œuvre pour détecter les transactions suspectes (73-74)
  - Sous-section 3 Consignation écrite des résultats des analyses effectuées (75)
- Section 3 Obligation de conserver certains documents et informations (76-79)
- Sous-section 1 Documentation relative à l'identification et à la vérification de l'identité (76)
  - Sous-section 2 Documentation relative aux transactions (77-78)
  - Sous-section 3 Conservation des documents et informations (79)

## Chapitre 2 Obligations renforcées de vigilance à l'égard de la clientèle (80-94)

- Section 1 Entrée en relation d'affaires à distance (81-84)
- Section 2 Les personnes politiquement exposées (« PPE ») (85-88)  
Régime applicable (87-88)
- Section 3 Banques correspondantes (89-90)
- Section 4 Pays et territoires non coopératifs (PTNC) et situations similaires (91-94)

## Chapitre 3 Exécution des mesures de vigilance par des tiers (95-104)

- Section 1 Régime du tiers introducteur (97-101)
  - Sous-section 1 Tiers acceptés (98-100)
  - Sous-section 2 Conditions (101)
- Section 2 Externalisation (102-104)

## Chapitre 4 Obligations simplifiées de vigilance à l'égard de la clientèle (105-111)

## Chapitre 5 Obligations d'organisation interne adéquate (112-116)

- Section 1 Obligation d'instaurer des procédures écrites de contrôle interne et de communication (113)
- Section 2 Obligation de former et de sensibiliser le personnel (114-115)
- Section 3 Obligation de disposer de systèmes permettant de répondre aux demandes d'informations des autorités luxembourgeoises (116)

## Chapitre 6 Obligations de coopération avec les autorités (117-144)

- Section 1 Obligation générale de coopérer avec les autorités chargées de l'application des lois (117)
- Section 2 Obligation de coopérer avec les autorités luxembourgeoises responsables de la lutte contre le blanchiment et le financement du terrorisme (118-144)
  - Sous-section 1 Obligation de fournir au procureur d'Etat auprès du tribunal d'arrondissement à Luxembourg, à sa demande, toutes les informations requises (119)
  - Sous-section 2 Obligation d'informer, de sa propre initiative, le procureur d'Etat auprès du tribunal d'arrondissement à Luxembourg de tout soupçon ou certitude d'un blanchiment ou d'un financement du terrorisme (120-144)
    - Paragraphe 1 Personnes chargées d'informer le procureur d'Etat (120-122)
    - Paragraphe 2 Circonstances dans lesquelles le procureur d'Etat doit être informé (123-132)
      - I. Précisions des critères à prendre en compte pour détecter un blanchiment ou un financement du terrorisme (124-126)
      - II. Précisions sur l'obligation d'information en matière de lutte contre le blanchiment et le financement du terrorisme (127-130)
      - III. Précisions sur l'obligation d'information en cas d'entrée en contact sans nouer une relation d'affaires et/ou sans effectuer une transaction (131-132)

- Paragraphe 3 Dispense de l'obligation au secret professionnel et absence de responsabilité de toute sorte en cas de déclaration de bonne foi (133-136)
- Paragraphe 4 Obligation de transmettre les mêmes informations à la CSSF que celles transmises au procureur d'Etat (137)
- Paragraphe 5 Pouvoirs du procureur d'Etat à la suite d'une information (138-139)
- I. Instruction de blocage (138)
  - II. Instruction de blocage limitée dans le temps (139)
- Paragraphe 6 Comportement du professionnel du secteur financier en cas de transaction suspecte et d'information du procureur d'Etat (140-144)
- I. Interdiction d'exécuter la transaction avant d'avoir informé le procureur d'Etat (140-141)
  - II. Interdiction d'avertir le client dont les transactions se trouvent bloquées ou pourraient être bloquées du fait d'une instruction du procureur d'Etat (142)
  - III. Relations avec les organes internes de contrôle du groupe (143-144)

Chapitre 7 Obligations en cas de virement et de transfert de fonds (145)

**Titre 3 Contrôle du respect des obligations professionnelles (146-152)**

Chapitre 1 L'autorité compétente : la CSSF (146-147)

Chapitre 2 Le réviseur d'entreprises (148-151)

Chapitre 3 L'auditeur interne et la personne chargée plus particulièrement de la lutte contre le blanchiment et le financement du terrorisme (152)

**Titre 4 Sanctions pénales et administratives en cas de non respect des obligations professionnelles (153)**

**Partie III Dispositions abrogatoires (154)**

Annexes (I - VI)

## **Introduction**

### **I Evolution du cadre législatif et réglementaire**

1. Depuis que la loi du 7 juillet 1989 avait pour la première fois en droit luxembourgeois érigé en infraction pénale spéciale le blanchiment du produit d'une activité illicite, en l'occurrence le trafic des stupéfiants, et que la circulaire IML 89/57 avait dégagé les règles à observer par les professionnels du secteur financier pour leur éviter d'être utilisés à des fins de blanchiment, la législation et la réglementation luxembourgeoises en matière de lutte contre le blanchiment ont été constamment renforcées.

D'abord, la loi du 5 avril 1993 relative au secteur financier, en transposant la directive communautaire 91/308/CEE et les recommandations du Groupe d'action financière sur le blanchiment de capitaux (« GAFI ») émises en 1990, a défini un certain nombre d'obligations professionnelles à respecter par les professionnels du secteur financier afin d'éviter qu'ils ne soient utilisés à des fins de blanchiment.

Ensuite, la circulaire IML 94/112 (abrogeant la circulaire IML 89/57) avait fourni, sur base notamment des dispositions précitées de la loi du 5 avril 1993, des indications et instructions détaillées sur la façon dont les professionnels du secteur financier sont censés exécuter les obligations professionnelles que la loi leur impose.

Depuis lors, le dispositif de lutte contre le blanchiment a considérablement évolué tant au niveau international que national.

Au niveau international, il convient de citer la première révision des 40 recommandations du GAFI en 1996, l'extension de la lutte contre le blanchiment au financement du terrorisme par l'émission des recommandations spéciales du GAFI en octobre 2001, l'adoption de la directive 2001/97/CE en décembre 2001 qui a modifié la directive 91/308/CEE susdite et finalement la deuxième révision des 40 recommandations du GAFI en juin 2003.

Au niveau national, il y a lieu de citer la loi du 11 août 1998 qui, entre autres, a étendu le champ d'application de l'infraction de blanchiment, la loi du 12 août 2003 portant répression du terrorisme et de son financement ainsi que la loi du 12 novembre 2004 qui a transposé la directive 2001/97/CE, tout en complétant et renforçant le dispositif législatif luxembourgeois sur un certain nombre de points à la lumière des expériences acquises au cours des années précédentes en matière de lutte contre le blanchiment au niveau international et au Luxembourg.

Toute cette évolution a rendu nécessaire l'émission par la Commission de surveillance du secteur financier (« CSSF ») de nombreuses circulaires constituant des compléments à la circulaire de base IML 94/112, qui avaient pour objet soit de la modifier, soit de la préciser sur certains points.

La circulaire CSSF 05/211 du 13 octobre 2005 a alors été introduite dans le but de regrouper, d'une façon cohérente dans une circulaire unique, toutes les indications et instructions concernant l'application pratique des obligations professionnelles, ceci afin d'améliorer la lisibilité de la réglementation existante.

Par ailleurs, en prenant en compte les changements intervenus ainsi que les expériences acquises, elle a adapté les indications et instructions précises et détaillées existantes sur la

façon dont les professionnels du secteur financier sont censés exécuter les obligations professionnelles que la loi leur impose afin d'éviter d'être utilisés à des fins de blanchiment ou de financement du terrorisme.

2. L'évolution continue de la réglementation en matière de lutte contre le blanchiment et le financement du terrorisme a ensuite donné lieu à l'adoption de plusieurs textes communautaires touchant directement à la réglementation applicable aux professionnels surveillés par la CSSF :

- la directive 2005/60/CE du 26 octobre 2005 relative à l'utilisation du système financier aux fins de blanchiment et de financement du terrorisme ;
- la directive 2006/70/CE du 1er août 2006 a introduit des mesures de mise en œuvre de la directive 2005/60/CE 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 ;
- le règlement (CE) n° 1781/2006 du 15 novembre 2006 relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds, afin de contribuer à la protection des systèmes de paiement contre les flux d'argent sale.

Les directives précitées, basées dans une large mesure sur les 40 recommandations du GAFI largement modifiées et développées en 2003, ont été transposées en droit luxembourgeois par une loi du 17 juillet 2008 portant transposition desdites directives et modifiant la loi du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme. Cette loi a modifié l'article 39 de la loi modifiée du 5 avril 1993 relative au secteur financier en y adaptant les références aux nouvelles dispositions applicables et, en matière de virements électroniques, au règlement 1781/2006 du 15 novembre 2006 relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds.

Une deuxième loi datant du même jour, la loi du 17 juillet 2008, également relative à la lutte contre le blanchiment et contre le financement du terrorisme mais de nature essentiellement pénale, a adapté l'article 506-1 du code pénal afin de mettre le dispositif luxembourgeois en conformité avec les exigences internationales en ce qui concerne la définition du blanchiment.

La présente circulaire, qui remplace la circulaire CSSF 05/211 du 13 octobre 2005, se situe dans la suite de l'évolution de la réglementation décrite ci-avant.

Les points forts de la nouvelle réglementation en matière de lutte contre le blanchiment et le financement du terrorisme, déjà partiellement anticipés par la circulaire CSSF 05/211 et exposés en détail ci-après, peuvent être résumés comme suit :

- Introduction d'une approche générale basée sur le risque : comme le risque de blanchiment ou de financement du terrorisme n'est pas toujours le même, il convient que les professionnels concentrent leurs efforts surtout sur les clients et situations

présentant un risque réel de blanchiment ou de financement du terrorisme. Sur cette base, la nouvelle législation introduit des mesures de vigilance standard que les professionnels doivent appliquer systématiquement mais dont ils peuvent adapter l'étendue en fonction de l'appréciation du risque. La loi du 17 juillet 2008 prévoit ensuite des cas spécifiques limitativement énumérés où des mesures de vigilance simplifiées sont suffisantes. Il existe finalement des situations où les professionnels doivent en sus des mesures de vigilance standard appliquer des mesures de vigilance renforcées alors qu'elles comportent un risque accru de blanchiment ou de financement du terrorisme : il s'agit de situations jugées comme telles par les professionnels, ainsi que de plusieurs cas spécifiques expressément visés par la loi où le risque de blanchiment ou de financement du terrorisme est particulièrement élevé.

- Dispositions précises sur l'identification du client et définitions détaillées de certaines notions comme celle de « bénéficiaire effectif » et de « personne politiquement exposée » ;
- Description détaillée du déroulement de la procédure d'identification du client ;
- Recours à des tiers déterminés dans le cadre de la procédure d'identification du client ;
- Une innovation majeure introduite dans le cadre de la nouvelle législation concerne le nouveau mode de détermination des pays tiers reconnus comme disposant d'un dispositif en matière de lutte contre le blanchiment et le financement du terrorisme équivalent à celui prescrit par la loi du 12 novembre 2004 modifiée par celle du 17 juillet 2008. Suivant un accord intervenu entre les Etats membres, une liste commune des pays tiers considérés comme disposant d'un système de lutte contre le blanchiment et le financement du terrorisme équivalent a été établie. Cette liste a été rendue obligatoire au Luxembourg par le règlement grand-ducal du 29 juillet 2008 portant établissement de la liste des « pays tiers imposant des obligations équivalentes » au sens de la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme (Mémorial A n° 119 du 11.08.2008, p. 1811) (Annexe I). Il convient de noter que figurent sur la liste les pays considérés actuellement comme disposant d'un dispositif équivalent. Cette liste est donc sujette à révision, en particulier sur la base des rapports d'évaluation publics adoptés par le GAFI, les organismes régionaux de type GAFI, le Fonds monétaire international ou la Banque mondiale, rapports établis sur base des Recommandations du GAFI et suivant une méthodologie d'évaluation commune.

Il convient de rappeler dans ce contexte la signification de « pays tiers » au sens de l'article 1<sup>er</sup> (4) et (5) de la loi modifiée du 12 novembre 2004. Il s'agit d'un Etat autre qu'un Etat membre de l'Union européenne ou de l'Espace économique européen. Contrairement aux pays tiers qui ne sont considérés comme équivalents que s'ils figurent sur la liste précitée, les Etats membres de l'Union européenne et de l'Espace économique européen sont équivalents de plein droit.

## **II Personnes responsables en matière de lutte contre le blanchiment et le financement du terrorisme**

3. Les dirigeants ayant obtenu l'agrément requis par la loi sont responsables pour assurer le respect des dispositions légales et réglementaires, mettre en place, conformément aux dispositions reprises au point 112 et suivants de la présente circulaire, des politiques et des procédures internes en matière de lutte contre le blanchiment et le financement du terrorisme et en assurer leur bonne application.

En ce qui concerne plus particulièrement l'organisation interne, ils doivent veiller à la mise en place de procédures adéquates de contrôle interne et de communication afin de prévenir et d'empêcher la réalisation d'opérations liées au blanchiment ou au financement du terrorisme, y compris des procédures d'acceptation, d'identification et de suivi des clients ainsi que d'évaluation et de gestion des risques.

Ils doivent également définir le besoin en ressources humaines et techniques pour atteindre ces objectifs.

Sans préjudice de la responsabilité des dirigeants susdits, ceux-ci doivent désigner une personne chargée plus particulièrement de la lutte contre le blanchiment et le financement du terrorisme.

En ce qui concerne les établissements de crédit et les entreprises d'investissement, il doit s'agir du responsable de la fonction *compliance*. Conformément à la circulaire CSSF 04/155 relative à la fonction *compliance*, le responsable de la fonction *compliance* doit notamment veiller à ce que le professionnel du secteur financier dispose de règles en matière de lutte contre le blanchiment et le financement du terrorisme et assurer le respect de ces règles. Par ailleurs, il est la personne de contact principale des autorités compétentes dans cette matière et, en particulier, celui qui est en charge des déclarations de soupçons au procureur d'Etat auprès du tribunal d'arrondissement de Luxembourg.

Pour ce qui est des autres professionnels du secteur financier, il doit s'agir d'un dirigeant ayant obtenu l'agrément requis par la loi et qui a été spécifiquement désigné pour exercer cette fonction.

## **III Approche basée sur le risque**

4. Dans le cadre de la lutte contre le blanchiment et le financement du terrorisme, les professionnels du secteur financier doivent adopter une approche ciblée par rapport au risque réel, aussi bien lors de l'identification des clients que lors du suivi des transactions, en tenant compte des spécificités de leurs activités respectives et des différences d'échelle et de taille qu'ils présentent.

5. Le dispositif luxembourgeois en matière de lutte contre le blanchiment et le financement du terrorisme comportant, à la lumière de la réglementation existante au niveau européen et mondial, un volet pénal et un volet préventif, la présente circulaire traitera dans la partie I des infractions de blanchiment et de financement du terrorisme et dans sa partie II des obligations professionnelles.

## **Partie I Les infractions de blanchiment et de financement du terrorisme**

6. Le droit luxembourgeois connaît les infractions pénales spéciales de blanchiment et de financement du terrorisme.

L'article 1<sup>er</sup> de la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et le financement du terrorisme dispose que:

- Par « blanchiment » est désigné tout acte tel que défini aux articles 506-1 du code pénal et 8-1 de la loi modifiée du 19 février 1973 concernant la vente de substances médicamenteuses et la lutte contre la toxicomanie ;
- Par « financement du terrorisme » est désigné tout acte tel que défini à l'article 135-5 du code pénal.

### **Titre 1 L'infraction de blanchiment**

7. En vertu des articles 506-1 et 8-1 susdits, commettent une infraction de blanchiment :

- « ceux qui ont sciemment facilité, par tout moyen, la justification mensongère de l'origine des biens formant l'objet ou le produit, direct ou indirect, ou constituant un avantage patrimonial quelconque tiré de l'une ou de plusieurs des infractions primaires visées ;
- ceux qui ont sciemment apporté leur concours à une opération de placement, de dissimulation ou de conversion des biens formant l'objet ou le produit direct ou indirect des infractions primaires visées ou constituant un avantage patrimonial quelconque tiré de l'une ou de plusieurs de ces infractions ;
- ceux qui ont acquis, détenu ou utilisé les biens formant l'objet ou le produit direct ou indirect des infractions primaires visées ou constituant un avantage patrimonial quelconque tiré de l'une ou de plusieurs de ces infractions, sachant, au moment où ils les recevaient, qu'ils provenaient de l'une ou plusieurs des infractions visées ou de la participation à l'une ou plusieurs de ces infractions ».

Ces articles donnent une définition de l'infraction de blanchiment tout en énumérant les faits constitutifs de ce délit et en spécifiant les catégories d'infractions primaires qui pourront donner lieu à ce délit.

## **Chapitre 1 Les infractions primaires**

8. Le blanchiment présuppose l'existence d'une infraction primaire dont l'objet ou les produits peuvent donner lieu à une infraction de blanchiment.

Les infractions primaires comprennent celles indiquées ci-après. Elles sont classées en suivant la liste des catégories d'infractions désignées retenue dans le glossaire des 40 recommandations du GAFI. La présentation ne peut toutefois pas être exhaustive, puisque la liste en question ne vise pas seulement toutes les infractions explicitement citées à l'article 506-1 du code pénal et à l'article 8-1 de la loi du 19 février 1973 concernant la vente de substances médicamenteuses et la lutte contre la toxicomanie mais aussi d'autres infractions qui, conformément au même article 506-1 dernier tiret, sont punies « d'une peine privative de liberté d'un minimum supérieur à 6 mois » :

Participation à un groupe criminel organisé et à un racket :

- les crimes et délits commis dans le cadre ou en relation avec une association formée dans le but d'attenter aux personnes ou propriétés ou dans le cadre ou en relation avec une organisation criminelle (articles 322 à 324 ter du Code pénal) ;

Terrorisme, y compris son financement :

- les infractions de terrorisme et de financement du terrorisme (articles 135-1 à 135-6 du Code pénal) ;

Traite d'êtres humains et trafic illicite de migrants :

- les infractions sexuelles sur mineurs (article 379 du Code pénal) ;
- le proxénétisme (article 379 bis du Code pénal) ;
- les infractions à l'article 33 de la loi modifiée du 28 mars 1972 concernant: 1° l'entrée et le séjour des étrangers; 2° le contrôle médical des étrangers; 3° l'emploi de la main-d'œuvre étrangère, tel que repris à l'article 143 de la loi du 29 août 2008 portant sur la libre circulation des personnes et l'immigration ;

Exploitation sexuelle, y compris celle des enfants :

- les infractions aux articles 372 à 377 du code pénal ;
- les infractions sexuelles sur mineurs (article 379 du Code pénal) ;
- le proxénétisme (article 379 bis du Code pénal) ;

Trafic illicite de stupéfiants et de substances psychotropes :

- les infractions à l'article 8-1 de la loi du 19 février 1973 concernant la vente de substances médicamenteuses et la lutte contre la toxicomanie ;

Trafic d'armes :

- les infractions à la législation sur les armes et munitions (notamment la loi du 15 mars 1983 sur les armes et munitions) ;

Trafic illicite de biens volés et autres biens :

- les infractions à l'article 10 de la loi du 21 mars 1966 concernant a) les fouilles d'intérêt historique, préhistorique, paléontologique ou autrement scientifique ; b) la sauvegarde du patrimoine culturel mobilier ;
- les infractions à l'article 5 de la loi du 11 janvier 1989 réglant la commercialisation des substances chimiques à activité thérapeutique ;
- les infractions à l'article 18 de la loi du 25 novembre 1982 réglant le prélèvement de substances d'origine humaine ;

Corruption :

- la corruption publique et privée (articles 246 à 253, 310 et 310-1 du code pénal) ;

Fraude et escroquerie :

- les infractions aux articles 489 à 490 du code pénal (banqueroute) ;
- les infractions aux articles 491 à 495 du code pénal (abus de confiance) ;
- les infractions à l'article 496 du code pénal (escroquerie) ;
- les fraudes aux intérêts financiers de l'Etat et des institutions internationales (articles 496-1 à 496-4 du code pénal) ;

Contrefaçon de monnaie :

- les infractions aux articles 162 à 178 du code pénal (dans les cas où la peine minimale prévue est supérieure à 6 mois)<sup>1</sup> ;

Contrefaçon et le piratage de produits :

- les infractions aux articles 184, 187, 187-1, 191 et 309 du code pénal ;
- les infractions aux articles 82 à 85 de la loi du 18 avril 2001 sur le droit d'auteur ;

Crimes et délits contre l'environnement :

- les infractions à l'article 64 de la loi modifiée du 19 janvier 2004 concernant la protection de la nature et des ressources naturelles ;
- les infractions à l'article 9 de la loi modifiée du 21 juin 1976 relative à la lutte contre la pollution de l'atmosphère ;
- les infractions à l'article 25 de la loi modifiée du 10 juin 1999 relative aux établissements classés ;
- les infractions à l'article 26 de la loi du 29 juillet 1993 concernant la protection et la gestion de l'eau ;
- les infractions à l'article 35 de la loi modifiée du 17 juin 1994 relative à la prévention et à la gestion des déchets ;

Meurtres et blessures corporelles graves :

- les infractions aux articles 392 à 410 du code pénal (dans les cas où la peine minimale prévue est supérieure à 6 mois)<sup>1</sup> ;

---

<sup>1</sup> En vertu de l'article 506-1 (1) dernier tiret

Enlèvement, séquestration et prise d'otages :

- les infractions aux articles 368 à 370 du code pénal (enlèvement de mineurs) ;
- les infractions à l'article 442-1 du code pénal (prise d'otages) <sup>1</sup> ;

Vol :

- les infractions aux articles 463 et 464 du code pénal ;
- les infractions aux articles 467 à 479 du code pénal (vol qualifié, vol avec violences ou menaces) (dans les cas où la peine minimale prévue est supérieure à 6 mois) <sup>1</sup> ;

Contrebande :

- les infractions aux articles 220 et 231 de la loi générale sur les douanes et accises ;

Extorsion :

- les infractions à l'article 470 du code pénal <sup>1</sup> ;

Faux :

- les infractions aux articles 193 à 212 du code pénal (dans les cas où la peine minimale prévue est supérieure à 6 mois) <sup>1</sup> ;

Piraterie :

- les infractions à l'article 31 de la loi modifiée du 31 janvier 1948 relative à la réglementation de la navigation aérienne <sup>1</sup> ;
- les infractions à l'article 64 du code disciplinaire et pénal pour la marine <sup>1</sup> ;

Délits d'initiés et manipulation de marchés :

- les infractions à l'article 32 de la loi du 9 mai 2006 relative aux abus de marché.

Il convient de souligner que les éléments constitutifs de l'infraction de blanchiment sont réunis même lorsque l'infraction primaire a été commise à l'étranger, à condition cependant que cette dernière constitue une infraction primaire au Luxembourg et à l'étranger.

## **Chapitre 2 L'élément matériel**

**9.** Le blanchiment consiste dans tout acte ayant trait au produit ou à l'objet, c.-à-d. à tout avantage économique, tiré de l'infraction primaire.

La définition légale du blanchiment est très large et vise un ensemble de stratagèmes qui ont tous pour but de procurer une justification mensongère de l'origine des biens formant l'objet ou le produit tirés des infractions primaires.

## **Chapitre 3 L'élément intentionnel**

**10.** Pour commettre une infraction de blanchiment, l'élément intentionnel est déterminant. Quiconque blanchit sciemment les produits ou l'objet provenant d'une des infractions primaires visées commet une infraction de blanchiment.

## **Titre 2 L'infraction de financement du terrorisme**

**11.** En vertu de l'article 135-5 du Code pénal, constitue une infraction de financement du terrorisme « le fait de fournir ou de réunir par quelque moyen que ce soit, directement ou indirectement, illicitement et délibérément, des fonds, des valeurs ou des biens de toute nature, dans l'intention de les voir utilisés ou en sachant qu'ils seront utilisés, en tout ou en partie, en vue de commettre une ou plusieurs des infractions prévues aux articles 135-1 à 135-4 et 442-1<sup>2</sup>, même s'ils n'ont pas été effectivement utilisés pour commettre une de ces infractions ».

## **Titre 3 Les sanctions pénales**

**12.** Quiconque commet une infraction de blanchiment est passible de peines d'emprisonnement (1 à 5 ans) et/ou amendes (1.250 à 1.250.000 euros) prévues aux articles 506-1 et 8-1 susdits.

Il convient de rappeler que sont punissables aux termes de ces articles, l'auteur du blanchiment, les co-auteurs et les complices.

Quiconque commet une infraction de financement de terrorisme est passible des peines prévues aux articles 135-1 à 135-4 et 442-1 du code pénal suivant les distinctions y établies.

Il convient de relever ici que la violation des obligations professionnelles telles que décrites aux points 13 à 144 de la présente circulaire est également pénalement sanctionnée tel que précisé au point 153 ci-dessous.

---

<sup>2</sup> L'article 442-1 du code pénal vise l'infraction de prise d'otages.

## **Partie II Volet préventif du dispositif de lutte contre le blanchiment et contre le financement du terrorisme : les obligations professionnelles**

### **Titre 1 Le champ d'application des obligations professionnelles**

#### **Chapitre 1 Le champ d'application matériel**

**13.** La loi du 12 novembre 2004 avait étendu les obligations professionnelles existant en matière de lutte contre le blanchiment à la lutte contre le financement du terrorisme, infraction incriminée par l'article 135-5 du code pénal. Par conséquent, les moyens préventifs à mettre en œuvre pour combattre le blanchiment et le financement du terrorisme sont de même nature.

#### **Chapitre 2 Le champ d'application personnel**

##### **Section 1 Les professionnels du secteur financier exerçant au Luxembourg**

**14.** Le cercle des personnes soumises aux obligations professionnelles a été étendu par la loi modifiée du 12 novembre 2004 à d'autres acteurs du secteur financier ainsi qu'à une série d'autres personnes déterminées ne relevant pas de ce secteur, mais particulièrement concernées par la lutte contre le blanchiment et le financement du terrorisme.

**15.** La présente circulaire vise exclusivement les professionnels du secteur financier soumis aux obligations professionnelles qui tombent sous la surveillance de la CSSF. Ils sont dans la suite indifféremment appelés « professionnels » ou « professionnels du secteur financier ».

Il s'agit en l'occurrence des :

- établissements de crédit et autres professionnels du secteur financier (PSF) agréés ou autorisés à exercer leur activité au Luxembourg en vertu de la loi modifiée du 5 avril 1993 relative au secteur financier.  
Sont visés non seulement les établissements de crédit ayant le statut de banque universelle, mais également les établissements de type particulier tels que les établissements de monnaie électronique ;
- autres professionnels du secteur financier (PSF) : sont visés non seulement tous les PSF spécifiquement énumérés à la partie I, chapitre 2 (articles 24 à 29-5) de la loi modifiée du 5 avril 1993 relative au secteur financier, mais également toutes les autres personnes exerçant une activité du secteur financier et agréées en vertu de l'article 13 (1) de la prédite loi ;

- organismes de placement collectif et sociétés d'investissement en capital à risque qui commercialisent leurs parts ou actions et qui sont visés par la loi modifiée du 20 décembre 2002 concernant les organismes de placement collectif ou par la loi du 13 février 2007 relative aux fonds d'investissement spécialisés ou par la loi du 15 juin 2004 relative à la société d'investissement en capital à risque (SICAR).

La loi modifiée du 12 novembre 2004 soumet aux obligations de vigilance les OPC qui commercialisent eux-mêmes leurs parts, c.-à-d. qui ont un contact direct avec les investisseurs, dans la mesure où ils exercent des activités de commercialisation de leurs parts sans passer par l'intermédiaire d'autres professionnels. Il faut préciser que les OPC qui commercialisent eux-mêmes leurs parts ont la possibilité de recourir à des tiers pour l'exécution matérielle des obligations de vigilance dans les conditions décrites aux points 95 à 104 ci-après.

Les souscriptions et rachats dans les OPC qui ne commercialisent pas eux-mêmes leurs parts passent nécessairement par des intermédiaires. Ces OPC ne sont pas soumis par la loi aux obligations de vigilance dans la mesure où l'intermédiaire est un établissement de crédit ou un établissement financier (tel que défini à l'article 2 (2) de la loi modifiée du 12 novembre 2004) soumis à des obligations équivalentes à celles prévues par la loi modifiée du 12 novembre 2004.

Au cas où l'intermédiaire n'est pas un établissement de crédit ou un établissement financier soumis à des obligations équivalentes à celles prévues par la loi modifiée du 12 novembre 2004, la responsabilité de l'identification de l'intermédiaire et des investisseurs (en tant que bénéficiaires effectifs) repose sur l'OPC/le professionnel luxembourgeois concerné.

- sociétés de gestion visées par la loi modifiée du 20 décembre 2002 concernant les organismes de placement collectif et qui commercialisent des parts ou des actions d'organismes de placement collectif ou qui exercent des activités additionnelles ou auxiliaires au sens de la loi modifiée du 20 décembre 2002 concernant les organismes de placement collectif ;
- fonds de pension sous la surveillance prudentielle de la CSSF, à savoir les assep et les sepcav réglementées par la loi modifiée du 13 juillet 2005.

**16.** Comme les dispositions de la loi modifiée du 12 novembre 2004 sont considérées d'ordre public, elles doivent être respectées par les professionnels du secteur financier exerçant leur activité au Luxembourg sous forme de succursale (article 2 (2) de la loi modifiée du 12 novembre 2004) ou de filiale.

En ce qui concerne les professionnels qui opèrent à Luxembourg en régime de libre prestation de services à partir d'un établissement à l'étranger, ils doivent appliquer les dispositions en matière de lutte contre le blanchiment et le financement du terrorisme de leur pays d'origine, à condition qu'ils soient soumis dans ce pays à une réglementation en matière de lutte contre le

blanchiment et le financement du terrorisme équivalente à la réglementation luxembourgeoise. Si tel n'est pas le cas, ils doivent respecter les dispositions luxembourgeoises en la matière.

Inversement, les professionnels luxembourgeois opérant en régime de libre prestation à l'étranger doivent appliquer les dispositions luxembourgeoises en matière de lutte contre le blanchiment et le financement du terrorisme.

## **Section 2 Les succursales et filiales à l'étranger des professionnels du secteur financier visés exerçant au Luxembourg (article 2(2))**

### **Sous-section 1 Principe général**

**17.** Les succursales et filiales (des professionnels visés par la présente circulaire) établies dans un autre Etat membre de l'Union européenne ou de l'Espace économique européen sont soumises dans l'Etat d'établissement respectif à une réglementation en matière de lutte contre le blanchiment et le financement du terrorisme de l'Etat d'établissement respectif équivalente à la réglementation luxembourgeoise et communautaire.

**18.** Concernant les succursales et filiales établies dans des pays tiers, c.-à-d. des pays qui ne sont membres ni de l'Union européenne ni de l'Espace économique européen, l'article 2 (2) de la loi modifiée du 12 novembre 2004 prévoit que parmi les professionnels visés par cette loi, les établissements de crédit et les établissements financiers (tels que définis à l'article 2 (2) de la loi modifiée du 12 novembre 2004) sont obligés d'appliquer des mesures au moins équivalentes à celles prescrites par la loi modifiée du 12 novembre 2004 ou la directive 2005/60/CE en matière de vigilance à l'égard du client et de conservation des documents dans leurs succursales et filiales majoritaires situées dans ces pays.

A cette fin, les établissements de crédit et les établissements financiers (tels que définis à l'article 2 (2) de la loi modifiée du 12 novembre 2004) communiquent les mesures et les procédures pertinentes, le cas échéant, aux succursales et aux filiales majoritaires situées dans des pays tiers.

Dans le cas de sociétés dans lesquelles un professionnel du secteur financier détient une participation non majoritaire mais comprise entre 20% et 50%, il appartient au professionnel du secteur financier, qui n'est pas entreprise mère, de faire tout son possible, de concert avec les autres actionnaires ou associés concernés, pour que soit mis en place dans ces sociétés un dispositif de contrôle en matière de lutte contre le blanchiment et le financement du terrorisme qui répond à des standards équivalents à ceux prescrits au Luxembourg.

### **Sous-section 2 Filiales et succursales établies dans des pays tiers dont la réglementation ne permet pas d'appliquer les mesures équivalentes**

**19.** Lorsqu'il est constaté par l'établissement concerné (tel que visé au point 18 ci-avant) qu'il existe dans le pays tiers des dispositions qui empêchent l'application de mesures au moins équivalentes aux normes luxembourgeoises ou européennes en matière de vigilance à l'égard du client et de conservation des documents, les établissements de crédit et les établissements financiers concernés doivent en informer la CSSF afin que le problème

puisse être communiqué à la Commission européenne conformément à l'article 31 (2) de la directive 2005/60/CE.

L'obligation d'informer la CSSF existe par rapport à tous pays tiers tels que définis à l'article 1 (5) de la loi modifiée du 12 novembre 2004 y compris ceux figurant sur la liste incluse dans le règlement grand-ducal du 29 juillet 2008 portant établissement de la liste des « pays tiers imposant des obligations équivalentes ».

Les établissements de crédit et établissements financiers concernés doivent en plus prendre des mesures supplémentaires pour faire face de manière efficace au risque de blanchiment ou de financement du terrorisme pouvant résulter de la situation/défaillance de la réglementation en question. Ils informeront la CSSF des mesures effectivement prises dans ce contexte.

Il convient de souligner que le non-respect des obligations professionnelles imposées aux succursales ou filiales concernées par la loi luxembourgeoise, ou par la loi étrangère lorsqu'elles sont plus sévères, risque de mettre en cause les autorisations requises pour le maintien de telles succursales ou filiales, voire le maintien de l'agrément requis pour exercer une activité du secteur financier au Luxembourg.

### **Sous-section 3 Contrôle du respect des obligations professionnelles auprès des filiales et succursales**

**20.** La personne chargée plus particulièrement de la lutte contre le blanchiment et le financement du terrorisme est responsable du contrôle du respect des obligations professionnelles auprès des filiales et succursales visées au point 18.

Par ailleurs, l'audit interne et la personne chargée plus particulièrement de la lutte contre le blanchiment et le financement du terrorisme de la maison mère ou du siège sont tenus de vérifier périodiquement, conformément au point 152 ci-après, que les filiales ou succursales visées aux points 18 et 19 respectent effectivement toutes leurs obligations professionnelles afin qu'elles soient au moins conformes à la loi modifiée du 12 novembre 2004 ou à la directive 2005/60/CE, conformément à l'article 2 (2) de ladite loi.

En ce qui concerne les sociétés visées au point 18, 3<sup>e</sup> alinéa, le professionnel du secteur financier s'efforce d'obtenir une synthèse des rapports d'audit et/ou de *compliance* de ces sociétés et les fait analyser par la personne chargée plus particulièrement de la lutte contre le blanchiment et le financement du terrorisme.

## **Titre 2 Le contenu des obligations professionnelles**

**21.** En vertu de la loi modifiée du 12 novembre 2004, les obligations professionnelles en matière de lutte contre le blanchiment et le financement du terrorisme applicables aux professionnels du secteur financier sont les suivantes :

1. obligation d'appliquer des mesures de vigilance à l'égard de la clientèle (article 3 (2)) ;
2. obligation d'accorder une attention particulière à certaines activités et transactions (article 3 (7)) ;
3. obligation de conserver certains documents et informations (article 3 (6)) ;
4. obligations d'organisation interne adéquate (article 4) ;
5. obligation de coopérer avec les autorités et obligation de déclaration (article 5).

S'ajoute une obligation professionnelle spécifique uniquement applicable aux établissements de crédit et autres professionnels du secteur financier (PSF), à savoir :

6. obligation d'incorporer aux virements et transferts de fonds ainsi qu'aux messages s'y rapportant, les informations sur le donneur d'ordre conformément au Règlement (CE) No 1781/2006 du Parlement Européen et du Conseil du 15 novembre 2006 relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds.

**22.** Pour assurer une mise en œuvre correcte et uniforme de ces obligations professionnelles, tous les professionnels du secteur financier doivent se conformer aux instructions détaillées énoncées ci-dessous.

### **Chapitre 1 Les obligations de vigilance à l'égard de la clientèle**

#### **Section 1 Mesures de vigilance à l'égard de la clientèle**

**23.** En vertu de l'article 3 (1) de la loi modifiée du 12 novembre 2004, les professionnels ont l'obligation d'appliquer des mesures de vigilance à l'égard de leur clientèle dans les cas suivants :

- a) lorsqu'ils nouent une relation d'affaires ;
- b) lorsqu'ils concluent, à titre occasionnel, une transaction d'un montant de 15.000 euros au moins, que la transaction soit effectuée en une seule ou plusieurs opérations entre lesquelles un lien semble exister ;
- c) lorsqu'il y a suspicion de blanchiment ou de financement du terrorisme, indépendamment de tous seuils, exemptions ou dérogations applicables ;

- d) lorsqu'il existe des doutes concernant la véracité ou la pertinence des données précédemment obtenues aux fins de l'identification d'un client.

D'après l'article 3 (2) de la loi modifiée du 12 novembre 2004, les mesures de vigilance à appliquer à l'égard de la clientèle doivent comprendre les mesures suivantes :

- a) identification du client et vérification de son identité, sur la base de documents, de données ou d'informations de source fiable et indépendante ;
- b) identification du/des bénéficiaire(s) effectif(s), au cas où il(s) est/sont différent(s) du client, et prise de mesures adéquates et adaptées au risque pour vérifier son (leur) identité, respectivement comprendre la structure de propriété et de contrôle du client personne morale, fiducie ou construction juridique similaire.

L'identification doit ainsi aller au-delà du client direct et s'étendre aux personnes pour lesquelles le client direct agit et qui sont communément appelées « bénéficiaires effectifs ».

- c) obtention d'informations sur l'objet et la nature envisagée de la relation d'affaires ;
- d) exercice d'une vigilance constante de la relation d'affaires et tenue à jour des documents, données ou informations détenues.

Une interdiction pure et simple d'ouverture de compte est celle prévue à l'article 3-2 (5) de la loi modifiée du 12 novembre 2004 qui vise toute relation de correspondant bancaire avec une société bancaire écran ou avec une banque connue pour permettre à une société bancaire écran d'utiliser ses comptes (v. point 89 ci-après).

**24. Approche basée sur le risque :** Les professionnels doivent mettre en œuvre chacune des mesures de vigilance prévues à l'article 3 (2) de la loi modifiée du 12 novembre 2004, mais ils peuvent en ajuster la portée en fonction du risque associé au type de client, de relation d'affaires, de produit ou de transaction concerné. Ils doivent dans ce cas être en mesure de prouver que l'étendue des mesures telles qu'ajustée est appropriée au vu des risques de blanchiment et de financement du terrorisme. La justification relative à l'adaptation des mesures de vigilance en fonction de l'appréciation du risque doit être exposée dans les procédures internes du professionnel visées à l'article 4 (1) de la loi modifiée du 12 novembre 2004.

**L'approche basée sur le risque permet dès lors uniquement au professionnel du secteur financier de déterminer et d'adapter l'envergure des mesures de vigilance en fonction de l'appréciation de risque portée sur le client ou la transaction, mais elle ne permet pas de purement et simplement renoncer à l'application d'une, de certaines ou de toutes ces mesures dans leur entièreté.**

Lorsque les professionnels du secteur financier se trouvent face à des situations qui présentent un risque élevé de blanchiment ou de financement du terrorisme - dans les cas spécifiques expressément visés à l'article 3-2 de la loi modifiée du 12 novembre 2004 ou celles considérées comme telles par le professionnel suivant son appréciation du risque -, les mesures de vigilance de base visées à l'article 3 de la loi modifiée du 12 novembre ne sont plus suffisantes. Dans ce cas, les professionnels doivent prendre des mesures de vigilance renforcées tel que prévu à l'article 3-2 de la loi modifiée du 12 novembre 2004 et comme exposé aux points 80 à 94 de la présente circulaire. Il existe aussi des situations où le risque de blanchiment ou de financement du terrorisme est reconnu comme faible : dans ces cas, l'article 3-1 de la loi modifiée du 12 novembre 2004 prévoit l'application, dans des cas limitativement énumérés, d'obligations de vigilance simplifiées à l'égard de la clientèle (points 105 à 111 de la présente circulaire).

### **Sous-section 1 Identification des clients et vérification de leur identité**

**25.** La loi distingue entre clients en relation d'affaires et clients occasionnels.

#### **A. Clients en relation d'affaires**

##### *Paragraphe 1 Notions de relation d'affaires et de client*

**26.** Les professionnels doivent appliquer les mesures de vigilance visées à l'article 3 (1) de la loi modifiée du 12 novembre 2004 lorsqu'ils nouent une relation d'affaires avec un client, c.-à-d. en vertu de la loi modifiée du 12 novembre 2004, une relation d'affaires, professionnelle ou commerciale liée aux activités professionnelles des professionnels qui est censée, au moment où le contact est établi, s'inscrire dans une certaine durée.

La notion de « client » englobe non seulement la personne au nom de laquelle un compte ou un livret est ouvert, mais également tous ses co-titulaires et ses mandataires.

**27.** Tout professionnel du secteur financier est obligé d'exiger l'identification de ses clients moyennant un ou des documents, des données ou des informations de source fiable et indépendante lorsqu'il noue des relations d'affaires, et, en particulier lorsqu'il ouvre un compte ou un livret, ou offre des services de garde des avoirs que ce soit sous forme d'ouverture d'un compte ou de mise à disposition d'un coffre.

L'entrée en relation d'affaires se traduisant en principe toujours, sous une forme ou sous une autre, par une « ouverture de compte », cette locution sera employée ci-dessous dans ce sens.

**28.** Sont aussi à considérer comme des clients en relation d'affaires ceux pour lesquels sont ouverts des comptes de passage, servant uniquement à une ou plusieurs opérations ponctuelles.

## ***Paragraphe 2 Caractère préalable de l'identification et de la vérification de l'identité***

### ***a. Principe général***

**29.** Conformément à l'article 3 (4) de la loi modifiée du 12 novembre 2004, l'identification du client et du bénéficiaire effectif ainsi que la vérification de leurs identités doit avoir lieu avant l'établissement d'une relation d'affaires respectivement l'ouverture d'un compte ou l'exécution de la transaction. Cela signifie qu'en principe l'identification et la vérification de l'identité du client se font dès le premier contact.

Comme la vérification de l'identité peut exiger plus de temps, il est possible qu'elle se fasse durant l'établissement de la relation d'affaires, c.-à-d. qu'elle soit légèrement décalée dans le temps par rapport à l'identification du client. Cette façon de procéder est acceptée afin de ne pas interrompre l'exercice normal des activités et lorsque le risque de blanchiment ou de financement du terrorisme qui en résulte est seulement faible suivant l'appréciation du professionnel. Pendant ce temps, en attendant que la vérification de l'identité ait été effectuée, il n'est pas permis d'ouvrir un compte au client ni d'exécuter une transaction pour le client.

En revanche, il n'est dans ces circonstances permis d'ouvrir un compte qu'aux conditions visées au point 30 ci-après.

**30.** En effet, par dérogation à la réglementation décrite ci-avant, l'article 3 (4) 4<sup>e</sup> alinéa autorise cependant l'ouverture d'un compte bancaire sans que l'identité du client ait fait l'objet de vérification, à condition qu'aucune transaction ne soit réalisée par le client ou pour son compte jusqu'à ce que la vérification de son identité ait été complètement effectuée à la satisfaction du professionnel. A ce sujet, des garanties suffisantes doivent être mises en place afin de faire en sorte qu'aucune transaction ne soit réalisée dans ces circonstances : celles-ci doivent être intégrées dans les procédures internes de l'établissement de crédit concerné.

Concernant la notion de transaction, il convient de noter qu'elle ne vise pas un transfert par lequel le compte bancaire est crédité, mais seulement les opérations par lesquelles il est disposé des avoirs sur le compte bancaire par le client.

Si avant que la vérification de l'identité du client et, le cas échéant, du bénéficiaire effectif ne soit entièrement accomplie, le professionnel du secteur financier accepte des fonds du client sur un compte non opérationnel ouvert dans les conditions visées à l'article 3 (4) 4<sup>e</sup> alinéa, ou, serait-ce à titre provisoire et sur un compte bloqué, il n'est pas en droit de restituer les avoirs, par décaissement ou par virement, au profit ou sur l'ordre de ce client, tant que l'identité du client et, le cas échéant, du bénéficiaire effectif n'a pas été vérifiée à son entière satisfaction. En attendant, il incombe au professionnel du secteur financier de continuer à assurer la garde de ces biens dans l'intérêt du client, conformément aux conditions sous lesquelles il les a reçus, à moins qu'il ne les consigne si les conditions pour une consignation sont remplies.

Si le professionnel constate qu'il n'est pas en mesure de se conformer aux obligations de vigilance prévues à l'article 3 (2) a) à c) de la loi modifiée du 12 novembre 2004, il lui est interdit d'exécuter une transaction par compte bancaire, d'établir une relation d'affaires et d'exécuter une transaction. Si une relation d'affaires existe, il doit y mettre fin. Dans tous ces cas, il doit envisager de transmettre une déclaration de soupçon sur le client concerné au procureur d'Etat auprès du tribunal d'arrondissement de Luxembourg.

Il y a lieu de relever que le professionnel du secteur financier engage sa responsabilité s'il permet néanmoins au client de disposer des fonds ou de faire simplement état de l'existence du compte avant que l'identification et la vérification de l'identité du client ne soient entièrement accomplies.

Conformément à l'article 3 (4) 4<sup>e</sup> alinéa de la loi modifiée du 12 novembre 2004, l'ouverture/la tenue de comptes anonymes ou de livrets d'épargne anonymes est interdite. Cette interdiction découle de l'obligation d'identifier et de connaître le client sur la base des mesures de vigilance visées au point 23 ci-avant. Les professionnels prennent les mesures appropriées afin que l'interdiction de l'ouverture/de tenue de tels comptes ou livrets soit respectée. Lorsque des comptes ou livrets d'épargne numérotés sont ouverts, les professionnels doivent les administrer de façon à toujours pouvoir intégralement respecter les obligations qui leur incombent en vertu de la loi modifiée du 12 novembre 2004 et de la présente circulaire.

#### Clients de tiers introducteurs

**31.** Il se peut que l'ouverture de compte pour un client soit demandée par un professionnel du secteur financier, auprès duquel le client dispose déjà d'un compte et qui intervient dans le cadre de l'exécution des mesures de vigilance par un tiers introducteur visé à l'article 3-3 de la loi modifiée du 12 novembre 2004 et aux points 95 à 104 de la présente circulaire. Dans ce cas, l'ouverture du compte peut se faire, sous la responsabilité du professionnel auprès duquel le client est introduit, sur la base des informations requises qu'il aura obtenues, sans qu'une nouvelle identification/vérification de l'identité du client soit exigée.

#### ***b. Exception***

##### Sociétés en voie de formation

**32.** Il est permis d'ouvrir un compte pour une société en voie de formation, sur base de l'identification et de la vérification de l'identité des fondateurs de cette société, et de délivrer à un notaire un certificat de blocage des fonds reçus sur ce compte. L'identification et la vérification de l'identité des fondateurs doivent être accompagnées d'une déclaration des fondateurs qu'ils agissent soit pour leur propre compte soit pour des bénéficiaires effectifs qu'ils nomment. L'identification et la vérification de l'identité de la société doivent être complétées au plus tôt au moyen des documents visés au point 40 ci-après (statuts, extrait récent du registre du commerce ou documents équivalents) et avant que le professionnel du secteur financier ne puisse se dessaisir des fonds reçus sur le compte. Il en est de même en ce qui concerne l'identification et la vérification de l'identité des bénéficiaires effectifs de la

société nommés par les fondateurs et ses éventuels autres bénéficiaires effectifs et dont l'identification et la vérification de l'identité doivent se faire conformément aux points 47 et suivants de la présente circulaire.

### **c. Autorisation écrite nécessaire**

**33.** Toute ouverture de compte pour un nouveau client doit être soumise pour autorisation par écrit à un préposé ou à un organe du professionnel du secteur financier spécifiquement habilité à cet effet. Cette personne ou cet organe doit d'une part apprécier s'il est indiqué d'ouvrir un compte à ce client, d'autre part porter la responsabilité pour l'identification et la vérification de l'identité du client et, le cas échéant, du bénéficiaire effectif, et pour la documentation afférente.

**34.** En ce qui concerne les clients considérés comme présentant un risque élevé, dont notamment ceux relevés aux points 80 à 94 ci-dessous, des mesures de vigilance renforcées sont obligatoires.

### ***Paragraphe 3 Identification et vérification de l'identité du client sur base de documents, de données ou d'informations de source fiable et indépendante***

**35.** La loi modifiée du 12 novembre 2004, article 3 (2) a) édicte l'obligation d'identifier le client et de vérifier son identité sur la base de documents, de données ou d'informations de source fiable et indépendante. Si dans le passé l'opération de vérification était inhérente à ce que l'on entendait par « identifier un client », le nouvel article 3 (2) a) fait une distinction entre l'identification et la vérification.

Ainsi, l'opération d'identification consiste à sortir un client de l'anonymat et de disposer d'un nom, d'une identité. L'identification peut ainsi se faire par le fait de compléter un formulaire de demande d'entrée en relation d'affaires et d'y indiquer le numéro d'un document d'identité. L'opération de vérification quant à elle consiste à faire le lien avec la réalité en s'assurant que cette identité se rapporte effectivement à la personne avec laquelle on traite, que cette personne existe réellement et que les documents, données et informations sont respectivement fiables et probants. Ceux-ci peuvent être mis à la disposition par le client, mais l'exigence qu'ils soient de source indépendante s'oppose à ce qu'ils soient le produit du client lui-même.

Normalement, l'identification de clients personnes physiques, mais aussi de personnes morales, et la vérification de leur identité, se fait en une seule étape, sur la base de documents officiels.

Il convient de distinguer entre clients personnes physiques et clients personnes morales.

### ***a. Client personne physique***

**36.** L'identification et la vérification de l'identité d'un client personne physique doivent se faire en principe sur base d'une pièce de légitimation officielle permettant d'attester l'identité de la personne (p.ex. passeport, carte d'identité, permis de conduire, carte de séjour ainsi que tout document officiel muni d'une photo permettant d'établir sans équivoque l'identité de la personne en question).

Lorsque le client ne possède pas de documents d'identification répondant entièrement aux critères requis, les professionnels du secteur financier doivent vérifier l'identité du client en se basant sur des documents de sources diverses tout en effectuant les vérifications nécessaires permettant d'établir l'identité du client avec une certitude suffisante. Au cas où l'identité ne peut être vérifiée avec une certitude suffisante, le professionnel doit refuser l'entrée en relation d'affaires et l'exécution de toute transaction. En cas de soupçon de blanchiment ou de financement du terrorisme, il doit faire une déclaration au procureur auprès du tribunal d'arrondissement de Luxembourg (cf. points 118 et suivants de la présente circulaire).

**37.** Le professionnel du secteur financier doit en outre :

- s'assurer que les documents produits se rapportent bien à leur porteur en comparant la signature figurant sur la pièce de légitimation avec celle apposée sur la demande d'ouverture du compte et, le cas échéant, en comparant la photo sur la pièce de légitimation avec la personne même du client ;
- en fonction de l'appréciation du risque, faire une copie des documents d'identité et les conserver dans le dossier, ou reporter les données suivantes sur les documents d'ouverture du compte: nom et prénom du client, date et lieu de naissance, nationalité, adresse exacte, profession, numéro de la pièce d'identité ;
- veiller à ce que la demande d'ouverture de compte, signée par le client, se fasse en principe sur un formulaire du professionnel du secteur financier luxembourgeois ;
- veiller à ce que tous les documents d'ouverture du compte soient dûment et lisiblement complétés, datés et signés par le client.

**38.** Lorsque le client exerce une activité du secteur financier qui implique la gestion de fonds de tiers, la copie de l'autorisation requise à cet effet ou la mention que pareille autorisation n'est pas requise, est à porter au dossier.

### ***b. Client personne morale***

**39.** L'identification et la vérification de l'identité doivent se faire à deux niveaux, à savoir :

- personne morale ;
- représentants (mandataires) de la personne morale.

## I. Identification et vérification de l'identité de la personne morale

**40.** L'identification et la vérification de l'identité d'un client personne morale doivent se faire sur base des pièces suivantes :

- 1) statuts (ou document constitutif équivalent)
- 2) extrait récent du registre de commerce (ou document équivalent).

En ce qui concerne les documents sous 1) et 2) ci-dessus, il s'agit d'obtenir la preuve de la constitution et du statut juridique de la personne morale (nationalité, forme juridique), ainsi que des renseignements concernant le nom de la société, le nom des administrateurs, le nom des dirigeants et les dispositions régissant le pouvoir d'engager la personne, ainsi que l'adresse du siège.

Concernant le dernier point, les professionnels sont obligés de demander s'il s'agit d'une société domiciliée au Luxembourg et, si tel est le cas, auprès de qui elle est domiciliée. Lorsqu'il s'agit d'une société étrangère ayant une adresse au Luxembourg, les professionnels du secteur financier doivent en outre obtenir une information claire et précise au sujet du droit suivant lequel la société a été constituée ou organisée et, le cas échéant, l'adresse de son siège principal à l'étranger. Ces informations ou données peuvent être obtenues à partir des registres publics, auprès du client ou à partir d'autres sources fiables.

**41.** Lorsque le client exerce une activité du secteur financier qui implique la gestion de fonds de tiers, la copie de l'autorisation requise à cet effet ou la mention que pareille autorisation n'est pas requise, est à porter au dossier.

## II. Identification et vérification de l'identité des représentants (mandataires) de la personne morale

**42.** L'identification et la vérification de l'identité concernant les représentants (mandataires) des personnes morales ou les personnes déléguées par lesdits organes se limitent, en principe, aux personnes membres des organes de la personne morale agissant au nom de la société dans ses relations avec le professionnel du secteur financier, c.-à-d. disposant des pouvoirs sur les comptes de la personne morale auprès du professionnel du secteur financier. L'identification et la vérification de l'identité de ces personnes doivent être les mêmes que pour les clients personnes physiques.

Le professionnel du secteur financier doit également vérifier si l'organe compétent a effectivement autorisé l'ouverture du compte en question et si les personnes disposant de pouvoirs sur le compte ont effectivement ce droit en vertu d'une disposition statutaire ou d'une décision de l'organe sociétaire compétent.

### ***c. Vérification par rapport aux situations exigeant l'application de mesures de vigilance renforcées***

**43.** Dans le cadre de l'identification et de la vérification de l'identité, le professionnel du secteur financier doit vérifier si le client en question n'exige pas l'application des mesures de vigilance renforcées en vertu de l'article 3-2 de la loi modifiée du 12 novembre 2004 et des points 80 à 94 de la présente circulaire. Il doit notamment vérifier si le client, le(s) bénéficiaire(s) effectif(s) ainsi que les personnes qui ont pouvoir sur le compte, ne figurent pas sur les listes de terroristes reprises dans les circulaires visées en annexe III de la présente circulaire.

### **B. Clients occasionnels**

**44.** L'identification et la vérification de l'identité, ainsi que l'application des autres mesures de vigilance, vaut également pour toute transaction, avec des clients autres que ceux avec lesquels des relations d'affaires sont nouées, lorsque le montant de la transaction atteint ou excède la valeur de 15.000 euros, qu'elle soit effectuée en une seule ou en plusieurs opérations entre lesquelles un lien semble exister. Si le montant total n'est pas connu au moment de l'engagement de la transaction, le professionnel du secteur financier concerné procédera à l'identification et la vérification de l'identité du client dès le moment où il en aura connaissance et qu'il constatera que le seuil de 15.000 euros est atteint. Les professionnels du secteur financier sont tenus de procéder à l'identification et à la vérification de l'identité du client même si le montant de la transaction est inférieur au seuil de 15.000 euros, dès qu'il y a soupçon de blanchiment ou de financement du terrorisme. Sont visées les transactions ponctuelles, notamment au guichet, pour lesquelles il n'y a ni préparation de dossier, ni ouverture de compte.

**45.** Lorsque l'identification et la vérification de l'identité d'un client occasionnel sont exigées, elles doivent se faire et être documentées selon les mêmes modalités que pour les clients en relation d'affaires.

L'hypothèse dans laquelle l'identification et la vérification de l'identité d'un client occasionnel deviennent obligatoires parce qu'il y a soupçon de blanchiment ou de financement du terrorisme, fait appel au jugement du professionnel du secteur financier.

Si l'identification d'un tel client et, le cas échéant, ses réponses aux questions complémentaires posées par le professionnel du secteur financier, ne parviennent pas à lever le soupçon, voire le confirment, le professionnel du secteur financier doit d'une part s'abstenir d'exécuter la transaction et d'autre part faire une déclaration d'opération suspecte au procureur d'Etat (cf. points 118 et suivants de la présente circulaire).

**46.** Il est rappelé pour le bon ordre que des lois spécifiques, adoptées pour des raisons différentes que pour la lutte contre le blanchiment, imposent des obligations d'identification qui s'ajoutent à celles prévues par la loi modifiée du 12 novembre 2004. Il va de soi que ces lois spécifiques doivent être respectées. Il en va ainsi notamment en ce qui concerne l'article 5 de la loi modifiée du 3 septembre 1996 concernant la dépossession involontaire de titres au porteur, qui exige de tous les professionnels du secteur financier qu'ils vérifient et inscrivent l'identité exacte des personnes avec lesquelles ils effectuent une opération sur

titres, quel que soit le montant en cause. Il en va ainsi également de l'article 74 de la loi du 19 brumaire an VI (9 novembre 1797) relative à la surveillance du titre des matières d'or et d'argent, qui prescrit aux professionnels financiers de retenir l'identité des personnes dont ils achètent ou auxquelles ils vendent de l'or ou de l'argent.

## **Sous-section 2 Identification et vérification de l'identité des bénéficiaires effectifs**

### ***Paragraphe 1 Définition du bénéficiaire effectif***

**47.** L'article 1<sup>er</sup> (7) de la loi modifiée du 12 novembre 2004 définit le bénéficiaire effectif comme étant toute personne physique qui, en dernier lieu, possède ou contrôle le client et/ou toute personne physique pour laquelle une transaction est exécutée ou une activité réalisée.

Le bénéficiaire effectif comprend au moins:

a) pour les sociétés :

- i) toute personne physique qui, en dernier lieu, possède ou contrôle une entité juridique du fait qu'elle possède ou contrôle directement ou indirectement un pourcentage suffisant d'actions ou de droits de vote dans cette entité juridique, y compris par le biais d'actions au porteur, autre qu'une société cotée sur un marché réglementé qui est soumise à des obligations de publicité conformes à la législation communautaire ou à des normes internationales équivalentes ; un pourcentage dépassant 25% des actions est considéré comme suffisant pour satisfaire à ce critère ;
- ii) toute personne physique qui exerce autrement le pouvoir de contrôle sur la direction d'une entité juridique ;

b) dans le cas de personnes morales, telles que les fondations, et de constructions juridiques, comme les fiducies, qui gèrent ou distribuent les fonds :

- i) lorsque les futurs bénéficiaires ont déjà été désignés, toute personne physique qui est bénéficiaire d'au moins 25% des biens d'une construction juridique ou d'une entité;
- ii) dans la mesure où les individus qui sont les bénéficiaires de la personne morale ou de la construction juridique ou de l'entité n'ont pas encore été désignés, le groupe de personnes dans l'intérêt principal duquel la personne morale ou la construction juridique ou l'entité ont été constitués ou produisent leurs effets;
- iii) toute personne physique qui exerce un contrôle sur au moins 25% des biens d'une construction juridique ou d'une entité.

**48.** Il convient de noter que les « bénéficiaires effectifs » sont aussi souvent appelés « personnes pour le compte desquelles le client agit », « bénéficiaires économiques », « bénéficiaires réels », « ayants droit économiques » ou « *beneficial owners* ».

## ***Paragraphe 2 Règles générales***

**49.** L'article 3 (2) b) de la loi modifiée du 12 novembre 2004 oblige les professionnels à effectuer l'identification du bénéficiaire effectif si le client n'agit pas pour son propre compte. Le professionnel doit dès lors obtenir des informations sur l'identité du bénéficiaire effectif. Cette obligation s'applique aussi bien lorsque le client est une personne physique que lorsqu'il s'agit d'une personne morale, fiducie ou construction juridique.

En ce qui concerne la vérification de l'identité du bénéficiaire effectif, la loi n'exige pas qu'elle se fasse sur base d'informations de source fiable et indépendante, comme c'est le cas pour la vérification de l'identité du client, mais elle adopte une approche plus flexible et basée sur le risque.

Ainsi, les professionnels doivent prendre des mesures adéquates et adaptées au risque pour vérifier l'identité du bénéficiaire effectif, de telle manière qu'ils aient l'assurance de le connaître.

Concernant des clients qui sont des personnes morales, des fiducies ou des constructions juridiques, les mesures adéquates à prendre par les professionnels et dont l'importance dépend également du risque de blanchiment et de financement du terrorisme, sont destinées à leur permettre de comprendre la structure de propriété et de contrôle du client.

On peut à ce sujet se référer au considérant 10 de la directive 2005/60/CE d'après lequel, pour satisfaire à cet impératif, les professionnels sont libres de recourir aux registres publics contenant des informations sur les bénéficiaires effectifs, de demander à leurs clients toute donnée utile ou d'obtenir autrement des informations, tout en tenant compte du fait que l'importance de ces mesures en matière d'obligation de vigilance dépend du risque de blanchiment d'argent et de financement du terrorisme, lequel varie en fonction du type de client, de relation d'affaires, de produit ou de transaction.

**50.** L'identification/la vérification de l'identité du bénéficiaire effectif constitue un élément d'information très important inhérent au client, permettant de mieux connaître celui-ci. Ainsi, des soupçons de blanchiment ou de financement du terrorisme relatifs à un bénéficiaire effectif rejaillissent sur le client et doivent faire l'objet d'une déclaration au procureur d'Etat conformément à l'article 5 (1) a) de la loi modifiée du 12 novembre 2004 et aux points 118 et suivants de la présente circulaire.

**51.** Toutefois, lorsqu'il s'agit d'une situation permettant l'application des mesures simplifiées de vigilance à l'égard de la clientèle telles que prévues à l'article 3-1 de la loi, l'identification d'éventuels bénéficiaires effectifs n'est pas exigée.

## ***Paragraphe 3 Client personne physique***

**52.** D'une façon générale, lors de l'identification d'un client, il faut que le professionnel du secteur financier exige de lui une déclaration écrite qu'il agit pour son propre compte ou, le cas échéant, qu'il n'est pas bénéficiaire effectif/n'agit pas pour son propre compte. Concernant le client personne physique, c'est essentiellement la première partie de la définition précitée du bénéficiaire effectif qui s'applique. Il s'agit de toute personne

physique qui, en dernier lieu, contrôle le client et/ou toute personne physique pour laquelle une transaction est exécutée ou une activité réalisée.

Lorsque le professionnel du secteur financier a la certitude que son client n'agit pas pour son propre compte, notamment en vertu de sa déclaration, il est tenu d'obtenir du client les informations nécessaires relatives à l'identité du ou des bénéficiaires effectifs. Concernant la vérification de ces informations, le professionnel doit prendre des mesures adéquates adaptées au risque de blanchiment et de financement du terrorisme et notamment obtenir du client les documents nécessaires pour établir l'identité du ou des bénéficiaires effectifs. Il est recommandé d'exiger dans chaque cas un écrit émanant du bénéficiaire effectif lui-même à l'appui des affirmations du client.

**53.** Lorsque le professionnel du secteur financier a un doute sur le point de savoir si son client agit pour son propre compte, il est tenu de lever ce doute, soit en obtenant du client l'assurance écrite et crédible que ce dernier agit pour son propre compte, soit en identifiant le bénéficiaire effectif de la façon indiquée ci-dessus. Il convient de souligner que le doute n'est pas forcément levé par une déclaration négative du client ou par le fait qu'un tiers affirme être le bénéficiaire effectif. S'il n'est pas possible au professionnel du secteur financier de lever son doute, il doit s'abstenir de traiter avec le client.

Il doit par ailleurs, en fonction des circonstances, envisager de faire une déclaration au procureur d'Etat.

***Cas particulier : Clients dont l'activité professionnelle implique la conservation de fonds de tiers (p.ex. avocats, notaires, ...)***

**54.** Lorsqu'un notaire ou membre d'une autre profession juridique indépendante (p. ex. un avocat) souhaite ouvrir un compte auprès d'un professionnel du secteur financier, celui-ci doit demander expressément à un tel client s'il agit pour compte propre ou pour compte d'autrui et il doit apprécier la plausibilité de la réponse afin de déterminer si l'ouverture d'un compte groupé (« *pooled account* ») est nécessaire. Le professionnel du secteur financier est tenu d'obtenir du client, lors de l'acceptation et dans le cadre du fonctionnement de la relation d'affaires, les informations qu'il juge nécessaires pour s'assurer que les relations ne servent pas au blanchiment ou au financement du terrorisme.

Au cas où un tel client agit pour compte propre, les procédures d'identification habituelles telles que précisées dans la présente circulaire s'appliquent.

**55.** Au cas où un tel client agit pour compte de tiers, il est utile de rappeler que les personnes visées ci-avant peuvent ouvrir des comptes groupés servant fondamentalement à deux fins différentes :

- a) Les fonds qui passent par ces comptes peuvent trouver leur origine dans l'activité professionnelle des personnes précitées consistant à assister leur client dans la préparation ou la réalisation de transactions concernant notamment :
  - l'achat et la vente de biens immeubles ou d'entreprises commerciales ;
  - la gestion de fonds, de titres ou d'autres actifs, appartenant au client ;

- l'organisation des apports nécessaires à la constitution, à la gestion ou à la direction de sociétés ou de structures similaires ;
- la constitution, la domiciliation, la gestion ou la direction de fiducies (trusts, fondations), de sociétés ou de structures comparables.

Dans les cas mentionnés ci-avant, conformément à l'article 3-1 (2) b) (et tel que mentionné également au point 110 de la présente circulaire), le professionnel dépositaire des fonds peut appliquer les mesures de vigilance simplifiées à l'égard de ces clients, c.-à-d. que le compte groupé peut être ouvert sans que le professionnel agissant comme dépositaire ait l'obligation d'identifier les bénéficiaires effectifs. Cela n'est cependant possible que si le client est un notaire ou membre d'une autre profession juridique indépendante (p. ex. un avocat) établi dans un Etat membre ou dans un pays tiers où ces professions sont soumises à des exigences de lutte contre le blanchiment et le financement du terrorisme satisfaisant aux normes internationales (se référer à ce sujet à la liste des « pays tiers imposant des obligations équivalentes » publiée par règlement grand-ducal du 29 juillet 2008) et où le respect de ces obligations est contrôlé. Il convient en plus de noter que conformément à l'article 3-1 (2) b) de la loi modifiée du 12 novembre 2004, les informations relatives à l'identité des bénéficiaires effectifs doivent être soumises au professionnel dépositaire concerné s'il en fait la demande.

Avant d'ouvrir un compte groupé sans identification des bénéficiaires effectifs, le professionnel dépositaire doit s'assurer que le client en question remplit effectivement les exigences précitées et, le cas échéant, il doit demander au client de s'engager par écrit à soumettre immédiatement les informations relatives à l'identité des bénéficiaires effectifs si la demande en est faite. Il est recommandé d'exiger en plus un certificat de l'ordre professionnel concerné qu'aucune obligation professionnelle n'interdit au notaire respectivement au membre de la profession juridique indépendante en question de mettre ces informations à la disposition du professionnel dépositaire (cf. également point 110 de la présente circulaire).

Si le client ne remplit pas les conditions précitées, l'identification des bénéficiaires effectifs doit être effectuée avant l'ouverture du compte groupé.

- b) Les fonds qui passent par ces comptes trouvent leur origine dans toute autre activité professionnelle des personnes précitées consistant notamment à conseiller leurs clients en ce qui concerne l'évaluation de la situation juridique de ces derniers à l'exclusion des activités citées au point a) ci-dessus ou à représenter leurs clients dans une procédure en justice.

Dans ce cas, le professionnel du secteur financier doit évaluer la plausibilité des assertions de ces personnes et il pourra se dispenser de procéder à l'identification des bénéficiaires effectifs s'il est satisfait des explications reçues par ces personnes.

**56.** Dans tous les cas les professionnels du secteur financier continuent d'être tenus de suivre avec diligence l'évolution des opérations effectuées par ces personnes et doivent s'entourer de tous les renseignements nécessaires pour écarter tout risque de blanchiment ou de financement du terrorisme.

#### ***Paragraphe 4 Client personne morale***

**57.** Lorsque le professionnel du secteur financier veut entrer en relations d'affaires avec des personnes morales, des fiducies ou des constructions juridiques similaires, la/les personne(s) qu'il doit identifier au titre de bénéficiaire(s) effectif(s) sont toujours des personnes physiques. Conformément à la loi, il s'agit des personnes physiques qui, en dernier lieu, possèdent ou contrôlent le client ou pour lesquelles le client fait exécuter une transaction ou réaliser une activité. La loi modifiée du 12 novembre 2004 donne, en définissant le bénéficiaire effectif (point 47 ci-avant), des indications précises sur la nature et l'importance du rapport qu'une personne physique doit avoir avec une personne morale, une fiducie ou une construction juridique similaire afin de pouvoir être considérée comme bénéficiaire effectif.

Il convient de noter que contrairement à la vérification de l'identité du bénéficiaire effectif, l'identification elle-même est une mesure de vigilance qui ne se prête pas à être ajustée en fonction du risque de blanchiment ou de financement du terrorisme, alors qu'il s'agit de disposer simplement du nom, du lieu et de la date de naissance, de la nationalité, de l'adresse de résidence d'une personne physique. A ce sujet, le professionnel du secteur financier se basera essentiellement sur les informations fournies par le client.

**58.** En ce qui concerne la vérification de l'identité du/des bénéficiaire(s) effectif(s) d'une personne morale, construction juridique ou fiducie, celle-ci inclut la compréhension de la propriété et de la structure de contrôle du client.

Pour s'acquitter de manière satisfaisante de cette obligation, le professionnel du secteur financier doit adopter des mesures adéquates en fonction du risque.

Les informations ou données pertinentes sur les bénéficiaires effectifs et sur le contrôle des personnes morales peuvent être obtenues à partir des registres publics ou à partir d'autres sources fiables et indépendantes.

**59.** Il faut que le professionnel du secteur financier exige de la personne répondant aux critères de bénéficiaire effectif de la définition au point 47, une déclaration écrite et crédible attestant qu'elle est le bénéficiaire effectif. Lorsqu'une telle déclaration ne peut pas être obtenue, ou lorsque le professionnel a des doutes concernant la véracité de la déclaration d'une personne qui déclare être bénéficiaire effectif et que ce doute ne peut pas être levé, le professionnel doit s'abstenir de traiter avec le client. Il doit par ailleurs, en fonction des circonstances, envisager dans ce cas de faire une déclaration au procureur d'Etat.

#### ***Paragraphe 5 Sociétés domiciliées***

**60.** Les professionnels du secteur financier doivent respecter, outre la présente circulaire, toutes leurs obligations légales telles qu'elles ont été détaillées dans les circulaires CSSF 01/28, CSSF 01/29, CSSF 01/47 et CSSF 02/65.

### **Sous-section 3 Obtention d'informations sur l'objet et la nature envisagée de la relation d'affaires**

**61.** L'obligation de connaître ses clients impose au professionnel du secteur financier d'aller au-delà d'une identification purement documentaire.

L'entrée en relations d'affaires avec un nouveau client implique par conséquent un jugement sur le client. Ce jugement doit être étayé par l'obtention d'informations sur l'objet et la nature envisagée de la relation d'affaires. Ces informations permettent aussi au professionnel de connaître les activités professionnelles ou commerciales du client ainsi que son profil de risque.

**62.** Ces informations devraient permettre au professionnel du secteur financier de réduire au mieux le risque d'être utilisé à des fins de blanchiment ou de financement du terrorisme et plus tard de détecter les transactions suspectes parce qu'elles ne sont pas en conformité avec les informations reçues.

Un fait insolite constaté au moment de l'identification pourrait être l'indice d'un blanchiment ou d'un financement du terrorisme et devrait en tant que tel amener le professionnel du secteur financier à demander des informations complémentaires.

Une attention particulière doit être exercée lorsque la motivation de la relation d'affaires recherchée n'est pas claire ou lorsque le client a recours à des constructions dont la justification économique n'est pas apparente (enchevêtrement de comptes, comptes à désignation pouvant induire en erreur, ...).

### **Sous-section 4 Exercice d'une vigilance constante de la relation d'affaires et tenue à jour des documents, données ou informations détenues**

**63.** Conformément à l'article 3 (2) d) de la loi modifiée du 12 novembre 2004, les professionnels du secteur financier doivent exercer une vigilance constante de la relation d'affaires, notamment en examinant les transactions conclues pendant toute la durée de la relation d'affaires et, si nécessaire, sur l'origine des fonds, de manière à vérifier que ces transactions sont cohérentes par rapport à la connaissance qu'a le professionnel de son client, de ses activités commerciales et de son profil de risque, et en tenant à jour les documents, données ou informations détenus.

#### ***Paragraphe 1 La vigilance constante de la relation d'affaires***

**64.** Les professionnels du secteur financier doivent ainsi mettre en place une méthodologie pour établir le degré de risque de chaque client tout en ciblant les clients à risque élevé visés à l'article 3-2 de la loi modifiée du 12 novembre 2004.

Par ailleurs, ils sont tenus d'effectuer une surveillance continue de leurs clients dès le début et pendant toute la relation d'affaires. L'envergure de cette mesure peut être ajustée en fonction du degré de risque de blanchiment et de financement du terrorisme attribué au

client en question. Suivant l'appréciation du risque, le professionnel devra également connaître l'origine des fonds du client en question.

Doivent être considérés notamment comme clients à risque élevé ceux visés aux points 80 à 94 (mesures de vigilance renforcées).

**65.** Pour être capable de respecter l'obligation de vigilance constante de la relation d'affaires, il est recommandé à chaque professionnel du secteur financier de limiter le nombre de clients par chargé de clientèle en fonction du type de client et de ses systèmes et moyens techniques.

### ***Paragraphe 2 La tenue à jour des documents et informations***

**66.** Lors de l'identification initiale du client et de la vérification de son identité sur base d'un document valide, chaque professionnel du secteur financier a dû s'assurer de l'identité du client.

L'identification n'est pas remise en cause par le fait que le document en question (par exemple carte d'identité ou passeport) vient un jour à expiration.

Les professionnels du secteur financier peuvent ainsi s'en remettre aux mesures d'identification et de vérification déjà effectuées, à moins que, dans le cadre du suivi de la relation d'affaires, ils n'aient des doutes quant à la véracité des informations obtenues. Ils peuvent avoir des doutes de blanchiment ou de financement du terrorisme en liaison avec ce client, lorsque les opérations exécutées sur le compte du client changent sensiblement, d'une manière non conforme à l'activité du client et lorsque le professionnel du secteur financier réalise qu'il n'a pas d'informations suffisantes sur le client. Dans ces cas, le professionnel du secteur financier peut être amené, selon son appréciation de la situation et du risque, à mettre le dossier d'identification à jour ou à renouveler l'identification.

## **Section 2 Obligation d'accorder une attention particulière à certaines activités et transactions**

### **Sous-section 1 Transactions particulièrement susceptibles d'être liées au blanchiment ou au financement du terrorisme**

**67.** En vertu de l'article 3 (7) de la loi modifiée du 12 novembre 2004, les professionnels du secteur financier sont obligés d'examiner avec une attention particulière toute activité qui leur paraît particulièrement susceptible, de par sa nature, d'être liée au blanchiment ou au financement du terrorisme, et notamment les transactions complexes ou d'un montant inhabituellement élevé, ainsi que tous les types inhabituels de transactions n'ayant pas d'objet économique apparent ou d'objet licite visible.

**68.** Afin d'éviter d'être utilisé à des fins de blanchiment ou de financement du terrorisme et pour pouvoir détecter des transactions suspectes, il importe que le professionnel du secteur financier ait une bonne compréhension des transactions que ses clients lui demandent d'exécuter. A cet effet, le professionnel du secteur financier est tenu de suivre avec diligence l'évolution des opérations effectuées pour ses clients et de s'entourer, le cas échéant, de tous les renseignements nécessaires pour écarter au mieux le risque d'un blanchiment ou de financement du terrorisme.

**69.** Relèvent aussi de ce genre d'opérations visées au point 67 ci-avant, celles impliquant des montants faibles mais à fréquence anormalement élevée, les transactions qui appartiennent à des segments de risque (p.ex. pays à risques) et les transactions inhabituelles par rapport aux transactions normalement effectuées par le client en question (p.ex. transaction anormale par rapport au fonctionnement normal du compte ; transactions qui ne concordent pas avec les déclarations faites lors de l'ouverture du compte ; provenance et/ou destination des fonds). En annexe II à la présente circulaire se trouve une liste indicative d'exemples de telles transactions.

**70.** L'article 3 (7) de la loi modifiée du 12 novembre 2004 ne se réfère plus expressément, contrairement à la formulation antérieure de la loi sur ce point, ni aux circonstances qui entourent une transaction ni à la qualité des personnes impliquées, mais seulement à la nature d'une activité/transaction particulièrement susceptible d'être liée au blanchiment ou au financement du terrorisme. La notion de nature d'une activité/transaction est néanmoins à comprendre de manière large en y incluant les notions de « qualité des personnes impliquées » et de « circonstances qui entourent une activité/transaction ». Il convient de rapprocher cette disposition de l'article 5 (1) a) qui se réfère à la personne concernée, son évolution, l'origine des avoirs, la nature et la finalité ou les modalités de l'opération comme étant des critères en fonction desquels le professionnel du secteur financier peut avoir un soupçon de blanchiment ou de financement du terrorisme.

L'examen d'une opération par rapport à la qualité des personnes impliquées couvre aussi bien le cas des personnes politiquement exposées résidant à l'étranger visées aux points 85 et suivants de la présente circulaire que celui des personnes originaires (en raison de leur nationalité, de leur centre d'activité ou de leur résidence) de pays dont le dispositif contre le blanchiment et le financement du terrorisme est considéré au niveau international comme déficient (cf. points 91 à 93 ci-après).

**71.** Les professionnels du secteur financier doivent tenir compte de la particularité de la lutte contre le financement du terrorisme, étant donné que dans ce cas on assiste souvent par rapport à la lutte contre le blanchiment au procédé inverse, c.-à-d. que de l'argent provenant de sources qui peuvent être tout à fait licites, est injecté dans les réseaux et systèmes terroristes.

**72.** Si, malgré les efforts du professionnel du secteur financier pour obtenir les renseignements nécessaires à la compréhension d'une transaction, il lui reste des doutes quant à l'absence de tout lien avec le blanchiment ou le financement du terrorisme, sans pour autant qu'il ait pu avoir un soupçon de blanchiment ou de financement du terrorisme, il doit

refuser d'exécuter la transaction, voire rompre la relation d'affaires avec le client. S'il relève un fait qui pourrait être l'indice d'un blanchiment ou d'un financement du terrorisme respectivement qui donne lieu à soupçon, il doit faire une déclaration au procureur d'Etat près du tribunal d'arrondissement de Luxembourg (cf. points 118 et suivants de la présente circulaire).

## **Sous-section 2 Procédures, systèmes et mécanismes à mettre en œuvre pour détecter les transactions suspectes**

**73.** Les professionnels du secteur financier doivent disposer de procédures et mettre en place des mécanismes et systèmes pour être capables de détecter d'une part les clients et bénéficiaires effectifs qui figurent sur des listes officielles (p.ex. listes de terroristes) ou privés/internes (p.ex. personnes politiquement exposées résidant à l'étranger), ainsi que les fonds provenant de pays qui figurent sur des listes officielles (p.ex. pays sous embargo ou pays visés aux points 91 et suivants) et d'autre part les transactions douteuses/suspectes, car anormales ou inhabituelles par nature ou par rapport aux transactions normales du client en question.

Ces mécanismes et systèmes doivent être élaborés en collaboration avec la personne chargée plus particulièrement de la lutte contre le blanchiment et le financement du terrorisme.

**74.** En fonction du nombre des clients et des transactions à risque, il est recommandé de mettre en place un système informatique aidant à détecter des transactions susceptibles d'être liées au blanchiment ou au financement du terrorisme, ceci afin d'assurer une surveillance efficace des transactions.

La mise en place d'un outil informatique anti-blanchiment ne dispense cependant pas les professionnels du secteur financier de poursuivre leur politique en matière de lutte contre le blanchiment ou le financement du terrorisme par d'autres moyens. La responsabilité du professionnel du secteur financier ne peut être transférée au concepteur de logiciel. En cas de mise en place d'un outil informatique en matière de lutte contre le blanchiment ou le financement du terrorisme, le paramétrage de cet outil doit se faire sous le contrôle de la personne qui est chargée plus particulièrement de la lutte contre le blanchiment et le financement du terrorisme. Toute modification inopportune volontaire ou involontaire des paramètres peut en effet affaiblir, à moyen ou long terme, l'efficacité de l'outil informatique pour détecter des opérations de blanchiment ou de financement du terrorisme.

## **Sous-section 3 Consignation écrite des résultats des analyses effectuées**

**75.** Le professionnel du secteur financier doit retenir par écrit le résultat de l'examen auquel il aura procédé à propos des activités/transactions considérées par lui comme particulièrement susceptibles d'être liées au blanchiment ou au financement du terrorisme.

### **Section 3 Obligation de conserver certains documents et informations**

#### **Sous-section 1 Documentation relative à l'identification et à la vérification de l'identité**

**76.** La documentation relative à l'identification et à la vérification de l'identité d'un client doit comprendre notamment en ce qui concerne les clients personnes physiques :

- la demande d'ouverture de compte signée et datée par le client, reprenant ses nom et prénom, son lieu et sa date de naissance, sa nationalité, son adresse exacte, sa profession ainsi que le numéro et la date de son document d'identité officiel ;
- le cas échéant, la copie du document d'identité officiel requis pour l'identification et la vérification de l'identité ;
- la documentation relative à la vérification de l'identité du/des bénéficiaire(s) effectif(s).

En ce qui concerne les sociétés et autres personnes morales, la documentation comprendra notamment la demande d'ouverture de compte signée et datée par les représentants visés au point 42 ci-dessus, reprenant la dénomination sociale, la forme juridique de la société ou personne morale, sa date de constitution, l'adresse exacte de son siège social (ainsi que, le cas échéant, s'il s'agit d'une société domiciliée, le siège de son domicile au Luxembourg), le droit par lequel elle est régie, l'identité du/des bénéficiaire(s) effectif(s), ainsi que la documentation relative à la vérification de l'identité du/des bénéficiaire(s) effectif(s) et les documents visés aux points 40 à 42 de la présente circulaire.

Concernant les constructions juridiques et fiducies (*trust*) visées au point 23, le professionnel du secteur financier inclura dans la documentation notamment la demande d'ouverture de compte ainsi que tous documents lui ayant permis de comprendre la structure de propriété et de contrôle du client.

#### **Sous-section 2 Documentation relative aux transactions**

**77.** La documentation relative aux transactions doit comprendre notamment :

- le relevé des transactions (la nature et la date de la transaction, le type et le montant de la devise, le type et le numéro de compte) ;
- la correspondance pertinente ;
- les contrats.

**78.** Toutes ces pièces doivent permettre de reconstituer les transactions individuelles. Les résultats des examens visés au point 75 auxquels le professionnel du secteur financier aura procédé à propos des transactions particulièrement susceptibles d'être liées au blanchiment ou au financement du terrorisme devront également être conservés.

### **Sous-section 3 Conservation des documents et informations**

**79.** Les établissements de crédit et les autres professionnels du secteur financier sont obligés de conserver les documents et informations mentionnés aux points 76 à 78 ci-dessus, à l'effet de servir d'élément de preuve dans toute enquête en matière de blanchiment ou de financement du terrorisme ou dans une analyse d'un éventuel blanchiment ou d'un éventuel financement du terrorisme menée par les autorités luxembourgeoises responsables de la lutte contre le blanchiment et le financement du terrorisme.

En ce qui concerne les mesures de vigilance à l'égard du client, une copie ou les références des documents exigés doivent être conservées pendant au moins cinq ans après la fin de la relation d'affaires avec le client, sans préjudice des délais de conservation plus longs prescrits par d'autres lois.

En ce qui concerne les relations d'affaires et les transactions, les pièces justificatives et enregistrements consistant en des documents originaux ou des copies ayant force probante similaire au regard du droit luxembourgeois, doivent être conservés pendant au moins cinq ans à partir de l'exécution des transactions ou de la fin de la relation d'affaires, sans préjudice des délais de conservation plus longs prescrits par d'autres lois.

### **Chapitre 2 Obligations renforcées de vigilance à l'égard de la clientèle**

**80.** Les professionnels du secteur financier doivent mettre en œuvre chacune des mesures de vigilance de base visées à l'article 3 de la loi modifiée du 12 novembre 2004 et dans la présente circulaire à l'égard de tous les clients. Mais en présence de situations qui comportent un risque plus élevé de blanchiment de capitaux ou de financement du terrorisme, ils doivent en plus appliquer des procédures d'identification et de vérification de l'identité renforcées à l'égard de la clientèle.

Les professionnels doivent appliquer ces mesures de vigilance renforcées, en fonction de leur appréciation du risque, dans les situations qui par leur nature peuvent présenter un risque élevé de blanchiment ou de financement du terrorisme. Ils doivent dès lors analyser les facteurs de risque pouvant être inhérents à leurs activités et clientèle spécifiques et établir, le cas échéant, de telles mesures renforcées de vigilance à l'égard de la clientèle.

Les professionnels doivent notamment accorder une attention particulière à toute menace de blanchiment ou de financement du terrorisme pouvant résulter de produits ou de transactions favorisant l'anonymat et prendre des mesures, le cas échéant, pour empêcher leur utilisation à des fins de blanchiment ou de financement du terrorisme.

Les cas visés ci-après sont d'office considérés comme situations à risque élevé et exigent dès lors la mise en œuvre des mesures de vigilance renforcées spécifiques indiquées. Les professionnels doivent prévoir l'application de ces mesures dans leurs procédures internes. En-dehors de ces cas légaux, la présente circulaire cite le cas des pays et territoires non-coopératifs et situations similaires auxquels des mesures de vigilance renforcées doivent être appliquées.

## **Section 1 Entrée en relation d'affaires à distance**

**81.** L'article 3-3 de la loi modifiée du 12 novembre 2004 vise tout d'abord la situation où le professionnel du secteur financier noue des relations d'affaires avec ou effectue une transaction pour un client qui n'est pas physiquement présent aux fins de l'identification. Dans ces cas, le professionnel doit prendre des mesures spécifiques appropriées pour compenser le risque élevé de blanchiment et de financement du terrorisme découlant de cette situation. Ces mesures doivent garantir l'identification du client et la vérification de son identité.

Il convient de noter que l'article 3-1 (4) d) de la loi modifiée du 12 novembre 2004 prévoit aussi un cas de figure particulier où en raison du faible risque de blanchiment ou de financement du terrorisme l'application de mesures de vigilance simplifiées est justifiée.

**82.** Le professionnel a le choix entre les trois types de mesures suivantes à appliquer avant l'entrée en relation d'affaires, mais peut être amené, en fonction de son appréciation du degré de risque associé au client, à appliquer plusieurs de ces mesures :

- mesures garantissant que l'identité du client est établie au moyen de documents, données ou informations supplémentaires (p. ex. justification de l'activité professionnelle exercée par le client, de l'origine des fonds, de l'adresse du client etc.) ;
- mesures complémentaires assurant la vérification ou la certification des documents fournis ou exigeant une attestation de confirmation de la part d'un établissement de crédit.

Le professionnel peut ainsi exiger une copie de la pièce d'identité du client, certifiée conforme par une autorité compétente (p.ex. ambassade, consulat, notaire, commissaire de police) ou par une institution financière soumise à une réglementation équivalente en matière de lutte contre le blanchiment et le financement du terrorisme.

- mesures garantissant que le premier paiement des opérations soit effectué au moyen d'un compte ouvert au nom du client auprès d'un établissement de crédit.

Dans ce cas, le professionnel peut exiger une simple copie de la pièce d'identité du client ainsi que toutes autres informations le cas échéant requises sous condition que le premier transfert d'avoirs soit effectué à partir d'un compte ouvert au nom du client auprès d'un établissement de crédit soumis à une obligation d'identification équivalente.

Une procédure acceptée par la CSSF consiste à ce que l'ordre de virement signé par le client soit envoyé directement par la banque luxembourgeoise à la banque du client, muni d'un numéro de référence. Lors de la réception du transfert, la banque luxembourgeoise peut vérifier à l'aide du numéro de compte et du numéro de référence que l'argent provient effectivement d'un compte appartenant au client auprès de sa banque d'origine. Toute autre procédure doit être préalablement soumise pour accord à la CSSF.

**83.** Le professionnel du secteur financier doit par ailleurs veiller avec une attention particulière à recevoir non seulement toute la documentation requise, mais également des

réponses complètes et satisfaisantes à toutes les questions qu'il sera le cas échéant amené à poser au client en vue de porter un jugement éclairé sur ce client et sur le but de la relation d'affaires recherchée.

**84.** Avant d'ouvrir un compte ou d'effectuer une transaction, les professionnels du secteur financier doivent analyser toutes les informations fournies par le client, conformément à leurs procédures d'acceptation de clients.

## **Section 2 Les personnes politiquement exposées (« PPE »)**

**85.** Afin d'éviter d'être impliqués dans un acte de blanchiment d'argent, les professionnels du secteur financier doivent appliquer des mesures de vigilance renforcées lorsqu'ils veulent établir des relations d'affaires ou accepter et garder des avoirs appartenant, directement ou indirectement, à des PPE résidant à l'étranger.

La loi modifiée du 12 novembre 2004, article 1<sup>er</sup>(9) à (12) donne d'importantes précisions concernant la notion de personnes politiquement exposées.

### **86. Définitions**

La loi définit les PPE comme étant les personnes physiques qui occupent ou se sont vu confier une fonction publique importante ainsi que les membres directs de leur famille ou des personnes connues pour leur être étroitement associées. Ainsi, la définition se décompose en trois parties :

- A) Par « personnes physiques qui occupent ou se sont vu confier une fonction publique importante », il faut comprendre l'ensemble de personnes physiques comprenant :
- a) les chefs d'Etat, les chefs de gouvernement, les ministres, ministres délégués et secrétaires d'Etat ;
  - b) les parlementaires ;
  - c) les membres des cours suprêmes, des cours constitutionnelles ou d'autres hautes juridictions dont les décisions ne sont pas susceptibles de recours, sauf circonstances exceptionnelles ;
  - d) les membres des cours des comptes ou des conseils des banques centrales ;
  - e) les ambassadeurs, les chargés d'affaires et les officiers supérieurs des forces armées ;
  - f) les membres des organes d'administration, de direction ou de surveillance des entreprises publiques.

D'après la loi, aucune des catégories citées aux points a) à f) ci-dessus ne couvre des personnes occupant une fonction intermédiaire ou inférieure.

Les catégories visées aux points a) à e) ci-dessus comprennent, le cas échéant, les fonctions exercées aux niveaux communautaire et international.

B) La loi modifiée du 12 novembre 2004 définit les « membres directs de la famille » comme l'ensemble de personnes physiques comprenant:

- a) le conjoint ;
- b) tout partenaire considéré par le droit interne comme l'équivalent d'un conjoint. Il s'agit en principe des dispositifs légaux d'organisation de la vie commune de deux personnes existant dans certains pays.
- c) les enfants et leurs conjoints ou partenaires ;
- d) les parents.

C) Les « personnes connues pour être étroitement associées » sont l'ensemble de personnes physiques comprenant:

- a) toute personne physique connue pour être le bénéficiaire effectif d'une personne morale ou d'une construction juridique conjointement avec une personne physique qui occupe ou s'est vu confier une fonction publique importante, ou pour entretenir toute autre relation d'affaires étroite avec une telle personne ;
- b) toute personne physique qui est le seul bénéficiaire effectif d'une personne morale ou d'une construction juridique connue pour avoir été établie au profit de facto de la personne physique qui occupe ou s'est vu confier une fonction publique importante.

## 87. Régime applicable

Les mesures de vigilance renforcées visant spécifiquement les PPE s'appliquent seulement en ce qui concerne les transactions ou les relations d'affaires avec des PPE résidant dans un autre Etat membre ou dans un pays tiers, à l'exclusion des PPE résidant au Luxembourg.

Elles sont à appliquer en plus des mesures de vigilance de base visées à l'article 3 de la loi modifiée du 12 novembre 2004 et en fonction du risque de blanchiment et de financement du terrorisme du client concerné. Les professionnels doivent à ce sujet instaurer une politique et des procédures de contrôle particulières, afin de s'entourer de toutes les garanties nécessaires dans leurs relations avec un client appartenant ou venant à appartenir au cercle des personnes visées.

Les mesures de vigilance renforcées applicables aux PPE sont les suivantes :

- a) disposer de procédures adéquates adaptées au risque afin de déterminer si le client respectivement le bénéficiaire effectif est une personne politiquement exposée résidant à l'étranger telle que définie à l'article 1er de la loi modifiée du 12 novembre 2004. Les professionnels du secteur financier doivent ainsi disposer de procédures, connues de tous les employés en relation avec la clientèle, qui, en fonction du risque, permettent de détecter les PPE au sens de la définition prévue par la loi. Ces procédures consistent en tout premier lieu dans l'information à ce sujet directement obtenue du client, du recours à des informations publiquement disponibles respectivement de l'accès à des bases de données informatiques commerciales sur les personnes politiquement exposées;
- b) obtenir l'autorisation d'un niveau élevé de la hiérarchie avant de nouer une relation d'affaires avec de tels clients.

Ainsi, il convient d'impliquer la personne chargée plus particulièrement de la lutte contre le blanchiment et le financement du terrorisme dans la procédure d'acceptation d'un client PPE, ainsi que prévoir, le cas échéant, compte tenu de la sensibilité du sujet et de l'appréciation du risque, l'autorisation d'un des dirigeants ayant obtenu l'agrément requis par la loi, avant de nouer une relation d'affaires ou d'effectuer une transaction avec de tels clients.

- c) prendre toute mesure appropriée pour établir l'origine du patrimoine et l'origine des fonds impliqués dans la relation d'affaires ou la transaction. Suivant l'appréciation du risque, les professionnels doivent, en vérifiant l'origine des fonds, demander des documents probants à ce sujet ;
- d) assurer une surveillance continue renforcée de la relation d'affaires.

Sans préjudice d'autres raisons justifiant le cas échéant l'application de mesures de vigilance renforcées, les professionnels du secteur financier ne sont, en principe, pas tenus de considérer comme politiquement exposée une personne qui n'occupe plus de fonction publique importante depuis plus d'un an.

En ce qui concerne l'exigence d'identifier en tant que PPE également les personnes étroitement associées à des personnes physiques occupant une fonction publique importante, il est précisé que celle-ci ne s'applique que dans la mesure où la relation avec la personne étroitement associée est notoire ou que le professionnel a des raisons d'estimer que cette relation existe. Cela n'implique donc pas une recherche active de la part du professionnel.

Il résulte de la définition des PPE qu'il s'agit essentiellement de personnes exerçant des fonctions importantes au niveau national d'un Etat. Les fonctions exercées à un niveau inférieur au niveau national, c.-à-d. notamment régional ou local, ne sont en principe pas considérées comme importantes. Cependant, lorsque le degré d'exposition politique de ces fonctions est comparable à celui de positions analogues au niveau national, les professionnels du secteur financier devraient évaluer, en fonction du risque, s'il y a lieu de considérer les personnes exerçant ces fonctions publiques (à l'étranger) comme des PPE.

**88.** Il est rappelé que par la suite, l'évolution de la relation d'affaires doit également être suivie de façon étroite par le professionnel et notamment la personne chargée plus particulièrement de la lutte contre le blanchiment et le financement du terrorisme, conformément au point d) ci-avant.

### **Section 3 Banques correspondantes**

**89.** D'après l'article 3-2 (3) de la loi modifiée du 14 novembre 2004, les établissements de crédit ont l'obligation, en cas de relation transfrontalière de correspondant bancaire avec des établissements correspondants de pays tiers qui ne figurent pas sur la liste des « pays tiers imposant des obligations équivalentes » publiée par règlement grand-ducal du 29 juillet 2008 précité de :

- a) recueillir sur l'établissement client des informations suffisantes pour comprendre pleinement la nature de ses activités et pour apprécier, sur la base d'informations accessibles au public, sa réputation et la qualité de la surveillance dont il fait l'objet ;
- b) évaluer les contrôles contre le blanchiment et contre le financement du terrorisme mis en place par l'établissement correspondant ;
- c) obtenir l'autorisation d'un niveau élevé de leur hiérarchie avant de nouer de nouvelles relations de correspondant bancaire ;
- d) établir par des documents les responsabilités respectives de chaque établissement ;
- e) en ce qui concerne les comptes « de passage » («*payable through accounts*»), s'assurer que l'établissement de crédit client a vérifié l'identité des clients ayant un accès direct aux comptes de l'établissement correspondant et a mis en œuvre à leur égard une surveillance constante, et qu'il peut fournir des données pertinentes concernant ces mesures de vigilance à la demande de l'établissement correspondant.

Dans ce contexte, la loi modifiée du 12 novembre 2004 interdit expressément aux professionnels concernés de nouer ou de maintenir une relation de correspondant bancaire avec une société bancaire écran ou avec une banque connue pour permettre à une société bancaire écran d'utiliser ses comptes. Il est rappelé qu'une société bancaire écran est un établissement de crédit ou un établissement exerçant des activités équivalentes à celles d'un établissement de crédit, constitué dans un pays où il n'a aucune présence physique par laquelle s'exerceraient une direction et une gestion véritables et qui n'est pas rattaché à un groupe financier réglementé.

**90.** A part les situations exigeant une vigilance renforcée prévues par la loi, d'autres situations peuvent exister, comme celle des pays et territoires non coopératifs et les situations similaires impliquant des clients originaires (en raison de leur nationalité, de leur centre d'activité ou de leur résidence) d'un pays ou territoire dont le dispositif de lutte contre le blanchiment et le financement du terrorisme a été considéré comme déficient par le GAFI.

En plus, il peut également exister des clients devenus clients à risque élevé en raison de leur comportement, notamment en raison des transactions effectuées.

#### **Section 4 Pays et territoires non coopératifs (PTNC) et situations similaires**

**91.** Le GAFI publie des déclarations mettant en lumière les lacunes des systèmes de lutte contre le blanchiment et le financement du terrorisme de pays concernés qu'il désigne. Ces déclarations, qu'il faut distinguer des rapports d'évaluation mutuelle établis par le GAFI, sont destinées aux professionnels du secteur financier afin que ceux-ci prennent en considération les risques résultant des lacunes des régimes de lutte contre le blanchiment et le financement du terrorisme ainsi constatées en appliquant des mesures de diligence

renforcées. Les déclarations en question citant les pays actuellement visés peuvent être consultées sur le site internet du GAFI : [www.fatf-gafi.org](http://www.fatf-gafi.org)

**92.** Cette approche du GAFI a remplacé celle par laquelle il a publié dans le passé une liste reprenant les pays et territoires non coopératifs (PTNC) en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, c.-à-d. ceux dont la législation et la réglementation en matière de lutte contre le blanchiment et le financement du terrorisme sont considérées comme n'étant pas conformes aux recommandations du GAFI, ainsi qu'une deuxième liste sur laquelle figurent des PTNC contre lesquels des contre-mesures ont été décidées parce qu'ils ne font pas suffisamment d'efforts pour améliorer leur dispositif de lutte contre le blanchiment et le financement du terrorisme. Ces listes spécifiques ne reprennent actuellement plus aucun pays, de sorte qu'il convient de tenir compte des seules déclarations visées au point 91 ci-dessus.

**93.** Les professionnels du secteur financier doivent suivant l'appréciation du risque :

- se doter d'une politique et de procédures d'acceptation et de suivi des transactions en ce qui concerne les relations avec des contreparties situées dans les pays visés par les déclarations du GAFI, qu'il s'agisse de personnes physiques ou de personnes morales, y compris les professionnels du secteur financier. L'application de cette politique doit être suivie par la personne chargée plus particulièrement de la lutte contre le blanchiment et le financement de terrorisme ;
- procéder en particulier à une identification renforcée. Dans ce contexte, l'origine des fonds doit être vérifiée (au moindre doute ou incertitude, un document probant doit être réclamé) et le professionnel du secteur financier doit obtenir une confirmation du bénéficiaire effectif indiqué attestant par écrit qu'il est le bénéficiaire effectif ;
- impliquer la personne chargée plus particulièrement de la lutte contre le blanchiment et le financement du terrorisme dans la procédure d'acceptation de tels clients, ainsi que prévoir, le cas échéant, compte tenu de la sensibilité du sujet et de l'appréciation du risque, l'autorisation d'un des dirigeants ayant obtenu l'agrément requis par la loi, avant de nouer une relation d'affaires ou d'effectuer une transaction avec de tels clients ;
- examiner avec une attention toute particulière les transactions effectuées avec des contreparties situées dans les pays visés par les déclarations du GAFI, qu'il s'agisse de personnes physiques ou de personnes morales, y compris les professionnels du secteur financier, ou les transactions portant sur des fonds en provenance de ces pays ou territoires.

**94.** Le réviseur d'entreprises doit vérifier le respect des procédures internes en question et en rapporter spécifiquement dans le compte rendu analytique.

### **Chapitre 3 Exécution des mesures de vigilance par des tiers**

**95.** L'exécution des mesures de vigilance prévues à l'article 3 paragraphe (2) points (a) à (c) de la loi modifiée du 12 novembre 2004 ne doit pas nécessairement être effectuée par le professionnel du secteur financier lui-même. Ces mesures peuvent également être exécutées, sous certaines conditions, par des tiers. Le système de l'exécution des mesures de vigilance par des tiers permet d'éviter la répétition des procédures d'identification des clients ainsi que, le cas échéant, des retards dans l'exécution des transactions.

**96.** La loi modifiée du 12 novembre 2004 permet aux professionnels du secteur financier sous certaines conditions d'accepter des clients dont les mesures de vigilance ont été effectuées par une tierce personne (art. 3-3 (1) à (4)) (régime du **tiers introducteur**). Elle permet aussi de confier l'exécution des mesures de vigilance par contrat à un tiers (art. 3-3 (5)) (**externalisation**).

Il convient de noter que seule l'exécution matérielle des mesures de vigilance peut être effectuée par un tiers mais que la décision finale d'entrée en relation appartient toujours au professionnel du secteur financier lui-même.

De même, la responsabilité finale dans l'exécution des obligations de vigilance continue dans tous les cas d'incomber au professionnel qui recourt à des tiers. Le professionnel du secteur financier ne saurait déléguer cette responsabilité, éludant ainsi son obligation de connaître ses clients.

Le tiers exécutant les mesures de vigilance demeure de son côté également responsable de toutes obligations prévues par la loi modifiée du 12 novembre 2004 dans la mesure où il entretient avec le client une relation couverte par cette loi, y compris l'obligation de déclarer les transactions suspectes aux autorités compétentes et de conserver les documents.

#### **Section 1 Régime du tiers introducteur**

**97.** L'article 3-3 (1) à (4) de la loi modifiée du 12 novembre 2004 précise les conditions selon lesquelles les professionnels du secteur financier sont autorisés à accepter des clients dont l'identification a déjà été réalisée par une tierce personne.

##### **Sous-section 1 Tiers acceptés**

**98.** Tiers acceptés luxembourgeois : d'après l'article 3-3 (1) peuvent intervenir comme tiers introducteurs certains professionnels limitativement énumérés par la loi modifiée du 12 novembre 2004. Il s'agit des professionnels luxembourgeois suivants :

- a. établissements de crédit ou autres professionnels du secteur financier (PSF) agréés ou autorisés à exercer leur activité au Luxembourg en vertu de la loi modifiée du 5 avril 1993 relative au secteur financier ;
- b. entreprises d'assurances agréées ou autorisées à exercer leur activité au Luxembourg en vertu de la loi modifiée du 6 décembre 1991 sur le secteur des assurances, pour ce qui concerne des opérations relevant du point 11 de l'annexe de la loi modifiée du 6

décembre 1991 et les intermédiaires d'assurances agréés ou autorisés à exercer leur activité au Luxembourg en vertu de la loi modifiée du 6 décembre 1991 sur le secteur des assurances, lorsqu'ils s'occupent d'assurance vie et d'autres services liés à des placements ;

- c. organismes de placement collectif et sociétés d'investissement en capital à risque qui commercialisent leurs parts ou actions et qui sont visés par la loi modifiée du 20 décembre 2002 concernant les organismes de placement collectif ou par la loi du 13 février 2007 relative aux fonds d'investissement spécialisés ou par la loi du 15 juin 2004 relative à la société d'investissement en capital à risque (SICAR) ;
- d. sociétés de gestion visées par la loi modifiée du 20 décembre 2002 concernant les organismes de placement collectif et qui commercialisent des parts ou des actions d'organismes de placement collectif ou qui exercent des activités additionnelles ou auxiliaires au sens de la loi modifiée du 20 décembre 2002 concernant les organismes de placement collectif ;
- e. réviseurs d'entreprises au sens de la loi modifiée du 28 juin 1984 portant organisation de la profession de réviseur d'entreprises ;
- f. notaires au sens de la loi modifiée du 9 décembre 1976 relative à l'organisation du notariat ;
- g. avocats au sens de la loi modifiée du 10 août 1991 sur la profession d'avocat lorsqu'ils interviennent dans les cas a) à c) visés à l'article 2(1)12. de la loi modifiée du 12 novembre 2004.

**99.** Tiers acceptés d'autres Etats membres de l'Union européenne ou de l'Espace économique européen.

Il s'agit des personnes suivantes :

- a. établissements de crédit et établissements financiers au sens de l'article 3 de la directive 2005/60/CE d'autres Etats membres ;
- b. personnes (morales ou physiques, dans l'exercice de leur activité professionnelle) d'autres Etats membres énumérées à l'article 2 (1) point 3 a) à c) de la directive 2005/60/CE, c.-à-d.
  - i. commissaires aux comptes, experts-comptables externes et conseillers fiscaux;
  - ii. notaires et autres membres de professions juridiques indépendantes, lorsqu'ils participent, au nom de leur client et pour le compte de celui-ci, à toute transaction financière ou immobilière ou lorsqu'ils assistent leur client dans la préparation ou la réalisation de transactions portant sur: i) l'achat et la vente de biens immeubles ou d'entreprises commerciales; ii) la gestion de fonds, de titres ou d'autres actifs appartenant au client; iii) l'ouverture ou la gestion de comptes bancaires, d'épargne ou de portefeuilles; iv) l'organisation des apports nécessaires à la constitution, à la gestion ou à la direction de sociétés; v) la constitution, la gestion ou la direction de fiducies (trusts), de sociétés ou de structures similaires;
  - iii. prestataires de services aux sociétés et fiducies qui ne relèvent pas déjà du point i) ou du point ii) ci-avant.

Il faut que ces tiers introducteurs remplissent chacune des conditions suivantes :

1. ils sont soumis à une obligation d'enregistrement professionnel reconnu par la loi ;
2. ils appliquent à l'égard des clients des mesures de vigilance et de conservation des documents conformes à celles prévues dans la directive 2005/60/CE ;
3. ils sont soumis à la surveillance prévue au chapitre V, section 2 de la directive 2005/60/CE pour ce qui concerne le respect des exigences de la directive 2005/60/CE.

Pour les personnes visées au point a. ci-dessus, qui sont toutes soumises à une surveillance prudentielle conforme aux exigences de la directive 2005/60/CE, les conditions 1. à 3. qui précèdent sont de plein droit remplies.

#### **100. Tiers acceptés de pays tiers :**

Les mesures de vigilance peuvent également être effectuées par des établissements ou des personnes équivalents à ceux visés au point 99 ci-avant, situés sur le territoire d'un pays tiers (pays autre qu'un Etat membre de l'Union européenne ou d'un Etat partie à l'Accord sur l'Espace économique européen) visé par le règlement grand-ducal du 29 juillet 2008 portant établissement de la liste des « pays tiers imposant des obligations équivalentes » au sens de la loi modifiée du 12 novembre 2004, à condition de respecter chacune des conditions suivantes :

1. ils sont soumis à une obligation d'enregistrement professionnel reconnu par la loi ;
2. ils appliquent à l'égard des clients des mesures de vigilance et de conservation des documents conformes ou équivalentes à celles prévues dans la loi modifiée du 12 novembre 2004 ou dans la directive 2005/60/CE ;
3. ils sont soumis à une surveillance équivalente à celle prévue au chapitre V, section 2 de la directive 2005/60/CE.

### **Sous-section 2 Conditions**

**101.** Conformément à l'article 3-3 (2) et (3) de la loi modifiée du 12 novembre 2004, les professionnels qui recourent à des tiers pour l'exécution des obligations de vigilance doivent être sûrs dès le début de leur intervention que l'obtention des documents et informations visés est assurée.

Lorsqu'il s'agit d'un tiers étranger, le professionnel du secteur financier doit s'assurer que celui-ci est d'accord pour intervenir et qu'il mettra immédiatement à sa disposition, sans opposer de règles de confidentialité ou de secret professionnel, les informations demandées conformément aux obligations prévues à l'article 3 (2) points a) à c) de la loi modifiée du 12 novembre 2004 et, sur demande et sans délai, une copie adéquate des données d'identification et de vérification et de tout autre document pertinent concernant l'identité du client et du bénéficiaire effectif.

L'impossibilité pour le professionnel luxembourgeois d'obtenir sans délai les documents ou informations exigés afin qu'ils puissent servir notamment dans le cadre d'une demande de la part des autorités compétentes en matière de lutte contre le blanchiment et le financement du terrorisme constitue une violation de ses obligations professionnelles.

Dans l'hypothèse où le tiers est luxembourgeois, comme il s'agit obligatoirement d'un professionnel auquel s'applique l'article 3-3 (2) et (3) de la loi modifiée du 12 novembre 2004, l'obligation pour lui de fournir les informations et documents en question découle directement de cet article.

Conformément au paragraphe (4) de l'article 3-3 de la loi modifiée du 12 novembre 2004, lorsque les mesures de vigilance ont été exécutées par un tiers étranger conformément à l'article 3 (2) points a) à c) de la loi modifiée du 12 novembre 2004 ou à la directive 2005/60/CE, les résultats des mesures de vigilance exécutées à l'étranger sont reconnus et acceptés au Luxembourg, même si les documents et données sur lesquels portent les obligations de vigilance ont été exécutées sur la base de documents différents de ceux requis au Luxembourg.

## **Section 2 Externalisation**

**102.** Le paragraphe (5) de l'article 3-3 de la loi modifiée du 12 novembre 2004 permet de distinguer le régime du tiers introducteur visé aux points 97 à 101 ci-avant de la situation où les professionnels externalisent ou délèguent par voie contractuelle certaines tâches à d'autres personnes auxquelles ils font confiance et qui ne sont pas soumises à la loi modifiée du 12 novembre 2004 ou à une réglementation en matière de lutte contre le blanchiment et le financement du terrorisme équivalente. Dans le cas de l'externalisation des mesures de vigilance relatives au client, l'agent délégué ou fournisseur externalisé est réputé se confondre avec le professionnel, au sens où les procédures sont ceux du professionnel lui-même.

**103.** Il résulte du considérant 28 de la directive 2005/60/CE que lorsqu'il existe une relation contractuelle d'agence ou d'externalisation (*outsourcing*) entre des professionnels soumis à la loi modifiée du 12 novembre 2004 et des personnes physiques ou morales externes qui ne sont pas soumises à cette loi respectivement la directive précitée, les obligations qui incombent, au titre de la lutte contre le blanchiment ou le financement du terrorisme, à l'agent ou au fournisseur du service externalisé ne peuvent découler que du contrat et non de la loi modifiée du 12 novembre 2004. Il est clair que même si dans ce cas l'article 3-3 ne s'applique pas, la responsabilité entière du respect de la loi modifiée du 12 novembre 2004 continue d'incomber aux professionnels en question. Ceux-ci ont grand intérêt à s'entourer, par le choix de leurs cocontractants et par les termes de leurs contrats, des garanties adéquates pour être en mesure de satisfaire aux obligations de la loi.

Le professionnel ayant choisi un cocontractant auquel il peut faire entière confiance pour l'exécution des obligations de vigilance lui incombant doit toujours signer avec celui-ci un contrat écrit. Ce contrat peut se faire sous forme d'une lettre séparée par laquelle le délégué

s'engage vis-à-vis du professionnel du secteur financier à observer toutes les obligations figurant sur une liste détaillée.

Le contrat d'externalisation doit notamment définir avec précision les tâches déléguées en tenant compte des exigences prescrites par la loi modifiée du 12 novembre 2004 respectivement la directive 2005/60/CE, ainsi que la présente circulaire.

Il doit contenir au minimum une description détaillée des mesures de vigilance (y compris des mesures de vigilance simplifiées et renforcées) que le tiers est appelé à exécuter conformément aux dispositions de la loi modifiée du 12 novembre 2004 et doit décrire en particulier quels sont les informations et documents à réclamer et à vérifier par le délégué. Le contrat doit contenir des conditions relatives à la transmission des informations et documents requis au professionnel luxembourgeois. Le professionnel luxembourgeois devra ainsi être sûr que le tiers délégué mettra immédiatement à sa disposition, sans opposer de règles de confidentialité ou de secret ou d'autres obstacles quelconques, les informations requises et qu'il lui transmettra, sur demande et sans délai, une copie adéquate ou les originaux des données d'identification et de vérification et de tout autre document pertinent concernant l'identité du client et, le cas échéant, du bénéficiaire effectif. Ces documents comportent le document officiel d'identification et le formulaire d'ouverture de compte à l'entête de l'établissement luxembourgeois et reprennent toutes les autres informations nécessaires pour se conformer à l'obligation de connaître le client (but de la relation d'affaires, activité professionnelle, bénéficiaire effectif et le cas échéant l'origine des fonds).

Les copies doivent être certifiées conformes par les délégués ou les personnes admises en cas d'entrée en relation d'affaires à distance en vertu des points 81 à 84 de la présente circulaire. Le professionnel luxembourgeois ne saurait se satisfaire d'un certificat établi par un tiers, quelle que soit sa qualité, attestant que ce tiers connaît l'identité du client, l'a vérifiée et dispose de la documentation requise.

**104.** Les procédures internes des professionnels souhaitant recourir à des tiers introducteurs ou des délégués doivent également contenir des dispositions détaillées sur le régime applicable. Concernant en particulier l'externalisation, les procédures doivent contenir des dispositions relatives au choix du délégué afin que le professionnel puisse être sûr que l'agent respectera les engagements pris aux termes du contrat d'externalisation ou d'agence.

#### **Chapitre 4 Obligations simplifiées de vigilance à l'égard de la clientèle**

**105.** En principe, les professionnels doivent systématiquement appliquer les mesures prévues à l'article 3 de la loi modifiée du 12 novembre 2004, quitte à pouvoir adapter l'étendue de celles visées à l'article 3 (2) en fonction de leur appréciation du risque.

Cependant, afin de prendre en compte les situations où le risque de blanchiment ou de financement du terrorisme est faible, la loi modifiée du 12 novembre 2004 cite un nombre limité de situations où, sauf lorsqu'il y a suspicion de blanchiment ou de financement du terrorisme, les professionnels sont dispensés des obligations de vigilance visées à l'article 3

(2) et (4) 1<sup>er</sup> alinéa. En pratique, la plus grande incidence du régime de vigilance simplifiée se retrouve au niveau de l'identification et de la vérification de l'identité du bénéficiaire effectif à laquelle le professionnel peut en principe renoncer.

**106.** Il convient cependant de noter que ce régime des obligations simplifiées ne permet pas d'exclure toute vigilance de la part du professionnel luxembourgeois.

Ainsi, conformément à l'article 3-1 (3), les professionnels doivent tout d'abord toujours recueillir des informations suffisantes afin qu'ils soient en mesure d'établir s'il s'agit effectivement d'un cas auquel s'applique ou peut s'appliquer le régime des obligations simplifiées.

Ensuite, dans certains cas le professionnel doit d'abord s'assurer que le client, les produits ou transactions en question présentent effectivement un faible risque de blanchiment ou de financement du terrorisme, avant de pouvoir appliquer les mesures de vigilance simplifiées (article 3-1 (5) de la loi modifiée du 12 novembre 2004). Cette obligation de vérification préalable n'existe pas pour tous les cas où l'application de mesures de vigilance simplifiées est prévue, mais seulement dans les cas visés au paragraphe 2 points d) et e) ainsi qu'au paragraphe 4 point e) de l'article 3-1. Lors de cette appréciation, les professionnels doivent être particulièrement attentifs à toute activité desdits clients ou à tout type de produit ou de transaction pouvant être considéré comme particulièrement susceptible, par sa nature, d'être utilisé ou détourné à des fins de blanchiment ou de financement du terrorisme. Le professionnel n'est pas autorisé à appliquer le régime des obligations simplifiées lorsque cette évaluation préalable du risque ne permet pas de conclure qu'il est effectivement faible. Dans ce cas, le professionnel doit appliquer toutes les mesures de vigilance prévues à l'article 3 et peut même être amené, s'il s'avère que le risque est grand, à appliquer des mesures de vigilance renforcées.

Par ailleurs, le régime des obligations simplifiées est toujours écarté dans les cas de soupçon de blanchiment ou de financement du terrorisme au sens de l'article 3 (1) c) de la loi modifiée du 12 novembre 2004. Dans ce cas, une déclaration de soupçon doit être transmise au procureur d'Etat conformément à l'article 5 de la loi modifiée du 12 novembre 2004.

L'application du régime des obligations de vigilance simplifiée n'exonère pas le professionnel du secteur financier des autres obligations professionnelles en matière de lutte contre le blanchiment et le financement du terrorisme, notamment celles de suivi des transactions et de coopération avec les autorités que la loi lui impose à propos de tous ses clients.

**107.** Conformément à l'article 3-1 (1) de la loi modifiée du 12 novembre 2004, les exigences y visées ne s'appliquent pas aux professionnels lorsque le client est :

- un établissement de crédit ou un établissement financier luxembourgeois soumis à la loi modifiée du 12 novembre 2004, ou

- un établissement de crédit ou un établissement financier au sens de l'article 3 de la directive 2005/60/CE d'un autre Etat membre de l'Union européenne ou de l'Espace économique européen, ou
- un établissement de crédit ou un établissement financier établi dans un pays tiers d'un pays indiqué sur la liste figurant dans le règlement grand-ducal du 29 juillet 2008 portant établissement de la liste des pays tiers imposant des obligations équivalentes au sens de la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme et soumis à ce sujet à une surveillance.

Face à ces clients, et surtout ceux de pays tiers, le professionnel luxembourgeois doit tout d'abord s'assurer que le client est effectivement un établissement de crédit ou un établissement financier tel que décrit ci-avant. Cette obligation inclut sans s'y limiter celle de s'assurer que le client n'est pas, en relation avec les dispositions de l'article 3-2 (5), une société bancaire écran.

Si le client du professionnel du secteur financier est un OPC qui ne commercialise pas lui-même ses parts, une société de gestion ou un fonds de pension tel que décrit au point 15 de la présente circulaire, il doit être identifié sur base de ses documents constitutifs.

**108.** La condition d'équivalence est également remplie dans le chef de succursales ou de filiales d'établissements de crédit ou financiers d'un autre Etat membre de l'Union européenne ou de l'Espace économique européen ou issues d'un pays tiers figurant sur la liste publiée par règlement grand-ducal du 29 juillet 2008, peu importe le pays d'implantation de celles-ci, à condition que les établissements en question imposent à leurs succursales et filiales de veiller au respect des dispositions qui leur sont applicables, soit en vertu d'une disposition légale, soit en vertu d'une règle du groupe.

**109.** L'application des mesures simplifiées de vigilance à l'égard de la clientèle n'est pas autorisée au cas où un client auquel s'appliquent les mesures de vigilance simplifiées en vertu de l'article 3-1 de la loi modifiée du 12 novembre 2004 ne fait qu'introduire un ou plusieurs de ses clients auprès d'un professionnel du secteur financier. En effet, si le client n'est pas lui-même un tel client visé à l'article précité, il doit être identifié par le professionnel du secteur financier lui-même avec lequel il entre en relation, le cas échéant à distance ou dans le cadre de l'exécution des mesures d'identification par un tiers, en respectant les dispositions qui s'y appliquent.

**110.** Les cas où les professionnels luxembourgeois ont la faculté de renoncer à l'application des obligations de vigilance sont décrits en détail aux paragraphes (2) et (4) de l'article 3-1 de la loi modifiée du 12 novembre 2004.

Il s'agit des cas repris ci-après :

a) les sociétés dont les valeurs sont admises à la négociation sur un marché réglementé au sens de l'article 1<sup>er</sup>, point 11) de la loi du 13 juillet 2007 relative aux marchés d'instruments financiers dans un Etat membre au moins et les sociétés cotées de pays tiers qui sont

soumises à des exigences de publicité compatibles avec la législation communautaire, c.-à-d. la directive 2007/14/CE de la Commission du 8 mars 2007 portant modalités d'exécution de certaines dispositions de la directive 2004/109/CE sur l'harmonisation des obligations de transparence concernant l'information sur les émetteurs dont les valeurs mobilières sont admises à la négociation sur un marché réglementé ;

b) les bénéficiaires effectifs de comptes groupés tenus par des notaires ou des membres d'une autre profession juridique indépendante établis dans un Etat membre ou un pays tiers, sous réserve que lesdits professionnels soient soumis à des exigences de lutte contre le blanchiment ou le financement du terrorisme satisfaisant aux normes internationales et que le respect de ces obligations soit contrôlé, et sous réserve que les informations relatives à l'identité du bénéficiaire effectif soient mises à la disposition des établissements agissant en qualité de dépositaires pour les comptes groupés, lorsqu'ils en font la demande (cf. aussi points 54 à 56 de la présente circulaire).

c) les autorités publiques luxembourgeoises.

Le régime des obligations simplifiées de vigilance n'est donc pas applicable aux autorités publiques relevant d'un Etat étranger.

d) les clients (n'étant pas des personnes physiques) qui sont des autorités ou des organismes publics présentant un faible risque de blanchiment ou de financement du terrorisme et qui satisfont à tous les critères suivants :

- le client occupe une fonction publique en vertu du traité sur l'Union européenne, des traités instituant les Communautés ou du droit communautaire dérivé ;
- l'identité du client est accessible au public, transparente et certaine ;
- les activités du client, ainsi que ses pratiques comptables, sont transparentes ;
- soit le client est responsable devant une institution communautaire ou devant les autorités d'un Etat membre, soit il existe des procédures appropriées permettant de contrôler l'activité du client ;

e) les clients autres que ceux visés ci-dessus sous d), qui sont des personnes morales présentant un faible risque de blanchiment ou de financement du terrorisme et qui satisfont à tous les critères suivants:

- le client est une entité qui exerce des activités financières ne relevant pas du champ d'application de l'article 2 de la directive 2005/60/CE mais à laquelle la législation à laquelle le client est soumis a étendu les obligations de ladite directive. Cette entité ne comprend les filiales que dans la mesure où les obligations de la directive 2005/60/CE ont été étendues auxdites filiales en tant que telles ;
- l'identité du client est accessible au public, transparente et certaine ;
- le client est soumis par le droit national lui applicable, à l'obligation d'obtenir un agrément pour pouvoir exercer des activités financières et cet agrément peut être refusé si les autorités compétentes ne sont pas convaincues de l'aptitude et de l'honorabilité des personnes qui dirigent ou dirigeront effectivement les activités de cette entité ou de son bénéficiaire effectif. A cette fin, l'activité exercée par le client est surveillée par des autorités compétentes. Dans ce contexte, il convient d'entendre par « surveillance » une activité de surveillance comportant les pouvoirs les plus étendus, et notamment la

possibilité d'effectuer des inspections sur place. Ces inspections comprennent l'examen des politiques, des procédures et des livres et enregistrements, ainsi que le contrôle par sondage ;

- le client est soumis à une surveillance par des autorités compétentes pour ce qui concerne le respect de la législation nationale transposant ladite directive et, le cas échéant, des autres obligations prévues par la législation nationale lui applicable ;
- le non-respect par le client des obligations visées au présent point e) 1er tiret entraîne l'application de sanctions effectives, proportionnées et dissuasives, y compris des mesures administratives appropriées ou des sanctions administratives.

Il convient de rappeler que dans tous les cas visés ci-avant, les professionnels sont tenus de recueillir en toutes circonstances des informations suffisantes pour établir si le client remplit les conditions requises pour bénéficier d'une dérogation.

**111.** La loi modifiée du 12 novembre 2004 prévoit également la possibilité d'appliquer des procédures de vigilance simplifiées à l'égard de la clientèle en cas d'investissement dans certains produits et transactions présentant un risque faible de blanchiment ou de financement du terrorisme.

Il s'agit des cas repris ci-après :

a) les polices d'assurance vie dont la prime annuelle ne dépasse pas 1.000 euros ou dont la prime unique ne dépasse pas 2.500 euros ;

b) les contrats d'assurance retraite qui ne comportent pas de clause de rachat et qui ne peuvent être utilisés en garantie ;

c) les régimes de retraite ou dispositifs similaires versant des prestations de retraite aux employés, pour lesquels les cotisations se font par déduction du salaire et dont les règles ne permettent pas aux bénéficiaires de transférer leurs droits ;

d) la monnaie électronique au sens de l'article 12-10 de la loi modifiée du 5 avril 1993 relative au secteur financier lorsque, si le support ne peut pas être rechargé, la capacité maximale de chargement du support n'est pas supérieure à 150 euros; ou lorsque, si le support peut être rechargé, une limite de 2.500 euros est fixée pour le montant total des transactions dans une année civile, sauf lorsqu'un montant d'au moins 1.000 euros est remboursé dans la même année civile au porteur comme indiqué à l'article 12-12 de la loi modifiée du 5 avril 1993 relative au secteur financier ;

e) d'autres produits ou transactions se rapportant à ces produits présentant un faible risque de blanchiment ou de financement du terrorisme et qui satisfont à tous les critères suivants :

- le produit repose sur une base contractuelle écrite ;
- la transaction y afférente est effectuée via un compte détenu par le client auprès d'un établissement de crédit d'un Etat membre ou auprès d'un établissement de crédit situé dans un pays tiers qui impose des exigences équivalentes à celles que prévoit la loi modifiée du 12 novembre 2004 ou la directive 2005/60/CE ;

- le produit ou la transaction y afférente n'est pas anonyme et est de telle nature qu'il ou elle permet l'application en temps opportun de l'article 3, paragraphe 1, point c) ;
- le produit est soumis au seuil prédéterminé maximum de 15.000 euros, sous réserve des dérogations ci-dessous.

En cas de police d'assurance ou de produit d'épargne analogue, les seuils visés au sous-paragraphe a) du présent point 111 s'appliquent.

Pour les produits liés au financement d'actifs physiques, lorsque la propriété juridique et effective de ces actifs n'est transférée au client qu'à la cessation de la relation contractuelle, le seuil fixé au sous-paragraphe a) du présent point 111 peut être dépassé, à condition de ne dépasser un seuil maximum de 15.000 euros par an pour les transactions relatives à ce type de produit, que la transaction soit effectuée en une seule opération ou en plusieurs opérations apparaissant comme liées.

- les gains liés au produit ou à la transaction y afférente ne peuvent être réalisés au profit de tiers, sauf en cas de décès, d'incapacité, de survie à un âge avancé prédéterminé, ou d'événement analogue ;
- lorsque le produit ou la transaction y afférente permet le placement de fonds dans des actifs financiers ou des créances, y compris des produits d'assurance ou tout autre type de créance éventuelle :
  - i) les gains liés au produit ou à la transaction y afférente ne sont réalisables qu'à long terme ;
  - ii) le produit ou la transaction y afférente ne peut être utilisé en garantie ;
  - iii) au cours de la relation contractuelle, aucun paiement anticipé n'est effectué, aucune clause de rachat n'est utilisée et aucune résiliation anticipée n'intervient.

## **Chapitre 5 Obligations d'organisation interne adéquate**

**112.** En vertu de l'article 4 (1), (2) et (3) de la loi modifiée du 12 novembre 2004, les professionnels du secteur financier sont tenus :

- de mettre en place des mesures et des procédures adéquates et appropriées en matière de vigilance à l'égard du client, de déclaration, de conservation des documents et pièces, de contrôle interne, d'évaluation et de gestion des risques, de gestion du respect des obligations et de communication, afin de prévenir et d'empêcher les opérations de blanchiment ou de financement du terrorisme.
- de prendre les mesures adéquates et appropriées pour sensibiliser et former leurs employés concernés aux dispositions légales relatives aux obligations professionnelles en matière de lutte contre le blanchiment et le financement du terrorisme auxquelles ils sont soumis. Ces mesures comprennent la participation de leurs employés concernés à des programmes de formation spéciaux afin de les aider à reconnaître les opérations qui peuvent être liées au blanchiment ou au financement du terrorisme et de les instruire sur la manière de se comporter en pareil cas.

- de disposer de systèmes leur permettant de répondre de manière rapide et complète à toute demande d'informations des autorités luxembourgeoises responsables de la lutte contre le blanchiment et le financement du terrorisme, tendant à déterminer s'ils entretiennent ou ont entretenu au cours des cinq années précédentes une relation d'affaires avec une personne physique ou morale donnée, et quelle est ou a été la nature de cette relation.

Ces procédures et mesures doivent être établies par chaque professionnel en tenant compte de ses activités et de ses spécificités d'échelle et de taille et contrôlées conformément aux dispositions reprises au point 3 ci-dessus. Elles doivent être communiquées, le cas échéant, aux succursales et aux filiales visées à l'article 2 (2) de la loi modifiée du 12 novembre 2004.

### **Section 1 Obligation d'instaurer des procédures écrites de contrôle interne et de communication**

**113.** Chaque professionnel du secteur financier est tenu de mettre au point un programme de lutte contre le blanchiment et le financement du terrorisme, comprenant les politiques, procédures et contrôles internes nécessaires afin de satisfaire entièrement à chacune des obligations professionnelles découlant de la loi modifiée du 12 novembre 2004. Il convient que les professionnels ajustent les procédures en fonction des spécificités de leurs activités respectives et des différences d'échelle et de taille qu'ils présentent. Les procédures prévoient également la désignation d'une personne chargée plus particulièrement de la lutte contre le blanchiment et le financement du terrorisme, ainsi que des procédures adéquates relatives à l'embauche des employés.

A cet effet, chaque professionnel du secteur financier est tenu de disposer d'un manuel de procédures précis et complet, régulièrement mis à jour, comportant notamment :

- la description détaillée des procédures à suivre, quant au fond et quant à la forme, lors de l'entrée en relation d'affaires avec un client ou lors de transactions avec des clients occasionnels, par type de relation d'affaires ou de transaction ainsi que par type de client (particulier, commerçant, société commerciale, holding, etc.).

Les procédures doivent comporter une description et une justification des situations donnant, le cas échéant, lieu à un ajustement de la portée des obligations de vigilance en fonction de l'appréciation faite par le professionnel concerné du risque associé au type de client, de relation d'affaires, de produit ou de transaction concerné sur la base de l'article 3 (3) de la loi modifiée du 12 novembre 2004. Des mesures de vigilance simplifiées peuvent être prévues et des mesures de vigilance renforcées doivent l'être pour les situations, clients, produits et transactions respectifs, dont notamment ceux relevés aux points 80 et suivants ci-dessus.

Elles doivent aussi comporter des mesures destinées à empêcher l'utilisation de produits ou la réalisation de transactions favorisant l'anonymat visées à l'article 3-2 (6) de la loi modifiée du 12 novembre 2004, notamment dans le domaine des technologies nouvelles.

Les professionnels doivent, le cas échéant, disposer de dispositifs de gestion des risques spécifiques liés aux relations d'affaires ou aux transactions qui n'impliquent pas la présence physique des parties.

- la description détaillée des procédures à suivre quant au fond et quant à la forme, lorsque le professionnel du secteur financier est confronté à une demande d'entrée en relation d'affaires ou d'effectuer une transaction occasionnelle pour une personne (p.ex. un avocat ou un notaire) dont l'activité professionnelle normale implique la conservation de fonds de tiers auprès d'un professionnel financier respectivement l'ouverture d'un compte groupé.

Le point 54 de la présente circulaire précise en particulier que le professionnel du secteur financier doit demander expressément à une telle personne si elle agit pour compte propre ou pour compte d'autrui et qu'il doit apprécier la plausibilité de cette réponse.

- la description détaillée des procédures à suivre, quant au fond et quant à la forme, lorsque le professionnel sait, soupçonne ou a de bonnes raisons de soupçonner qu'un blanchiment ou un financement du terrorisme est en cours ;
- la description détaillée des procédures à suivre quant au fond et quant à la forme, lorsqu'est constaté un fait qui pourrait être l'indice d'un blanchiment ou d'un financement du terrorisme et dont le professionnel du secteur financier a eu connaissance dans l'exercice de son activité professionnelle sans qu'une relation d'affaires ait été nouée ou qu'une transaction ait été effectuée. Les procédures doivent prévoir que toute entrée en contact doit être documentée, quelle que soit la forme de cette entrée en contact. La notion d'entrée en contact avec un client vise toutes formes possibles de contact, y compris les entrées en contact par voie postale, par entretien téléphonique ou par voie électronique (Internet par exemple). Les procédures à adopter par les professionnels du secteur financier doivent être adaptées aux différentes formes d'entrée en contact possibles et notamment prévoir les questions adéquates à poser par le professionnel du secteur financier en fonction de la forme d'entrée en contact en question et du degré d'intensité de cette entrée en contact.

Le professionnel du secteur financier devra documenter tous les indices de blanchiment et de financement du terrorisme dont il a eu connaissance dans le cadre de son contact commercial.

La documentation doit contenir toutes les informations que le professionnel du secteur financier a obtenues sur la personne qui est entrée en contact avec lui. En outre, elle doit contenir les raisons du professionnel du secteur financier de ne pas entrer en relation d'affaires ou de ne pas effectuer la transaction en question pour ledit client potentiel. Lorsque la décision du professionnel du secteur financier de ne pas établir une relation d'affaires ou de ne pas effectuer une transaction a été prise sans qu'un fait lié à un indice de blanchiment ou de financement du terrorisme soit à la base de sa décision de refus, cette décision doit également être documentée dans la mesure du possible.

- la description détaillée des procédures à respecter quant au fond et quant à la forme, pour suivre l'évolution des opérations effectuées pour leurs clients afin de pouvoir détecter les transactions suspectes.

Des procédures spéciales doivent être mises en place pour assurer un suivi renforcé des clients à risque élevé, dont notamment ceux relevés aux points 80 et suivants ci-dessus.

- la description détaillée des procédures à suivre quant au fond et quant à la forme, pour respecter l'obligation de transmettre à la CSSF, parallèlement à toute transmission d'informations au procureur d'Etat sur base de l'article 5 (1) de la loi modifiée du 12 novembre 2004 les mêmes informations que celles communiquées au procureur d'Etat ;
- la description détaillée des procédures à suivre quant au fond et quant à la forme, si le professionnel du secteur financier recourt à des opérations à distance ;
- la définition exacte des responsabilités respectives de tous les employés intervenant dans ces procédures.

## **Section 2 Obligation de former et de sensibiliser le personnel**

**114.** Chaque professionnel du secteur financier est tenu de disposer d'un programme de formation et de sensibilisation de ses employés, adapté à l'évolution des techniques du blanchiment et de financement du terrorisme, comportant notamment :

- des programmes spéciaux de formation continue, prévoyant des cours donnés à des intervalles réguliers, s'adressant en particulier aux employés en contact direct avec la clientèle pour les aider à reconnaître les opérations de blanchiment ou de financement du terrorisme et les instruire sur les procédures à suivre ;
- des réunions d'information régulières, s'adressant aux employés pour les tenir au courant des règles et procédures préventives à respecter en matière de lutte contre le blanchiment ou le financement du terrorisme ;
- la désignation d'une ou de plusieurs personnes compétentes pour répondre à tout moment aux questions des autres employés à propos du blanchiment ou du financement du terrorisme ;
- la diffusion systématique d'une documentation sur le blanchiment et le financement du terrorisme, donnant notamment des exemples d'opérations de blanchiment ou de financement du terrorisme, telle que la liste indicative d'indices de blanchiment annexée à la présente circulaire.

**115.** Dans la mesure où les professionnels du secteur financier luxembourgeois reprennent les manuels de procédures et programmes de sensibilisation élaborés à l'étranger, p.ex. par leur siège ou leur maison mère, ils sont tenus d'adapter ces procédures et programmes aux normes applicables au Luxembourg.

### **Section 3 Obligation de disposer de systèmes permettant de répondre aux demandes d'informations des autorités luxembourgeoises**

**116.** D'après l'article 4 (3) de la loi modifiée du 12 novembre 2004, les établissements de crédit et les établissements financiers sont tenus de disposer de systèmes leur permettant de répondre de manière rapide et complète à toute demande d'informations des autorités luxembourgeoises responsables de la lutte contre le blanchiment et le financement du terrorisme, tendant à déterminer s'ils entretiennent ou ont entretenu au cours des cinq années précédentes une relation d'affaires avec une personne physique ou morale donnée, et quelle est ou a été la nature de cette relation.

Il importe en effet que les professionnels auxquels s'applique cette obligation soient en mesure de répondre rapidement et de façon complète aux demandes d'information de la part des autorités compétentes en matière de lutte contre le blanchiment et le financement du terrorisme concernant les relations d'affaires qu'ils entretiennent ou ont entretenu éventuellement avec des personnes nommément désignées y compris celles figurant sur les listes de personnes soupçonnées en matière de lutte contre le terrorisme et son financement.

Afin d'identifier ces relations d'affaires et d'être en mesure de donner rapidement suite à ces demandes d'information, les professionnels doivent disposer de systèmes efficaces, proportionnels à la taille et à la nature de leurs activités. Il est recommandé en particulier que les établissements de crédit et les grands établissements financiers disposent de systèmes électroniques permettant de détecter les personnes visées.

Ces systèmes électroniques sont également particulièrement importants dans le cadre des procédures qui entraînent des mesures telles que le gel ou la saisie d'avoirs, conformément à la législation nationale et communautaire applicable.

Il est rappelé que les procédures relatives au recours à des tiers en vue de l'exécution des mesures de vigilance doivent permettre une bonne coopération avec les autorités luxembourgeoises compétentes en matière de lutte contre le blanchiment et le financement du terrorisme.

## **Chapitre 6 Obligations de coopération avec les autorités**

### **Section 1 Obligation générale de coopérer avec les autorités chargées de l'application des lois**

**117.** En vertu de l'article 40 de la loi modifiée du 5 avril 1993 relative au secteur financier, les professionnels du secteur financier sont obligés de fournir une réponse et une coopération aussi complètes que possible à toute demande légale que les autorités chargées de l'application des lois leur adressent dans l'exercice de leurs compétences.

## **Section 2 Obligation de coopérer avec les autorités luxembourgeoises responsables de la lutte contre le blanchiment et le financement du terrorisme**

**118.** En vertu de l'article 5 de la loi modifiée du 12 novembre 2004, les professionnels du secteur financier, leurs dirigeants et employés sont obligés de coopérer pleinement avec les autorités luxembourgeoises responsables de la lutte contre le blanchiment et le financement du terrorisme.

### **Sous-section 1 Obligation de fournir au procureur d'Etat auprès du tribunal d'arrondissement à Luxembourg, à sa demande, toutes les informations requises**

**119.** En vertu de l'article 5 (1) b), les professionnels du secteur financier doivent pleinement coopérer avec le procureur d'Etat en lui fournissant promptement, à sa demande, toutes les informations nécessaires qu'il requerra. Il est rappelé que dans ce cas le secret professionnel est levé.

Il est rappelé dans ce contexte que les professionnels doivent se conformer aux procédures qu'ils doivent mettre en place sur la base de l'article 4 (3) de la loi modifiée du 12 novembre 2004 et visées au point 116 ci-avant.

### **Sous-section 2 Obligation d'informer, de sa propre initiative, le procureur d'Etat auprès du tribunal d'arrondissement à Luxembourg de tout soupçon ou certitude de blanchiment ou de financement du terrorisme**

#### ***Paragraphe 1 Personnes chargées d'informer le procureur d'Etat***

**120.** La transmission des informations au procureur d'Etat, sur sa demande ou à l'initiative des professionnels du secteur financier, est à effectuer par la personne chargée plus particulièrement de la lutte contre le blanchiment et le financement du terrorisme conformément aux procédures internes que les professionnels du secteur financier sont tenus d'instaurer. Il y a lieu de rappeler qu'il doit s'agir du responsable de la fonction *compliance* ou de son remplaçant en ce qui concerne les établissements de crédit et les entreprises d'investissement. Pour les autres professionnels du secteur financier, il doit s'agir d'un dirigeant ayant obtenu l'agrément requis par la loi.

Il convient de noter que l'identité des employés du professionnel ayant fourni les informations est tenue confidentielle par les autorités responsables sauf si sa révélation est indispensable pour assurer la régularité des poursuites en justice ou assurer la preuve des faits formant la base de ces poursuites.

**121.** Chaque professionnel du secteur financier est tenu d'informer la CSSF du nom des personnes désignées au procureur d'Etat comme responsables des informations à fournir au procureur d'Etat. Ces personnes seront aussi les personnes de contact de la CSSF pour toute question ayant trait au blanchiment ou au financement du terrorisme.

**122.** Dans ce contexte, le parquet du tribunal d'arrondissement de Luxembourg, étant compétent en la matière pour tout le territoire du Grand-Duché de Luxembourg, a adressé une circulaire à tous les professionnels du secteur financier pour régler les modalités pratiques des informations à fournir au procureur d'Etat (Circulaire 20/08 CRF du 12 novembre 2008).

### ***Paragraphe 2 Circonstances dans lesquelles le procureur d'Etat doit être informé***

**123.** Le présent point a pour objet d'apporter des précisions sur la démarche que le professionnel du secteur financier doit suivre lorsqu'il est confronté à une situation ou à une personne suspecte, afin de le sensibiliser aux risques auxquels il peut être exposé et de le sécuriser dans son comportement. En effet, en cas de déclaration intempestive, il risque que son client lui reproche d'avoir violé son obligation au secret professionnel. Il s'expose par contre à des poursuites pénales lorsqu'il s'abstient de déclarer dans l'hypothèse visée par l'article 5 de la loi modifiée du 12 novembre 2004.

Conformément à l'article 5 (1) a) de la loi modifiée du 12 novembre 2004, le professionnel doit promptement faire une déclaration au Parquet lorsqu'il soupçonne ou a de bonnes raisons de soupçonner qu'un blanchiment ou un financement du terrorisme est en cours, a eu lieu ou a été tenté. Il doit également faire une déclaration lorsqu'il sait, c.-à-d. a la certitude que tel est le cas.

#### **I. Précisions des critères à prendre en compte pour détecter un blanchiment ou un financement du terrorisme**

**124.** L'article 5 (1) a) susdit donne des indications sur les critères (personne concernée, évolution du client, origine des avoirs, nature, finalité ou modalités de l'opération) à prendre en compte pour apprécier si on est en présence d'un soupçon de blanchiment ou de financement du terrorisme. Par ailleurs, une liste non limitative d'indices de blanchiment se trouve en annexe II de la présente circulaire.

**125.** Afin d'informer les professionnels du secteur financier quant à la portée de l'infraction de blanchiment et de l'infraction de financement du terrorisme et quant à l'étendue de l'obligation de déclaration, la liste des infractions primaires au point 8 ci-dessus est divisée suivant les catégories d'infractions primaires retenues au niveau du GAFI.

**126.** Le professionnel du secteur financier doit déclarer au procureur d'Etat, dans le cadre de la lutte contre le financement du terrorisme, également les transactions dans lesquelles interviennent des personnes figurant sur les listes officielles reprenant des terroristes ou organisations terroristes présumés (v. Annexe III).

#### **II. Précisions sur l'obligation d'information en matière de lutte contre le blanchiment et le financement du terrorisme**

**127.** Au cas où le professionnel du secteur financier sait, soupçonne ou a de bonnes raisons de soupçonner qu'un blanchiment ou financement du terrorisme est en cours, a eu lieu, ou a

été tenté, il doit promptement en informer le procureur d'Etat auprès du tribunal d'arrondissement de Luxembourg. Un soupçon peut être provoqué notamment en raison de la personne concernée, de son évolution, de l'origine des avoirs, de la nature, de la finalité ou des modalités de l'opération.

Lorsqu'il se trouve face à une situation dont il estime qu'elle pourrait donner lieu à un soupçon de blanchiment ou de financement du terrorisme, le professionnel du secteur financier doit se demander si les fonds faisant l'objet d'une ou de plusieurs transactions sont susceptibles de provenir de l'une des infractions primaires visées au point 8 de la présente circulaire. Afin de pouvoir, dans de telles circonstances, déterminer s'il est dans l'obligation de déclarer, conformément à l'article 5 (2) a), le professionnel du secteur financier doit chercher à élucider la situation à bref délai, notamment en interrogeant le client sur l'origine des fonds et en l'invitant à fournir tous les renseignements utiles complémentaires.

**128.** Le professionnel du secteur financier appréciera ensuite la vraisemblance ou la plausibilité des explications fournies. S'agissant de contacts avec des PPE résidant à l'étranger telles que visées aux points 85 à 88, le professionnel doit prévoir l'intervention de la personne chargée plus particulièrement de la lutte contre le blanchiment et le financement du terrorisme. Si une telle démarche ne permet pas de clarifier la situation de façon satisfaisante ou lorsque le professionnel du secteur financier est personnellement convaincu que son soupçon est justifié, il est obligé d'en informer promptement le procureur d'Etat auprès du tribunal d'arrondissement de Luxembourg. Il est précisé que l'obligation d'informer le procureur d'Etat auprès du tribunal d'arrondissement de Luxembourg promptement existe dès le moment où le professionnel sait, soupçonne ou a effectivement de bonnes raisons de soupçonner qu'un blanchiment ou financement du terrorisme est en cours, a eu lieu ou a été tenté.

**129.** Le professionnel du secteur financier n'a cependant pas à qualifier pénalement les faits ni à en prouver l'exactitude. Cette tâche revient aux autorités judiciaires compétentes.

**130.** La démarche du professionnel sera la même lorsque les faits ont été commis à l'étranger.

### III. Précisions sur l'obligation d'information en cas d'entrée en contact sans nouer une relation d'affaires et/ou sans effectuer une transaction

**131.** En présence d'indices de blanchiment ou de financement du terrorisme, l'obligation d'informer le procureur d'Etat, telle que prévue à l'article 5 de la loi modifiée du 12 novembre 2004, couvre également le cas où le professionnel du secteur financier est entré en contact avec une personne ou une société sans qu'une relation d'affaires ait été nouée ou qu'une transaction ait été effectuée.

Dans ce cas, le professionnel devra documenter toutes les informations qu'il a obtenues sur la personne qui est entrée en contact avec lui ainsi que tous les indices de blanchiment ou de financement du terrorisme dont il a eu connaissance dans le cadre de ce contact.

**132.** Il n'y a pas de déclaration à faire lorsque la décision de ne pas établir une relation d'affaires ou de ne pas effectuer une transaction a été prise sans qu'un indice de blanchiment ou de financement du terrorisme soit venu à la connaissance du professionnel du secteur financier.

Dans ce cas, les raisons qui sont à la base du refus formel du préposé ou de l'organe du professionnel habilité à autoriser l'entrée en relation doivent également être documentées dans la mesure du possible, ensemble avec les informations que le professionnel a obtenues sur la personne qui est entrée en contact avec lui.

***Paragraphe 3 Dispense de l'obligation au secret professionnel et absence de responsabilité de toute sorte en cas de déclaration de bonne foi***

**133.** L'obligation au secret professionnel cesse lorsque la révélation d'un renseignement est autorisée ou imposée en vertu d'une disposition législative.

**134.** La loi modifiée du 12 novembre 2004 souligne qu'en cas de déclaration de bonne foi au procureur d'Etat, les professionnels du secteur financier n'encourent de responsabilité d'aucune sorte. En utilisant cette notion plus large que la seule référence à la responsabilité civile et pénale, la loi exclut également toute responsabilité disciplinaire.

**135.** Il convient en outre de souligner que les informations sur des soupçons ou certitudes de blanchiment ou de financement du terrorisme sont fournies au procureur d'Etat sous la responsabilité du professionnel du secteur financier.

**136.** L'exonération de responsabilité ne couvre pas les déclarations de mauvaise foi, telles que notamment des déclarations de faits dont le professionnel du secteur financier a la certitude qu'ils ne constituent pas des faits de blanchiment ou de financement de terrorisme ou des déclarations faites pour nuire au client ou à l'employeur alors que les éléments qui justifieraient des soupçons font défaut.

***Paragraphe 4 Obligation de transmettre les mêmes informations à la CSSF que celles transmises au procureur d'Etat***

**137.** Les professionnels du secteur financier doivent transmettre à la CSSF, afin qu'elle puisse exercer sa mission de surveillance prudentielle, séparément et parallèlement à toute transmission d'informations au procureur d'Etat sur base de l'article 5 (1) a), les mêmes informations que celles communiquées au procureur d'Etat quelle que soit l'origine de la procédure d'information et quel que soit le contenu de l'information communiquée.

***Paragraphe 5 Pouvoirs du procureur d'Etat à la suite d'une information***

**I. Instruction de blocage**

**138.** L'article 5 (3) permet le blocage par le procureur d'Etat d'une ou de plusieurs opérations suspectes, confirmant ainsi que l'instruction de blocage du procureur d'Etat peut bien porter non seulement sur une seule opération, mais aussi sur un ensemble d'opérations

en rapport avec une transaction suspecte ou un client suspecté de vouloir effectuer de telles transactions.

## II. Instruction de blocage limitée dans le temps

**139.** L'article 5 (3) donne des précisions sur les effets dans le temps d'une instruction de blocage du procureur d'Etat. L'instruction du procureur d'Etat de ne pas exécuter une ou des opérations est limitée à une durée maximale de validité de trois mois à partir de la communication écrite ou orale de l'instruction de blocage au professionnel du secteur financier.

En cas d'instruction orale, cette communication doit être suivie dans les trois jours d'une confirmation écrite par le procureur d'Etat. A défaut de communication écrite, les effets de l'instruction cessent le troisième jour à minuit.

### ***Paragraphe 6 Comportement du professionnel du secteur financier en cas de transaction suspecte et d'information du procureur d'Etat***

#### I. Interdiction d'exécuter la transaction avant d'avoir informé le procureur d'Etat

**140.** Les professionnels du secteur financier sont tenus de s'abstenir d'exécuter la transaction qu'ils savent ou soupçonnent d'être liée au blanchiment ou au financement du terrorisme avant d'en avoir informé le procureur d'Etat.

Si la transaction en question est soupçonnée de donner lieu à une opération de blanchiment ou à un financement du terrorisme et lorsqu'une telle abstention n'est pas possible ou est susceptible d'empêcher la poursuite des bénéficiaires d'une opération suspectée de blanchiment ou de financement du terrorisme, les professionnels du secteur financier concernés procèdent immédiatement après à l'information requise.

**141.** Il convient cependant que les professionnels évitent toujours d'exécuter une transaction lorsque celle-ci est touchée par des mesures visant à geler sans tarder les fonds et autres avoirs terroristes, des organisations terroristes, et des organisations qui financent le terrorisme, notamment en vertu de dispositions nationales ou communautaires directement applicables.

#### II. Interdiction d'avertir le client dont les transactions se trouvent bloquées ou pourraient être bloquées du fait d'une instruction du procureur d'Etat

**142.** L'article 5 (5) de la loi modifiée du 12 novembre 2004 donne des instructions claires quant au comportement à adopter envers le client dont les transactions se trouvent bloquées ou pourraient être bloquées du fait d'une enquête du procureur d'Etat.

Principe et exception :

Si le principe général du « *no tipping off* », c.-à-d. l'interdiction de communiquer aux clients concernés ou à des personnes tierces (la CSSF, les réviseurs d'entreprises agissant dans le cadre de la mission de contrôle des comptes des professionnels du secteur financier et les

avocats conseils des professionnels du secteur financier n'étant pas considérés comme personnes tierces) que des informations ont été transmises au procureur d'Etat ou qu'une enquête sur le blanchiment ou le financement du terrorisme est en cours ou pourrait être ouverte, est confirmé par l'article 5 (5) de la loi modifiée du 12 novembre 2004, l'article 5 (3) autorise le professionnel du secteur financier à invoquer l'instruction de blocage du procureur d'Etat à l'encontre du client pour motiver son refus d'exécuter l'ordre du client, si le client demande les motifs du refus.

### III. Relations avec les organes internes de contrôle du groupe

**143.** Afin de permettre de coordonner la lutte contre le blanchiment et le financement du terrorisme au niveau le plus élevé d'un groupe financier international dont le professionnel du secteur financier établi au Luxembourg fait partie, la législation luxembourgeoise permet un échange d'informations au sein d'un groupe en visant le cas de figure suivant.

**144.** L'article 41 de la loi modifiée du 5 avril 1993 relative au secteur financier, garantit aux organes internes de contrôle du groupe dont fait partie le professionnel du secteur financier établi au Luxembourg, l'accès, en cas de besoin, aux informations concernant des relations d'affaires déterminées, dans la mesure nécessaire à la gestion globale des risques juridiques et de réputation liés au blanchiment ou au financement du terrorisme au sens de la loi luxembourgeoise.

Cet échange d'informations ne risque pas d'enfreindre la règle du « *no tipping off* » puisque il résulte de l'article 5 (5) de la loi modifiée du 12 novembre 2004 que cette interdiction n'est pas applicable à ce type d'échange d'informations.

### Chapitre 7 Obligations en cas de virement et de transfert de fonds

**145.** En vertu de l'article 39, 2<sup>e</sup> alinéa de la loi modifiée du 5 avril 1993 relative au secteur financier, les établissements de crédit et les autres professionnels du secteur financier (PSF) sont obligés au respect des règles édictées par le règlement (CE) 1781/2006 du 15 novembre 2006 du Parlement européen et du Conseil relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds (v. Annexe IV). Cette disposition qui remplace l'ancien 2<sup>e</sup> alinéa de l'article 39 introduit par la loi du 12 novembre 2004 sert à confirmer l'application du règlement communautaire 1781/2006, en vigueur depuis le 1<sup>er</sup> janvier 2007 (cf. circulaire CSSF 06/274 du 22 décembre 2006). Elle assure également que les sanctions prévues à l'article 63 de la loi modifiée du 5 avril 1993 relative au secteur financier sont applicables à ce texte communautaire dont elle transpose ainsi l'article 15 qui impose aux Etats membres d'en déterminer le régime de sanctions.

Le règlement (CE) 1781/2006 oblige le prestataire de services de paiement du donneur d'ordre à incorporer aux virements et transferts de fonds ou aux messages s'y rapportant des informations sur le donneur d'ordre, c.-à-d. le client. Celles-ci doivent être plus ou moins détaillées selon qu'il s'agit de virements de fonds à l'intérieur de l'Union européenne ou de virements effectués de l'intérieur vers l'extérieur de l'Union européenne. Concernant, en particulier, les virements à l'intérieur de la Communauté, au lieu d'inclure des informations

complètes telles que définies au Règlement, il est possible d'appliquer un régime allégé suivant lequel les virements doivent seulement être accompagnés d'informations simplifiées, c.-à-d. le numéro de compte du donneur d'ordre ou un identifiant permettant de remonter jusqu'au donneur d'ordre. Dans ce cas, le prestataire de services de paiement du donneur d'ordre doit néanmoins être en mesure de mettre à la disposition du prestataire de services de paiement du bénéficiaire, dans les trois jours de la demande de ce dernier, les informations complètes sur le donneur d'ordre telles que définies à l'article 4 du règlement 1781/2006. Il est donc également possible d'appliquer le régime des informations complètes aux virements de fonds à l'intérieur de l'Union européenne.

Le règlement (CE) 1781/2006 impose également des obligations au prestataire de services de paiement du bénéficiaire du virement relatives notamment à la détection de transferts dont les informations sur le donneur d'ordre manquent.

Afin de vérifier si les informations requises sur le donneur d'ordre accompagnent effectivement les virements de fonds et de faciliter la détection d'opérations suspectes, les professionnels concernés doivent disposer de procédures efficaces pour détecter les informations manquantes sur le donneur d'ordre.

A ce sujet, le document « *Common understanding of the obligations imposed by European Regulation 1781/2006 on the information on the payer accompanying fund transfers to payment service providers of payees* » établi au niveau de CEBS, CESR et CEIOPS fournit des clarifications destinées à aider les professionnels concernés à se conformer aux dispositions du règlement communautaire en question (Annexe V).

## **Titre 3 Contrôle du respect des obligations professionnelles**

### **Chapitre 1 L'autorité compétente : la CSSF**

**146.** L'article 15 de la loi modifiée du 12 novembre 2004, en disposant que la CSSF est l'autorité compétente, sans préjudice des compétences du procureur d'Etat, pour assurer le respect des obligations professionnelles en matière de lutte contre le blanchiment et contre le financement du terrorisme, confirme expressément le rôle joué par la CSSF en matière de lutte contre le blanchiment et le financement du terrorisme.

**147.** Pour remplir cette mission, la CSSF :

- effectue régulièrement des contrôles sur place ;
- exige qu'en cas de déclaration au procureur d'Etat, une copie du dossier concerné soit transmise en même temps à la CSSF. Les dossiers doivent être également transmis à la CSSF lorsque l'enquête fait suite à une initiative des autorités judiciaires compétentes ;

- exige d'une part que le mandat que les professionnels du secteur financier donnent à leurs réviseurs d'entreprises pour le contrôle des comptes annuels comporte la mission de vérifier le respect des dispositions légales en matière de lutte contre le blanchiment et le financement du terrorisme, des circulaires CSSF en la matière ainsi que la bonne application des procédures internes y relatives et d'autre part que le rapport du réviseur d'entreprises soit transmis à la CSSF ;
- exige que le respect des mêmes obligations et procédures fasse l'objet d'une vérification à fréquence élevée par le responsable de la fonction *compliance* du professionnel du secteur financier et par son service d'audit interne.

## **Chapitre 2 Le réviseur d'entreprises**

**148.** Le mandat que le professionnel du secteur financier donne à son réviseur d'entreprises pour le contrôle des comptes annuels doit comporter la mission de vérifier le respect des obligations professionnelles légales en matière de lutte contre le blanchiment et le financement du terrorisme, de la présente circulaire et d'autres circulaires, ainsi que la bonne application des procédures internes pour la prévention du blanchiment et du financement du terrorisme.

**149.** Le compte rendu analytique doit fournir une description des procédures établies dans l'établissement en vue de la prévention du blanchiment et du financement du terrorisme, telles que définies dans la loi modifiée du 12 novembre 2004, dans l'article 39 de la loi modifiée du 5 avril 1993 ainsi que dans la présente circulaire.

Le compte rendu analytique fournira en particulier les éléments suivants :

- une description de la politique d'acceptation des clients ;
- une appréciation de l'adéquation des procédures internes du professionnel du secteur financier propres à la prévention du blanchiment et du financement du terrorisme et leur conformité aux dispositions de la loi modifiée du 12 novembre 2004, de l'article 39 de la loi modifiée du 5 avril 1993 ainsi que de la présente circulaire, notamment en matière d'identification des clients et des bénéficiaires effectifs. Le réviseur d'entreprises se prononcera également sur la bonne application des procédures en question. Le résultat de ces contrôles est à présenter en outre en annexe dans le tableau synoptique de l'Institut des réviseurs d'entreprises (IRE) « Respect de la présente circulaire ». Ce tableau établi par l'IRE avec les appréciations « oui », « non » et « n/a » (non applicable) est à compléter, le cas échéant, par des indications chiffrées ou des explications complémentaires. Le réviseur peut également y faire référence à d'autres endroits du compte rendu analytique ;
- une déclaration sur la réalisation d'un contrôle régulier du respect des procédures par le service audit interne et le responsable de la fonction *compliance* ;
- les mesures de formation et d'information des employés en matière de détection des opérations de blanchiment et de financement du terrorisme ;
- un historique statistique des transactions suspectes détectées, le nombre des cas de déclarations de transactions suspectes faites par le professionnel du secteur financier au procureur d'Etat ainsi que le montant total des fonds engagés.

Le réviseur d'entreprises doit indiquer sa méthode de sélection de l'échantillon des dossiers contrôlés et le taux de couverture de la population (nombre de dossiers contrôlés / nombre total de clients ; volume des dépôts contrôlés / volume total des dépôts).

**150.** En cas de constat d'une non conformité avec les dispositions légales ou réglementaires ou de lacunes, le réviseur d'entreprises doit donner des indications précises permettant à la CSSF de juger la situation (nombre de dossiers non complets en suspens qui est à rapporter également au nombre total de dossiers contrôlés, détail des lacunes constatées, etc.).

Il est souligné que les réviseurs d'entreprises sont appelés à avertir également la CSSF de tous les cas de déclarations qu'ils font en vertu de l'article 9-1 de la loi modifiée du 28 juin 1984 portant organisation de la profession de réviseur d'entreprises et qui concernent un professionnel du secteur financier tombant sous la surveillance de la CSSF.

**151.** Les succursales luxembourgeoises d'établissements de crédit et d'entreprises d'investissement d'origine communautaire doivent, en application de la loi modifiée du 5 avril 1993, mandater un réviseur d'entreprises pour effectuer dans la succursale luxembourgeoise les vérifications en question en conformité avec les normes luxembourgeoises. Le rapport de contrôle émis par le réviseur d'entreprises sera adressé par la succursale à la CSSF.

### **Chapitre 3 L'auditeur interne et la personne chargée plus particulièrement de la lutte contre le blanchiment et le financement du terrorisme**

**152.** Le respect des obligations légales et réglementaires ainsi que des procédures relatives à la lutte contre le blanchiment et le financement du terrorisme doit faire l'objet d'une vérification à fréquence élevée par la personne chargée plus particulièrement de la lutte contre le blanchiment et le financement du terrorisme. Ces contrôles sont à coordonner avec les contrôles que le service d'audit interne est tenu d'effectuer dans ce domaine également. En outre, chaque professionnel du secteur financier est tenu de définir les programmes et modalités suivant lesquels les vérifications susdites doivent être faites.

## **Titre 4 Sanctions pénales et administratives en cas de non respect des obligations professionnelles**

**153.** Le non respect de toutes les obligations professionnelles, à part celles en matière de virements, est passible d'une amende pénale de 1.250 à 125.000 euros pour ceux qui y ont contrevenu sciemment. Il convient de noter que ces sanctions pénales s'appliquent même en l'absence d'une infraction de blanchiment ou de financement du terrorisme.

Les contraventions aux obligations professionnelles sont aussi passibles d'amendes d'ordre sur la base de l'article 63 de la loi modifiée du 5 avril 1993 relative au secteur financier.

Le non respect des dispositions du règlement communautaire 1781/2006 visé à l'article 39 de la loi modifiée relative au secteur financier est également sanctionné par les amendes d'ordre prévues à l'article 63 de la loi modifiée du 5 avril 1993 relative au secteur financier.

### **Partie III Dispositions abrogatoires**

**154.** La présente circulaire remplace la circulaire CSSF 05/211 datée du 13 octobre 2005.

Veillez recevoir, Mesdames, Messieurs, l'assurance de nos sentiments très distingués.

COMMISSION DE SURVEILLANCE DU SECTEUR FINANCIER

Simone DELCOURT  
Directeur

Jean-Nicolas SCHAUS  
Directeur Général

Annexes.

## ANNEXE I

**Règlement grand-ducal du 29 juillet 2008 portant établissement de la liste des «pays tiers imposant des obligations équivalentes» au sens de la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme (Mémorial A n° 119 du 11.08.2008 p 1811).**

[ ]

**Art. 1er.** La liste des «pays tiers imposant des obligations équivalentes» au sens de la loi modifiée du 12 novembre 2004 relative à la lutte contre le blanchiment et contre le financement du terrorisme est la suivante:

- Afrique du Sud,
- Argentine,
- Australie,
- Brésil,
- Canada,
- Etats-Unis,
- Guernesey,
- Hong Kong,
- Ile de Man,
- Japon,
- Jersey,
- Mexique,
- Nouvelle-Zélande,
- Fédération de Russie,
- Singapour,
- Suisse,
- Territoires d’outre-mer français: Mayotte, Nouvelle-Calédonie, Polynésie française, Saint-Pierre-et-Miquelon, Wallis-et-Futuna,
- Territoires d’outre-mer néerlandais: Antilles Néerlandaises, Aruba.

**Art. 2.** Notre Ministre du Trésor et du Budget est chargé de l’exécution du présent règlement qui sera publié au Mémorial.

[ ]

## **ANNEXE II**

### **Indices de blanchiment**

La liste ci-après, adaptée à partir d'une liste élaborée par la Commission fédérale des banques suisses, vise essentiellement à sensibiliser le personnel des banques et autres professionnels du secteur financier et n'a nullement la prétention d'être complète. Une liste exhaustive exigerait une adaptation constante aux nouvelles méthodes de blanchiment. Un seul indice ou une transaction douteuse ne constituent pas nécessairement, pris isolément, une raison suffisante pour soupçonner une opération de blanchiment.

Dans la pratique, il se peut que seule la combinaison de plusieurs indices ou transactions douteuses laisse supposer qu'on se trouve en présence d'une activité de blanchiment.

#### **I. Indices généraux**

Les transactions présentent des risques particuliers de blanchiment :

- lorsque leur construction indique un but illicite, lorsque leur but économique n'est pas reconnaissable, voire lorsqu'elles apparaissent absurdes d'un point de vue économique ;
- lorsque les valeurs patrimoniales sont retirées peu de temps après avoir été portées en compte (compte de passage), pour autant que l'activité du client ne rende pas plausible un tel retrait immédiat ;
- lorsque l'on ne parvient pas à comprendre les raisons pour lesquelles le client a choisi précisément cette banque ou ce comptoir pour ses affaires ;
- lorsqu'elles ont pour conséquence qu'un compte, resté jusque-là largement inactif, devient très actif sans que l'on puisse en percevoir une raison plausible ;
- lorsqu'elles ne sont pas compatibles avec les informations et les expériences de l'intermédiaire financier concernant le client ou le but de la relation d'affaires.

En outre, doit être considéré comme suspect tout client qui donne à l'intermédiaire financier des renseignements faux ou fallacieux ou qui, sans raison plausible, refuse de lui fournir les informations et les documents nécessaires, admis par les usages de l'activité concernée.

Peut constituer un motif de suspicion, le fait qu'un client reçoive régulièrement des virements en provenance d'une banque établie dans un des pays considéré comme non coopératif par le « Groupe d'Action Financière (GAFI) », ou qu'un client procède de manière répétée à des virements en direction d'un tel pays.

## **II. Indices particuliers**

### **1. Opérations de caisse**

- Echange d'un montant important de billets de banque (euros ou étrangers) en petites coupures contre des grosses coupures.
- Opérations de change d'importance, sans comptabilisation sur le compte d'un client.
- Encaissement de chèques, chèques de voyage y compris, pour des montants importants.
- Achat ou vente de grandes quantités de métaux précieux par des clients occasionnels.
- Achat de chèques bancaires pour de gros montants par des clients occasionnels.
- Ordres de virement à l'étranger donnés par des clients occasionnels, sans raison légitime apparente.
- Conclusion fréquente d'opérations de caisse jusqu'à concurrence de montants juste inférieurs à la limite au-dessus de laquelle l'identification du client est exigée.
- Acquisition de titres au porteur avec livraison physique.

### **2. Opérations en compte ou en dépôt**

- Retraits fréquents de gros montants en espèces, sans que l'activité du client ne justifie de telles opérations.
- Recours à des moyens de financement en usage dans le commerce international, alors que l'emploi de tels instruments est en contradiction avec l'activité connue du client.
- Comptes utilisés de manière intensive pour des paiements, alors que lesdits comptes ne reçoivent pas ou reçoivent peu de paiements habituellement.
- Structure économiquement absurde des relations d'affaires entre un client et la banque (grand nombre de comptes auprès du même établissement, transferts fréquents entre différents comptes, liquidités excessives, etc.).
- Fourniture de garanties (gages, cautions, etc.) par des tiers inconnus de la banque qui ne paraissent pas être en relation étroite avec le client ni avoir de raison plausible de donner de telles garanties.
- Virements vers une autre banque sans indication du bénéficiaire.

- Acceptation de transferts de fonds d'autres banques sans indication du nom ou du numéro de compte du bénéficiaire ou du donneur d'ordre.
- Virements répétés de gros montants à l'étranger avec instruction de payer le bénéficiaire en espèces.
- Virements importants et répétés en direction ou en provenance de pays producteurs de drogue.
- Fourniture de cautions ou de garanties bancaires à titre de sûreté pour des emprunts entre tiers, non conformes au marché.
- Versements en espèces par un grand nombre de personnes différentes sur un seul et même compte.
- Remboursement inattendu et sans explications convaincantes d'un crédit compromis.
- Utilisation de comptes pseudonymes ou numériques dans l'exécution de transactions commerciales par des entreprises artisanales, commerciales ou industrielles.
- Retrait de valeurs patrimoniales peu de temps après que celles-ci ont été portées en compte (compte de passage).

### 3. Opérations fiduciaires

- Crédits fiduciaires (*back-to-back loans*) sans but licite reconnaissable.
- Détention fiduciaire de participations dans des sociétés non cotées en bourse, et dont la banque ne peut déterminer l'activité.

### 4. Autres

- Tentatives du client visant à éviter le contact personnel avec le professionnel du secteur financier

## **III. Indices qualifiés**

- Souhait du client de clôturer un compte et d'ouvrir de nouveaux comptes en son nom ou au nom de certains membres de sa famille sans traces dans la documentation de la banque (« *paper trail* »).
- Souhait du client d'obtenir quittance pour des retraits au comptant ou des livraisons de titres qui n'ont pas été réellement effectués ou qui ont été immédiatement redéposés dans le même établissement.
- Souhait du client d'effectuer des ordres de paiement avec indication d'un donneur d'ordre inexact.

- Souhait du client que certains versements soient effectués non pas directement depuis son propre compte, mais par le biais d'un compte Nostro du professionnel du secteur financier ou d'un compte « Divers ».
- Souhait du client d'accepter ou de faire documenter des garanties ne correspondant pas à la réalité économique ou d'octroyer des crédits à titre fiduciaire sur la base d'une couverture fictive.
- Poursuites pénales dirigées contre un client du professionnel du secteur financier pour crime, corruption ou détournement de fonds publics.

## **Annexe III**

### **Circulaires relatives à**

- l'identification et à la déclaration des relations d'affaires avec les milieux terroristes suivant les règlements CE du Conseil instituant certaines mesures restrictives spécifiques à l'encontre de certaines personnes et entités liées à Oussama ben Laden, au réseau Al-Qaïda et aux Taliban d'Afghanistan ;
- la lutte contre le terrorisme.

Une liste actualisée de ces circulaires se trouve sur le site internet de la CSSF ([www.cssf.lu](http://www.cssf.lu)).

Site internet utile en matière de listes de terroristes :

[http://ec.europa.eu/external\\_relations/cfsp/sanctions/index.htm](http://ec.europa.eu/external_relations/cfsp/sanctions/index.htm)

## **ANNEXE IV**

**Règlement (CE) N° 1781/2006 du Parlement européen et du Conseil du 15 novembre 2006 relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds**

## I

(Actes dont la publication est une condition de leur applicabilité)

**RÈGLEMENT (CE) N° 1781/2006 DU PARLEMENT EUROPÉEN ET DU CONSEIL**  
**du 15 novembre 2006**  
**relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds**  
**(Texte présentant de l'intérêt pour l'EEE)**

LE PARLEMENT EUROPÉEN ET LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité instituant la Communauté européenne, et notamment son article 95,

vu la proposition de la Commission,

vu l'avis de la Banque centrale européenne <sup>(1)</sup>,

statuant conformément à la procédure visée à l'article 251 du traité <sup>(2)</sup>,

considérant ce qui suit:

- (1) Les flux d'argent sale par la voie de virements de fonds peuvent mettre à mal la stabilité et la réputation du secteur financier et menacer ainsi le marché intérieur. Le terrorisme remet en cause les fondements mêmes de notre société. La bonne santé, l'intégrité et la stabilité du système des virements de fonds et la confiance dans l'ensemble du système financier pourraient être gravement compromises par les efforts mis en œuvre par les criminels et leurs complices pour masquer l'origine de leurs profits ou pour virer des fonds à des fins terroristes.
- (2) Pour favoriser leurs activités criminelles, les blanchisseurs et ceux qui financent le terrorisme pourraient essayer de tirer profit de la libre circulation des capitaux qu'implique une zone financière intégrée, à moins que certaines mesures de coordination ne soient arrêtées au niveau communautaire. Par sa portée, une intervention de la Communauté devrait garantir la transposition uniforme, dans l'ensemble de l'Union européenne, de la recommandation spéciale VII sur les virements électroniques (RS VII) du Groupe d'action financière internationale (GAFI), institué à Paris lors du sommet du G7 de 1989, et, en particulier, qu'il n'y ait aucune discrimination entre les paiements nationaux dans un État membre et les paiements transfrontaliers entre États membres. Des mesures adoptées au seul niveau des États membres, sans coordination, dans le

domaine des virements de fonds transfrontaliers, pourraient avoir des répercussions importantes sur le bon fonctionnement des systèmes de paiement au niveau de l'Union européenne et, partant, porter atteinte au marché intérieur dans le domaine des services financiers.

- (3) Au lendemain des attentats terroristes du 11 septembre 2001 aux États-Unis, le Conseil européen extraordinaire du 21 septembre 2001 a réaffirmé que la lutte contre le terrorisme était un objectif prioritaire de l'Union européenne. Le Conseil européen a approuvé un plan d'action visant au renforcement de la coopération policière et judiciaire, au développement des instruments juridiques internationaux de lutte contre le terrorisme, à la prévention du financement des activités terroristes, à l'amélioration de la sécurité aérienne et au renforcement de la cohérence entre toutes les politiques en la matière. Ce plan d'action a été révisé par le Conseil européen à la suite des attentats terroristes du 11 mars 2004 à Madrid et il prévoit maintenant expressément la nécessité de veiller à ce que le cadre législatif créé par la Communauté pour combattre le terrorisme et améliorer la coopération judiciaire soit adapté en fonction des neuf recommandations spéciales sur le financement du terrorisme adoptées par le GAFI.
- (4) Afin de prévenir le financement du terrorisme, des mesures visant à geler les fonds et les ressources économiques de certaines personnes, de certains groupes et entités ont été prises, notamment les règlements (CE) n° 2580/2001 du Conseil <sup>(3)</sup> et (CE) n° 881/2002 du Conseil <sup>(4)</sup>. Aux mêmes fins, des mesures visant à protéger le système financier contre la transmission de fonds et de ressources financières à des activités terroristes ont été prises. La directive 2005/60/CE du Parlement européen et du Conseil <sup>(5)</sup> contient un certain nombre de mesures visant à combattre l'exploitation du système financier à des fins de blanchiment de capitaux et de financement du terrorisme. Ces mesures ne sont cependant pas suffisantes pour empêcher les terroristes et autres criminels d'avoir accès aux systèmes de paiement et de les utiliser pour déplacer des fonds.

<sup>(1)</sup> JO C 336 du 31.12.2005, p. 109.

<sup>(2)</sup> Avis du Parlement européen rendu le 6 juillet 2006 (non encore paru au Journal officiel) et décision du Conseil rendue le 7 novembre 2006.

<sup>(3)</sup> JO L 344 du 28.12.2001, p. 70. Règlement modifié en dernier lieu par le règlement (CE) n° 1461/2006 de la Commission (JO L 272 du 3.10.2006, p. 11).

<sup>(4)</sup> JO L 139 du 29.5.2002, p. 9. Règlement modifié en dernier lieu par le règlement (CE) n° 1508/2006 de la Commission (JO L 280 du 12.10.2006, p. 12).

<sup>(5)</sup> JO L 309 du 25.11.2005, p. 15.

- (5) Pour favoriser une approche cohérente au niveau international de la lutte contre le blanchiment de capitaux et le financement du terrorisme, toute nouvelle initiative communautaire devrait tenir compte des développements à ce niveau, à savoir des neuf recommandations spéciales en matière de lutte contre le financement du terrorisme adoptées par le GAFI, et notamment la RS VII et la note interprétative révisée pour sa mise en œuvre.
- (6) La traçabilité complète des virements de fonds peut être un instrument particulièrement précieux et utile en matière de prévention, d'enquête et de détection des activités de blanchiment de capitaux ou de financement du terrorisme. Il convient donc, afin d'assurer une bonne transmission des renseignements sur le donneur d'ordre tout au long de la chaîne des paiements, de prévoir un système qui impose aux prestataires de services de paiement l'obligation de veiller à ce que les virements de fonds soient accompagnés d'informations exactes et utiles sur le donneur d'ordre.
- (7) Le présent règlement est applicable sans préjudice de la directive 95/46/CE du Parlement européen et du Conseil <sup>(1)</sup>. Par exemple, les informations collectées et conservées aux fins du présent règlement ne devraient pas être utilisées à des fins commerciales.
- (8) Les personnes dont l'activité se limite à convertir des documents sous format papier en données électroniques et qui agissent en vertu d'un contrat conclu avec un prestataire de services de paiement ne relèvent pas du champ d'application du présent règlement; il en va de même de toute personne physique ou morale qui ne fait que fournir à des prestataires de services de paiement un système de messagerie ou d'autres systèmes de support pour la transmission de fonds ou des systèmes de compensation et de règlement.
- (9) Il convient d'exclure du champ d'application du présent règlement les virements de fonds qui représentent un faible risque de blanchiment de capitaux ou de financement du terrorisme. Ces exclusions devraient concerner les cartes de crédit ou de débit, les retraits dans les distributeurs automatiques de billets, les prélèvements automatiques, les chèques sous forme d'images-chèques, le paiement de taxes, d'amendes ou d'autres impôts et les virements de fonds pour lesquels le donneur d'ordre et le bénéficiaire sont tous deux des prestataires de services de paiement agissant pour leur compte. En outre, pour tenir compte des caractéristiques particulières des systèmes de paiement nationaux, les États membres devraient pouvoir exempter les virements électroniques postaux, à condition qu'il soit toujours possible de remonter du virement de fonds jusqu'au donneur d'ordre. Dans les cas où les États membres ont appliqué la dérogation relative à la monnaie électronique prévue par la directive 2005/60/CE, elle devrait s'appliquer dans le cadre du présent règlement, à condition que le montant de la transaction n'excède pas 1 000 EUR.
- (10) La dérogation relative à la monnaie électronique, au sens de la directive 2000/46/CE du Parlement européen et du Conseil <sup>(2)</sup>, s'applique à la monnaie électronique, que l'émetteur de cette monnaie bénéficie ou non d'une exemption au titre de l'article 8 de ladite directive.
- (11) Afin de ne pas nuire à l'efficacité des systèmes de paiement, il convient de distinguer le niveau des exigences de vérification entre les virements de fonds effectués à partir d'un compte et les virements de fonds non effectués à partir d'un compte. Pour trouver un équilibre entre, d'une part, le risque de refouler des transactions dans la clandestinité en appliquant des exigences d'identification trop strictes et, d'autre part, la menace terroriste potentielle que posent les petits virements de fonds, dans le cas de virements de fonds non effectués à partir d'un compte, l'obligation de vérifier l'exactitude des informations sur le donneur d'ordre ne devrait s'appliquer qu'aux virements de fonds individuels d'un montant supérieur à 1 000 EUR, sans préjudice des obligations prévues par la directive 2005/60/CE. Pour les virements de fonds effectués à partir d'un compte, les prestataires de services de paiement ne sont pas tenus de vérifier les informations concernant le donneur d'ordre à l'occasion de chaque virement de fonds, lorsqu'il a été satisfait aux obligations prévues par la directive 2005/60/CE.
- (12) Compte tenu du règlement (CE) n° 2560/2001 du Parlement européen et du Conseil <sup>(3)</sup> et de la communication de la Commission intitulée «Un cadre juridique pour les paiements dans le marché intérieur», il suffit de prévoir que les virements de fonds au sein de la Communauté doivent être accompagnés d'informations simplifiées concernant le donneur d'ordre.
- (13) Afin de permettre aux autorités de pays tiers compétentes en matière de lutte contre le blanchiment de capitaux ou le financement du terrorisme de remonter à la source des fonds utilisés à ces fins, les virements de fonds effectués depuis la Communauté en dehors de la Communauté devraient être accompagnés d'informations complètes sur le donneur d'ordre. L'accès de ces autorités aux informations complètes sur le donneur d'ordre ne devrait être autorisé qu'aux fins de prévention, d'investigation et de détection du blanchiment de capitaux ou du financement du terrorisme.
- (14) Afin que les virements de fonds d'un donneur d'ordre unique en faveur de plusieurs bénéficiaires puissent être envoyés d'une manière peu coûteuse sous forme de lots de virements individuels de la Communauté en dehors de la Communauté, ces virements devraient pouvoir être accompagnés uniquement du numéro de compte du donneur d'ordre ou d'un identifiant unique, à condition que le lot contienne des informations complètes sur le donneur d'ordre.
- (15) Afin de vérifier si les informations requises sur le donneur d'ordre accompagnent effectivement les virements de fonds et de faciliter la détection d'opérations suspectes, le prestataire de services de paiement du bénéficiaire devrait disposer de procédures internes efficaces pour détecter les informations manquantes sur le donneur d'ordre.

<sup>(1)</sup> JO L 281 du 23.11.1995, p. 31. Directive modifiée par le règlement (CE) n° 1882/2003 (JO L 284 du 31.10.2003, p. 1).

<sup>(2)</sup> JO L 275 du 27.10.2000, p. 39.

<sup>(3)</sup> JO L 344 du 28.12.2001, p. 13.

- (16) En raison de la menace potentielle de financement du terrorisme que posent les virements anonymes, il convient de permettre au prestataire de services de paiement du bénéficiaire d'éviter ou de corriger de telles situations lorsqu'il constate que les informations sur le donneur d'ordre sont manquantes ou incomplètes. À cet égard, une certaine souplesse devrait être autorisée, en fonction du risque, en ce qui concerne l'étendue des informations à fournir sur le donneur d'ordre. En outre, le prestataire de services de paiement du donneur d'ordre devrait rester responsable de la fourniture d'informations exactes et complètes. Lorsque le prestataire de services de paiement du donneur d'ordre se situe en dehors du territoire de la Communauté, des obligations de vigilance renforcées à l'égard de la clientèle devraient s'appliquer, conformément à la directive 2005/60/CE, vis-à-vis des relations transfrontalières du correspondant bancaire avec ce prestataire de services de paiement.
- (17) Lorsque les autorités nationales compétentes donnent des orientations concernant l'obligation soit de rejeter tous les virements provenant d'un prestataire de services de paiement qui omet régulièrement de fournir les informations requises sur le donneur d'ordre, soit de décider s'il y a lieu, ou non, de restreindre la relation commerciale avec le prestataire de services de paiement ou d'y mettre fin, ces orientations devraient être fondées, entre autres, sur la convergence des meilleures pratiques et, en outre, prendre en compte le fait que la note interprétative révisée du GAFI sur la RS VII permet aux pays tiers de fixer un seuil de 1 000 EUR ou de 1 000 USD pour l'obligation de transmettre des informations sur le donneur d'ordre, et cela sans préjudice de l'objectif d'une lutte efficace contre le blanchiment de capitaux et le financement du terrorisme.
- (18) De toute façon, le prestataire de services de paiement du bénéficiaire devrait faire preuve d'une vigilance particulière, en fonction du risque, lorsqu'il constate que les informations sur le donneur d'ordre sont manquantes ou incomplètes, et devrait déclarer les opérations suspectes aux autorités compétentes conformément aux obligations de déclaration énoncées par la directive 2005/60/CE ainsi qu'aux mesures d'exécution nationales.
- (19) Les dispositions relatives aux virements de fonds pour lesquels les informations sur le donneur d'ordre sont manquantes ou incomplètes s'appliquent sans préjudice de toute obligation imposant aux prestataires de services de paiement de suspendre et/ou de rejeter les virements de fonds qui sont contraires aux dispositions de droit civil, administratif ou pénal.
- (20) Jusqu'à ce que les limites techniques qui peuvent empêcher un prestataire de services de paiement intermédiaire de satisfaire à l'obligation de transmettre toutes les informations reçues sur le donneur d'ordre aient disparu, ces prestataires devraient conserver ces informations. De telles limites techniques devraient disparaître dès que les systèmes de paiement seront améliorés.
- (21) Étant donné que dans les enquêtes criminelles il se peut que les informations requises ou les personnes impliquées ne soient identifiées que de nombreux mois, voire des années, après l'exécution du virement de fonds d'origine, les prestataires de services de paiement devraient conserver les informations sur le donneur d'ordre aux fins de la prévention, de l'investigation et de la détection des activités de blanchiment de capitaux ou de financement du terrorisme. Cette durée de conservation devrait être limitée.
- (22) Pour garantir la célérité de l'action dans le cadre de la lutte antiterroriste, les prestataires de services de paiement devraient répondre rapidement aux demandes d'informations concernant le donneur d'ordre que leur adressent les autorités compétentes en matière de lutte contre le blanchiment de capitaux ou le financement du terrorisme dans les États membres où ils sont situés.
- (23) Le nombre de jours ouvrables dans l'État membre du prestataire de services de paiement du donneur d'ordre détermine le nombre de jours pour répondre aux demandes d'informations concernant le donneur d'ordre.
- (24) Étant donné l'importance de la lutte contre le blanchiment de capitaux et le financement du terrorisme, les États membres devraient mettre en place, dans leur législation nationale, des sanctions effectives, proportionnées et dissuasives, applicables en cas de non-respect du présent règlement.
- (25) Il y a lieu d'arrêter les mesures nécessaires pour la mise en œuvre du présent règlement en conformité avec la décision 1999/468/CE du Conseil du 28 juin 1999 fixant les modalités de l'exercice des compétences d'exécution conférées à la Commission <sup>(1)</sup>.
- (26) Un certain nombre de pays et de territoires qui ne font pas partie du territoire de la Communauté partagent une union monétaire avec un État membre, font partie de la zone monétaire d'un État membre ou ont signé une convention monétaire avec la Communauté européenne représentée par un État membre, et ont des prestataires de services de paiement qui participent directement ou indirectement aux systèmes de paiement et de règlement de cet État membre. Afin d'éviter que l'application du présent règlement aux virements de fonds entre les États membres concernés et ces pays ou territoires ne produise un effet négatif significatif sur l'économie de ces pays ou territoires, il convient de prévoir que ces virements de fonds peuvent être traités comme des virements de fonds à l'intérieur des États membres concernés.

<sup>(1)</sup> JO L 184 du 17.7.1999, p. 23. Décision modifiée en dernier lieu par la décision 2006/512/CE (JO L 200 du 22.7.2006, p. 11).

- (27) Afin de ne pas décourager les donations à des fins charitables, les États membres devraient pouvoir exempter les prestataires de services de paiement situés sur leur territoire de l'obligation de collecter, de vérifier, d'enregistrer ou d'envoyer des informations sur le donneur d'ordre pour les virements de fonds à concurrence de 150 EUR effectués sur le territoire de cet État membre. Il convient également que cette option ne puisse être accordée que lorsque l'organisation à but non lucratif remplit certaines conditions, afin de permettre aux États membres de veiller à ce que les terroristes n'abusent pas de cette exemption pour couvrir ou faciliter le financement de leurs activités.
- (28) Étant donné que les objectifs du présent règlement ne peuvent pas être réalisés de manière suffisante par les États membres et peuvent donc, en raison des dimensions ou des effets du présent règlement, être mieux réalisés au niveau communautaire, la Communauté peut adopter des mesures conformément au principe de subsidiarité consacré à l'article 5 du traité. Conformément au principe de proportionnalité tel qu'énoncé audit article, le présent règlement n'excède pas ce qui est nécessaire pour atteindre ces objectifs.
- (29) Afin d'établir une approche cohérente dans le domaine dans la lutte contre le blanchiment de capitaux et le financement du terrorisme, les principales dispositions du présent règlement devraient s'appliquer à partir de la même date que les dispositions en la matière adoptées au niveau international,
- 3) «donneur d'ordre», soit la personne physique ou morale qui est le titulaire d'un compte et qui autorise un virement de fonds à partir dudit compte, soit, en l'absence de compte, la personne physique ou morale qui donne l'ordre d'effectuer un virement de fonds;
- 4) «bénéficiaire», la personne physique ou morale qui est le destinataire final prévu des fonds virés;
- 5) «prestataire de services de paiement», la personne physique ou morale dont l'activité professionnelle comprend la fourniture de services de virements de fonds;
- 6) «prestataire de services de paiement intermédiaire», un prestataire de services de paiement qui n'est ni celui du donneur d'ordre ni celui du bénéficiaire et qui participe à l'exécution du virement de fonds;
- 7) «virement de fonds», toute opération effectuée par voie électronique pour le compte d'un donneur d'ordre par l'intermédiaire d'un prestataire de services de paiement en vue de mettre des fonds à la disposition d'un bénéficiaire auprès d'un prestataire de services de paiement, le donneur d'ordre et le bénéficiaire pouvant être ou non la même personne;
- 8) «virement par lots», plusieurs virements de fonds individuels qui sont groupés en vue de leur transmission;
- 9) «identifiant unique», une combinaison de lettres, de numéros ou de symboles déterminée par le prestataire de services de paiement conformément aux protocoles du système de paiement et de règlement ou du système de messagerie utilisé pour effectuer le virement de fonds.

ONT ARRÊTÉ LE PRÉSENT RÈGLEMENT:

#### CHAPITRE I

### OBJET, DÉFINITIONS ET CHAMP D'APPLICATION

#### Article premier

##### Objet

Le présent règlement établit les règles relatives aux informations sur le donneur d'ordre qui doivent accompagner les virements de fonds, aux fins de la prévention, de l'enquête et de la détection des activités de blanchiment de capitaux et de financement du terrorisme.

#### Article 2

##### Définitions

Aux fins du présent règlement, on entend par:

- 1) «financement du terrorisme», le fait de fournir ou de réunir des fonds au sens de l'article 1<sup>er</sup>, paragraphe 4, de la directive 2005/60/CE;
- 2) «blanchiment de capitaux», tout agissement qui, lorsqu'il est commis intentionnellement, est considéré comme blanchiment de capitaux au sens de l'article 1<sup>er</sup>, paragraphes 2 ou 3, de la directive 2005/60/CE;

#### Article 3

##### Champ d'application

1. Le présent règlement est applicable aux virements de fonds, en toutes monnaies, qui sont envoyés ou reçus par un prestataire de services de paiement établi dans la Communauté.
2. Le présent règlement n'est pas applicable aux virements de fonds effectués à l'aide d'une carte de crédit ou de débit, à condition:
- a) que le bénéficiaire ait passé un accord avec le prestataire de services de paiement permettant le paiement de la fourniture de biens et de services;
- et
- b) qu'un identifiant unique, permettant de remonter jusqu'au donneur d'ordre, accompagne ces virements de fonds.

3. Lorsqu'un État membre choisit d'appliquer la dérogation prévue à l'article 11, paragraphe 5, point d), de la directive 2005/60/CE, le présent règlement ne s'applique pas aux virements de fonds effectués au moyen de monnaie électronique couverts par cette dérogation, sauf lorsque le montant de la transaction est supérieur à 1 000 EUR.

4. Sans préjudice du paragraphe 3, le présent règlement ne s'applique pas aux virements de fonds exécutés au moyen d'un téléphone portable ou d'un autre dispositif numérique ou lié aux technologies de l'information (TI), lorsque de tels virements sont effectués à partir d'un prépaiement et n'excèdent pas 150 EUR.

5. Le présent règlement ne s'applique pas aux virements de fonds exécutés au moyen d'un téléphone portable ou d'un autre dispositif numérique ou lié aux TI, lorsque de tels virements sont postpayés et satisfont à toutes les conditions suivantes:

- a) le bénéficiaire a passé un accord avec le prestataire de services de paiement permettant le paiement de la fourniture de biens et de services;
- b) un identifiant unique, permettant de remonter jusqu'au donneur d'ordre, accompagne le virement de fonds;

et

- c) le prestataire de services de paiement est soumis aux obligations énoncées par la directive 2005/60/CE.

6. Les États membres peuvent décider de ne pas appliquer le présent règlement aux virements de fonds effectués, sur leur territoire, sur le compte d'un bénéficiaire permettant le paiement de la fourniture de biens ou de services si:

- a) le prestataire de services de paiement du bénéficiaire est soumis aux obligations énoncées par la directive 2005/60/CE;

- b) le prestataire de services de paiement du bénéficiaire peut, grâce à un numéro de référence unique, remonter, par l'intermédiaire du bénéficiaire, jusqu'à la personne physique ou morale qui a effectué le virement de fonds dans le cadre d'un accord conclu avec le bénéficiaire aux fins de la fourniture de biens ou de services;

et

- c) le montant de la transaction est inférieur ou égal à 1 000 EUR.

Les États membres faisant usage de cette dérogation en informent la Commission.

7. Le présent règlement n'est pas applicable aux virements de fonds:

- a) pour lesquels le donneur d'ordre retire des espèces de son propre compte;

- b) pour lesquels il existe une autorisation de prélèvement automatique entre les deux parties permettant que des paiements soient effectués entre eux à l'aide de comptes à condition qu'un identifiant unique accompagne le virement de fonds pour permettre de remonter à la personne physique ou morale;

- c) effectués au moyen de chèques sous forme d'images-chèques;

- d) pour le paiement de taxes, d'amendes ou autres impôts aux autorités publiques, au sein d'un État membre;

- e) pour lesquels le donneur d'ordre et le bénéficiaire sont tous deux des prestataires de services de paiement opérant pour leur propre compte.

## CHAPITRE II

### OBLIGATIONS DU PRESTATAIRE DE SERVICES DE PAIEMENT DU DONNEUR D'ORDRE

#### Article 4

#### Informations complètes sur le donneur d'ordre

1. Les informations complètes sur le donneur d'ordre consistent en son nom, son adresse et son numéro de compte.

2. L'adresse du donneur d'ordre peut être remplacée par sa date et son lieu de naissance, son numéro d'identification de client ou son numéro national d'identité.

3. En l'absence de numéro de compte du donneur d'ordre, le prestataire de services de paiement du donneur d'ordre le remplace par un identifiant unique permettant de remonter jusqu'au donneur d'ordre.

#### Article 5

#### Informations accompagnant les virements de fonds et conservation des données

1. Les prestataires de services de paiement veillent à ce que les virements de fonds soient accompagnés des informations complètes sur le donneur d'ordre.

2. Avant de virer les fonds, le prestataire de services de paiement du donneur d'ordre vérifie les informations complètes sur le donneur d'ordre sur la base de documents, de données ou de renseignements obtenus auprès d'une source fiable et indépendante.

3. Dans le cas de virements de fonds effectués à partir d'un compte, la vérification peut être considérée comme ayant eu lieu:

- a) si l'identité d'un donneur d'ordre a été vérifiée lors de l'ouverture du compte et si les informations obtenues à cette occasion ont été conservées conformément aux obligations prévues à l'article 8, paragraphe 2, et à l'article 30, point a), de la directive 2005/60/CE;

ou

- b) si le donneur d'ordre relève de l'article 9, paragraphe 6, de la directive 2005/60/CE.

4. Toutefois, sans préjudice de l'article 7, point c), de la directive 2005/60/CE, dans le cas de virements de fonds qui ne sont pas effectués à partir d'un compte, le prestataire de services de paiement du donneur d'ordre ne vérifie les informations concernant le donneur d'ordre que si le montant est supérieur à 1 000 EUR, à moins que la transaction ne soit effectuée en plusieurs opérations qui semblent être liées et excèdent conjointement 1 000 EUR.

5. Le prestataire de services de paiement du donneur d'ordre conserve pendant cinq ans les informations complètes sur le donneur d'ordre qui accompagnent les virements de fonds.

#### Article 6

##### Virements de fonds au sein de la Communauté

1. Par dérogation à l'article 5, paragraphe 1, les virements de fonds pour lesquels le prestataire de services de paiement du donneur d'ordre et le prestataire de services de paiement du bénéficiaire sont tous deux situés dans la Communauté doivent seulement être accompagnés du numéro de compte du donneur d'ordre ou d'un identifiant unique permettant de remonter jusqu'au donneur d'ordre.

2. Toutefois, à la demande du prestataire de services de paiement du bénéficiaire, le prestataire de services de paiement du donneur d'ordre met à la disposition du prestataire de services de paiement du bénéficiaire les informations complètes sur le donneur d'ordre, dans les trois jours ouvrables suivant la réception de cette demande.

#### Article 7

##### Virements de fonds effectués de l'intérieur vers l'extérieur de la Communauté

1. Les virements de fonds destinés à un bénéficiaire dont le prestataire de services de paiement est situé en dehors de la Communauté sont accompagnés d'informations complètes sur le donneur d'ordre.

2. En cas de virements par lots effectués par un donneur d'ordre unique en faveur de bénéficiaires dont les prestataires de services de paiement sont situés hors de la Communauté, le paragraphe 1 n'est pas applicable aux virements individuels groupés dans ces lots, à condition que le fichier des lots contienne les informations complètes sur le donneur d'ordre et que les virements individuels portent le numéro de compte du donneur d'ordre ou un identifiant unique.

#### CHAPITRE III

##### OBLIGATIONS DU PRESTATAIRE DE SERVICES DE PAIEMENT DU BÉNÉFICIAIRE

#### Article 8

##### Détection d'informations manquantes sur le donneur d'ordre

Le prestataire de services de paiement du bénéficiaire est tenu de détecter que les champs relatifs aux informations concernant le

donneur d'ordre prévus dans le système de messagerie ou de paiement et de règlement utilisé pour effectuer un virement de fonds ont été complétés à l'aide de caractères ou d'éléments compatibles avec ce système de messagerie ou de paiement et de règlement. Ce prestataire doit disposer de procédures efficaces pour détecter si les informations suivantes sur le donneur d'ordre sont manquantes:

a) dans le cas des virements de fonds pour lesquels le prestataire de services de paiement du donneur d'ordre est situé dans la Communauté, les informations requises en vertu de l'article 6;

b) dans le cas des virements de fonds pour lesquels le prestataire de services de paiement du donneur d'ordre est situé en dehors de la Communauté, les informations complètes sur le donneur d'ordre visées à l'article 4 ou, le cas échéant, les informations requises en vertu de l'article 13;

et

c) dans le cas de virements par lots pour lesquels le prestataire de services de paiement du donneur d'ordre est situé en dehors de la Communauté, les informations complètes sur le donneur d'ordre visées à l'article 4 seulement dans le virement par lots, mais non dans les virements individuels regroupés dans les lots.

#### Article 9

##### Virements de fonds pour lesquels les informations sur le donneur d'ordre sont manquantes ou incomplètes

1. Lorsque le prestataire de services de paiement du bénéficiaire constate, au moment de la réception du virement de fonds, que les informations sur le donneur d'ordre requises par le présent règlement sont manquantes ou incomplètes, il rejette le virement ou demande des informations complètes sur le donneur d'ordre. Dans tous les cas, le prestataire de services de paiement du bénéficiaire se conforme à toute disposition légale ou administrative relative au blanchiment de capitaux et au financement du terrorisme, notamment aux règlements (CE) n° 2580/2001 et (CE) n° 881/2002 et à la directive 2005/60/CE, ainsi qu'à toute mesure d'exécution nationale.

2. Lorsqu'un prestataire de services de paiement omet régulièrement de fournir les informations requises sur le donneur d'ordre, le prestataire de services de paiement du bénéficiaire prend des dispositions qui peuvent, dans un premier temps, comporter l'émission d'avertissements et la fixation d'échéances, avant soit de rejeter tout nouveau virement de fonds provenant de ce prestataire de services de paiement, soit de décider, s'il y a lieu ou non, de restreindre sa relation commerciale avec ce prestataire de services de paiement ou d'y mettre fin.

Le prestataire de services de paiement du bénéficiaire déclare ce fait aux autorités responsables de la lutte contre le blanchiment de capitaux ou le financement du terrorisme.

*Article 10***Évaluation des risques**

Le prestataire de services de paiement du bénéficiaire considère les informations manquantes ou incomplètes sur le donneur d'ordre comme un facteur à prendre en compte dans l'appréciation du caractère éventuellement suspect du virement de fonds ou de toutes les opérations liées à ce virement et, le cas échéant, de la nécessité de le déclarer, conformément aux obligations prévues au chapitre III de la directive 2005/60/CE, aux autorités responsables de la lutte contre le blanchiment de capitaux ou le financement du terrorisme.

*Article 11***Conservation des données**

Le prestataire de services de paiement du bénéficiaire conserve pendant cinq ans toutes les informations qu'il a reçues sur le donneur d'ordre.

## CHAPITRE IV

**OBLIGATIONS DES PRESTATAIRES DE SERVICES DE PAIEMENT INTERMÉDIAIRES***Article 12***Conservation des informations sur le donneur d'ordre avec le virement**

Les prestataires de services de paiement intermédiaires veillent à ce que toutes les informations reçues sur le donneur d'ordre qui accompagnent un virement de fonds soient conservées avec ce virement.

*Article 13***Limites techniques**

1. Le présent article s'applique dans les cas où le prestataire de services de paiement du donneur d'ordre est situé hors de la Communauté et le prestataire de services de paiement intermédiaire est situé dans la Communauté.

2. À moins que le prestataire de services de paiement intermédiaire ne constate, au moment de la réception du virement de fonds, que les informations requises sur le donneur d'ordre en vertu du présent règlement sont manquantes ou incomplètes, il peut utiliser, pour transmettre les virements de fonds au prestataire de services de paiement du bénéficiaire, un système de paiement avec des limites techniques qui empêche les informations sur le donneur d'ordre d'accompagner le virement de fonds.

3. Lorsque le prestataire de services de paiement intermédiaire constate, au moment de la réception du virement de fonds, que les informations sur le donneur d'ordre requises en vertu du présent règlement sont manquantes ou incomplètes, il n'utilise un système de paiement avec des limites techniques que s'il peut informer le prestataire de services de paiement du bénéficiaire de ce fait, soit dans le cadre d'un système de messagerie ou de paiement qui prévoit la communication de ce fait, soit par une autre

procédure, à condition que le mode de communication soit accepté ou convenu entre les deux prestataires de services de paiement.

4. Lorsqu'il utilise un système de paiement avec des limites techniques, le prestataire de services de paiement intermédiaire met à la disposition du prestataire de services de paiement du bénéficiaire, sur demande de ce dernier et dans les trois jours ouvrables suivant la réception de la demande, toutes les informations qu'il a reçues sur le donneur d'ordre, qu'elles soient complètes ou non.

5. Dans les cas visés aux paragraphes 2 et 3, le prestataire de services de paiement intermédiaire conserve pendant cinq ans toutes les informations reçues.

## CHAPITRE V

**OBLIGATIONS GÉNÉRALES ET COMPÉTENCES EN MATIÈRE D'EXÉCUTION***Article 14***Obligations de coopération**

Tout prestataire de services de paiement donne suite, de manière exhaustive et sans délai, dans le respect des procédures prévues par le droit national de l'État membre dans lequel il est situé, aux demandes qui lui sont adressées par les autorités compétentes en matière de lutte contre le blanchiment de capitaux ou le financement du terrorisme de cet État membre et qui portent sur les informations relatives au donneur d'ordre accompagnant les virements de fonds et les informations conservées correspondantes.

Sans préjudice du droit pénal national et de la protection des droits fondamentaux, ces autorités ne peuvent exploiter ces informations qu'à des fins de prévention, d'investigation ou de détection des activités de blanchiment de capitaux ou de financement du terrorisme.

*Article 15***Sanctions et suivi**

1. Les États membres déterminent le régime des sanctions applicables en cas de non-respect des dispositions du présent règlement et prennent toutes les mesures nécessaires pour assurer leur mise en œuvre. Les sanctions doivent être effectives, proportionnées et dissuasives. Les sanctions sont applicables à partir du 15 décembre 2007.

2. Les États membres notifient le régime visé au paragraphe 1 à la Commission, au plus tard le 14 décembre 2007, dont ils informent les autorités chargées de son application, et ils lui signalent sans délai toute modification ultérieure y relative.

3. Les États membres ont obligation aux autorités compétentes d'exercer un contrôle effectif et de prendre les mesures nécessaires pour garantir le respect des dispositions du présent règlement.

*Article 16***Procédure de comité**

1. La Commission est assistée du comité sur la prévention du blanchiment de capitaux et du financement du terrorisme institué par la directive 2005/60/CE, ci-après dénommé «le comité».

2. Dans le cas où il est fait référence au présent paragraphe, les articles 5 et 7 de la décision 1999/468/CE s'appliquent, dans le respect des dispositions de l'article 8 de celle-ci et à condition que les mesures d'exécution adoptées conformément à cette procédure ne modifient pas les dispositions essentielles du présent règlement.

Le délai prévu à l'article 5, paragraphe 6, de la décision 1999/468/CE est fixé à trois mois.

## CHAPITRE VI

**DÉROGATIONS***Article 17***Accords avec des territoires ou des pays ne faisant pas partie du territoire de la Communauté**

1. La Commission peut autoriser un État membre à conclure des accords, en vertu de dispositions nationales, avec un pays ou un territoire qui ne fait pas partie du territoire de la Communauté, tel qu'il est défini à l'article 299 du traité, contenant des dérogations au présent règlement, afin de permettre que les virements de fonds entre ce pays ou territoire et l'État membre concerné soient traités comme des virements de fonds à l'intérieur de cet État membre.

Un tel accord ne peut être autorisé que:

a) si le pays ou le territoire concerné est lié à l'État membre concerné par une union monétaire, fait partie de la zone monétaire de cet État membre, ou s'il a signé une convention monétaire avec la Communauté représentée par un État membre;

b) si des prestataires de services de paiement du pays ou du territoire concerné participent, directement ou indirectement, aux systèmes de paiement et de règlement de cet État membre;

et

c) si le pays ou le territoire concerné impose aux prestataires de services de paiement relevant de sa juridiction l'application de règles identiques à celles instituées par le présent règlement.

2. Tout État membre qui souhaiterait conclure un accord visé au paragraphe 1 adresse une demande en ce sens à la Commission en lui communiquant toutes les informations nécessaires.

Dès réception de la demande d'un État membre par la Commission, les virements de fonds entre cet État membre et le pays ou territoire concerné sont provisoirement traités comme des virements de fonds à l'intérieur de cet État membre, jusqu'à ce qu'une décision soit arrêtée conformément à la procédure définie dans le présent article.

Si la Commission estime ne pas disposer de toutes les informations nécessaires, elle contacte l'État membre concerné dans les deux mois suivant la réception de sa demande en précisant les informations supplémentaires qui lui sont utiles.

Lorsque la Commission dispose de toutes les informations qu'elle juge nécessaires pour apprécier la demande, elle le notifie à l'État membre requérant dans un délai d'un mois et transmet la demande aux autres États membres.

3. Dans un délai de trois mois à compter de la notification visée au paragraphe 2, quatrième alinéa, la Commission décide, conformément à la procédure visée à l'article 16, paragraphe 2, d'autoriser ou non l'État membre concerné à conclure l'accord visé au paragraphe 1 du présent article.

En tout état de cause, la décision visée au premier alinéa est arrêtée dans les dix-huit mois suivant la réception de la demande par la Commission.

*Article 18***Virements de fonds à des organisations sans but lucratif à l'intérieur d'un État membre**

1. Tout État membre peut exempter les prestataires de services de paiement situés sur son territoire des obligations prévues à l'article 5 pour les virements de fonds destinés à des organisations sans but lucratif exerçant des activités à finalité charitable, religieuse, culturelle, éducative, sociale, scientifique ou fraternelle, à condition que ces organisations soient soumises à des obligations d'information et d'audit externe ou à la surveillance d'une autorité publique ou d'un organisme d'autorégulation reconnu en vertu du droit national et que ces virements de fonds soient limités à un montant maximal de 150 EUR par virement et effectués exclusivement sur le territoire de cet État membre.

2. Les États membres ayant recours au présent article communiquent à la Commission les mesures qu'ils ont adoptées pour appliquer l'option prévue au paragraphe 1, y compris une liste des organisations couvertes par l'exemption, les noms des personnes physiques qui exercent le contrôle final des organisations et une explication du mode de mise à jour de la liste. Ces informations sont également mises à la disposition des autorités chargées de la lutte contre le blanchiment de capitaux et le financement du terrorisme.

3. Une liste actualisée des organisations couvertes par cette exemption est communiquée par l'État membre concerné aux prestataires de services de paiement exerçant leurs activités sur son territoire.

*Article 19***Clause de révision**

1. Au plus tard le 28 décembre 2011 la Commission présente au Parlement européen et au Conseil un rapport contenant une évaluation économique et juridique complète de l'application du présent règlement, assorti, le cas échéant, de propositions visant à le modifier ou à l'abroger.

2. Ce rapport porte en particulier sur:

a) l'application de l'article 3 au regard des leçons tirées de l'usage abusif éventuel de la monnaie électronique telle que définie à l'article 1<sup>er</sup>, paragraphe 3, de la directive 2000/46/CE, ou de nouveaux moyens de paiement qui se seraient développés, à des fins de blanchiment de capitaux et de financement du terrorisme. En cas de risque d'un tel abus, la Commission présente une proposition visant à modifier le présent règlement;

b) l'application de l'article 13 en ce qui concerne les limites techniques susceptibles d'empêcher la transmission, au prestataire de services de paiement du bénéficiaire, des informations complètes sur le donneur d'ordre. Au cas où il serait possible de passer outre à ces limites techniques compte tenu de nouveaux développements dans le secteur des paiements, et eu égard aux coûts connexes à la charge des prestataires de services de paiement, la Commission présente une proposition visant à modifier le présent règlement.

## CHAPITRE VII

**DISPOSITIONS FINALES***Article 20***Entrée en vigueur**

Le présent règlement entre en vigueur le vingtième jour suivant celui de sa publication au *Journal officiel de l'Union européenne*, mais en aucun cas avant le 1<sup>er</sup> janvier 2007.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à Strasbourg, le 15 novembre 2006.

*Par le Parlement européen*  
*Le président*  
J. BORRELL FONTELLES

*Par le Conseil*  
*La présidente*  
P. LEHTOMÄKI

## **ANNEXE V**

*Common understanding of the obligations imposed by European Regulation 1781/2006 on the information on the payer accompanying fund transfers to payment service providers of payees*



**CEBS 2008 156/ CEIOPS-3L3-12-08/ CESR/08-773**

16 October 2008

**Common understanding of the obligations imposed by European Regulation 1781/2006 on the information on the payer accompanying funds transfers to payment service providers of payees**

**Background**

1. The European Regulation 1781/2006 on the information on the payer accompanying funds transfers to payment service providers of payees, which came into force on 1 January 2007, acts to implement the Financial Action Task Force's Special Recommendation VII in the European Union. The Regulation requires that Payment Service Providers "PSP"s (like banks and wire transfer offices) attach complete information about the payer to funds transfers made by electronic means. They must also check the information that accompanies incoming payments. The purpose of this regulation is to make it easier for the authorities to trace flows of money on occasions where that is deemed necessary.
2. This regulation sits alongside a wider body of EU and national legislation that aims to combat money laundering and the finance of terrorism, by, for example, mandating that financial institutions observe UN, EU and national sanctions, undertake due diligence checks on their customers when accounts are opened, monitor customers' behaviour on an ongoing basis, and inform the authorities when they form suspicions that they may have identified criminal or terrorist activity.
3. The Anti Money Laundering Task Force ("AMLTF") recognises that this Regulation is an important component of this wider regime. For example, when a bank checks incoming payments, it may find that information on the payer is missing or incomplete: this could be one of

the items of intelligence that contributes to a decision to file a suspicious transaction report with the authorities.

4. It has been brought to the AMLTF's attention that there appears to be an issue in relation to the information on the payer accompanying fund transfers to payment service providers of payees, arising out of this regulation. Further the Committee for the Prevention of Money Laundering and Terrorist Financing, chaired by the European Commission, and comprising of representatives from all Member States, asked the AMLTF to work on this topic, interacting with market participants. Also, the European Commission is ensuring appropriate contacts with the bodies working on payments issues too. The AMLTF has also analysed the possible conflict in the Regulation with the obligation to freeze the funds due to other provisions.
4. This paper aims to reflect a common understanding to deal with payments that lack the required information in respect of this regulation, which has been developed by the AMLTF, with the assistance of an informal consultation with the industry, including an Industry workshop held in January 2008, and has been subject to a three month public consultation launched in April 2008, which included a public hearing held on 6<sup>th</sup> May 2008.
5. This common understanding is based on the current functioning of payment, messaging and settlement systems, aims to ensure a level playing field between European payment service providers, and assist the reach of traceability<sup>1</sup> of transfers. This document aims to take into account the current level of compliance with the FATF Special Recommendation VII outside the EU, and the fact that funds transfers is a mass business. An annex describes some existing practices that our liaison with the financial services industry has identified. It outlines some measures that are currently being employed by payment services providers.

---

<sup>1</sup> Recital 6 of Directive 1781/2006 - The full traceability of transfers of funds can be a particularly important and valuable tool in the prevention, investigation and detection of money laundering or terrorist financing. It is therefore appropriate, in order to ensure the transmission of information on the payer throughout the payment chain, to provide for a system imposing the obligation on payment service providers to have transfers of funds accompanied by accurate and meaningful information on the payer.

6. The AMLTF was established in the second half of 2006 by CEBS, CESR and CEIOPS (- the three Level Three Committees, 3L3), with a view to providing a supervisory contribution in anti-money laundering (AML) and Counter Terrorism Finance issues, with a specific focus on the Third Anti-Money Laundering Directive. The AMLTF is composed of competent authorities from across Europe with supervisory responsibility for payment service providers.
7. The AMLTF acknowledges that there will be other competent authorities with these responsibilities, who are not represented on its committee. The AMLTF suggest that this paper would nonetheless represent a useful resource to these authorities.

## **1. Introduction**

1. This paper aims to reflect the common understanding of European supervisors concerning the application of Chapter III of the European Regulation 1781/2006 on the information on the payer accompanying funds transfers to payment service providers of payees (hereafter referred to as the "Regulation").
2. This common understanding is based on the current functioning of payment, messaging and settlement systems and aims to ensure a level playing field between European payment service providers (hereafter referred to as PSPs). The present common understanding takes into account the current level of compliance with the Special Recommendation VII outside the EU and the fact that funds transfers is a mass business.
3. This common understanding shall not be seen as an extension to this Regulation adding obligations, but rather as a clarification on the requirements in this Regulation, so as to provide PSPs with a common understanding of supervisory expectations on compliance with this Regulation.

## **2. Common understanding on Article 8 of the Regulation**

4. PSPs shall have effective procedures in place in order to detect whether in the messaging, payment or settlement system used to effect a transfer of funds, the fields relating to the information on the payer are complete in accordance with Articles 4 and 6. It is expected that PSPs undertake this obligation by applying both of the following elements.
5. First, as stated by the Regulation, the PSP of the payee shall detect whether, in the messaging, payment or settlement system used to effect a transfer of funds, the fields relating to the information on the payer have been completed using the characters or inputs admissible within the conventions of that messaging or payment and settlement system.
6. This first element will generally result from the mere application of the validation rules of the messaging, payment or settlement system, if those validation rules prevent payments being sent or received where the mandatory information concerning the payer is not present at all.
7. However, it is recognised that it is very difficult for a standard filter to be able to assess the completeness of all messages and that there will be instances where the payer information fields are completed with incorrect /meaningless information, where the payment will pass through the system.
8. Further PSPs are encouraged to apply filters to detect obvious meaningless information, such as information clearly intended to circumvent the intention of FATF Special Recommendation VII and this Regulation, based on their own experience, so as to assist PSPs in assessing whether they have been provided with meaningful information, as if so, the PSPs will then be obliged to reject the transfer, or to ask for information. PSPs should endeavour to apply this first element at the time of the processing.

9. Second, unless the PSP has detected the incompleteness of all transfers at the time of processing, the PSP should in addition to Article 8.1, subject incoming payment traffic to an appropriate level of monitoring to detect incomplete transfers or those with meaningless information by proceeding to appropriate post event random sampling to detect non compliant payments. Such sampling could focus more heavily on transfers from those higher risk sending PSPs, notably those PSPs who are already been identified by such sampling as having previously failed to comply with the relevant information requirement. PSPs identified as regularly failing should receive a particular attention in the application of this post event random sampling.

### **3. Common understanding on Articles 9 §1 and 10 of the Regulation**

10. By application of Article 8 along the lines suggested above, receiving PSPs may become aware of the incompleteness/meaninglessness of the information accompanying a transfer either at the time of processing (or even before), or later if undertaking the post event monitoring.

11. The present section takes into account Article 9 §1 and Article 10. The latter particularly refers to reporting obligations set out in Chapter III of the Third Directive. Chapter III of the Third Directive notably includes Articles 22 and 24 which are particularly important for the application of Article 9§1. Those Articles are taken into account by the present guidelines. It should also be noted that Article 9 §1 of the Regulation refers to Regulations 2580/2001 and 881/2002.

### **3.1 The PSP becomes aware, when receiving the transfer, that it is incomplete**

12.If the PSP becomes aware on receipt of the transfer, that it is incomplete, it should either reject the transfer, or ask for complete information. While it is asking for the complete information, it may either execute the transfer or hold the funds by temporarily suspending the transfer (if holding the funds is allowed by national law, bearing in mind any legal and consumer obligations).

#### **3.1.1 Internal policy, processes and procedures**

13.PSPs should adopt a policy defining their reaction on becoming aware of an incomplete transfer or with meaningless information.

14.Except for those PSPs that choose to systematically reject all such transfers, the PSP should endeavour to apply a mix of point 3.1.3, with 3.1.4 and/or 3.1.2. Without prejudice to any other applicable law or Regulation if any, the PSP should normally not execute systematically all incomplete transfers or transfers with meaningless information.

15.The PSP should define the criteria on which internal processes and procedures will be based in order to distinguish between transfers that they will execute directly and those that they will hold and/or those that they will reject. The PSP should draft those internal processes and procedures taking into account all applicable obligations. They should particularly mitigate their compliance risk when holding the funds or rejecting the transfer. Furthermore, the PSP shall particularly comply with Regulations 2580/2001 and 881/2002 and with any other lists they have an obligation to apply as it is provided by their jurisdiction.

16.The policy, processes and procedures should be approved at an appropriate hierarchic level and should be reviewed regularly.

### **3.1.2 The PSP chooses to reject the transfer (if allowed by national law)**

17. In this case, the PSP has no obligation to ask for the complete information. When rejecting a transfer, PSPs are encouraged to give the reason for the rejection to the PSP of the payer.

18. However, the PSP shall consider the incompleteness of the transfer or meaninglessness of the information as a factor in assessing whether any transaction related to the rejected transfer is suspicious and whether it must be reported to its FIU. The assessment of suspicion should be in accordance with existing Directives and requirements.

19. Depending on the risk criteria defined by the PSP in accordance with the risk based approach, the incompleteness/meaninglessness of information may or may not trigger the necessity to assess the transaction as being suspicious. If the transaction comes from a non EEA country which EU member states consider to be equivalent to the standards of the EU Directive 2005/60/EC, this could be considered accordingly in the risk assessment. PSPs should complete this assessment in accordance with the applicable obligations and their internal processes, procedures and policies.

### **3.1.3 The PSP chooses to execute the transfer**

20. Knowing that the transfer is incomplete or has meaningless information, the PSP chooses to execute it before asking for the complete /meaningful information to the PSP of the payer.

21. After having executed the transfer, it has to ask for complete information.

*Asking the complete information*

22. In this regard, the PSP should define criteria that it will use in order to determine on which occurrence it will send the request for complete information to the PSP of the payer.
23. Further, a maximum deadline between the receipt of payment and issuing a request for complete/meaningful information should be set, such as 7 working days.
24. Once the PSP has sent its request for complete/meaningful information, it should set a reasonable timeframe, such as 7 working days, or longer for messages received from outside the EEA, to receive this information and then, if the level of risk requires it, assess the suspicious character of the transaction or any related transaction and, if it did not receive a satisfactory answer to its request for further information regarding the relevant transfer, proceed to follow up on its request.

*Assessing the suspicious character*

25. As mentioned under point 3.1.2, PSPs should complete this assessment in accordance with the applicable obligations and their internal processes, procedures and policies. Depending on the risk criteria defined by the PSP in accordance with the risk based approach, the risk factor resulting from the incompleteness /meaninglessness of information may or may not trigger an internal transmission to the AML/CFT officer for assessment of its suspicious character.
26. In addition, it should be kept in mind that recital 16 of the Regulation particularly states that the accuracy and completeness of information on the payer should remain the responsibility of the PSP of the payer. Therefore, the PSPs of payees cannot be held responsible for the lack of information accompanying transfers they receive, including if they execute *de bona fide* a transfer without complete information on the payer that they would not have executed if the complete information had been provided.

*Follow up to the request for complete information.*

27. The PSP has to define policies and set up procedures and processes in order to complete an appropriate follow up to its requests for complete /meaningful information. The PSP should be able to demonstrate to its supervisor that those policies, processes and procedures are adequate in order to fulfil their objectives, and are effective in their application. The PSP could keep a record of its request, including any lack of reply, and make such a record available to the authorities.

28. For example, if the PSP of the payee did not receive a satisfactory answer to its request for complete/meaningful information after expiry of its desired timeframe, it should send a reminder, again with a desired timeframe by when it would expect to receive a response, after the first deadline has run out. The PSP may choose to batch up its follow up requests to such non responding PSPs.

29. The reminder should also notify that the sending PSP, in case it will not answer satisfactory within the deadline, will in future be subject to the internal high risk monitoring (cf. above 2.2.) and treated under the conditions of Art. 9 (2) of Regulation 1781/2006. An alternative could be that the PSP may choose to state this in its Terms and Conditions.

**3.1.4 The PSP chooses to hold the funds, (if allowed by national law)**

30. Section 3.1.1 of this common understanding defines how a PSP has to proceed in order to determine its reaction towards an incomplete transfer or a transfer with meaningless information. As mentioned in that section, it should be stressed that a PSP can temporarily suspend the execution of the transfer and thus holds the funds if this is requested by, or compatible with, the legal or regulatory framework to which it is subject. However, apart from suspending the transfer on the basis of the option to ask for complete information defined by Regulation 1781/2006 it may be necessary to "freeze" the funds for an undefined period of time compliant

with relevant "freezing" measures and economic sanctions (like those set out in Regulations 2580/2001 and 881/2002), with the obligation to refrain from executing transactions which are reported as suspicious (article 24(1) of Directive 2005/60/EC) and with the order to postpone such transactions issued by the competent authority (article 24(1) of Directive 2005/60/EC). Further, it is also stressed that PSPs should particularly mitigate their legal and compliance risk when holding the funds or rejecting the transfer, including in relation to their contractual obligations.

31. It can be considered that it is particularly appropriate to apply this option when there is need for clearing the situation internally or with other group members, databases or the FIU<sup>2</sup> in order to establish or reject the suspicion of money laundering.

32. When the PSP chooses to hold the funds, its first action should be to ask for the complete /meaningful information.

*Asking for the complete information*

33. In this regard, the PSP should define criteria that it will use in order to determine on which occurrence it will send the request for complete /meaningful information to the PSP of the payer. However, those processes and procedures should ensure that the PSP will ask, ideally at least once every 7 working days (or longer for payments from outside the EEA), for the complete /meaningful information from each PSP that sent at least one incomplete transfer during the previous 7 working days. The attention of the PSP is drawn on the fact that even if the maximum allowed deadline is the same as in section 3.1.3, they have to define themselves criteria in order to determine on which occurrence they will send the request. In the present section, those internally defined criteria should take into account the fact that they would in principle not be in a position to decide about rejecting the transfer or executing it as long as they will not have received the answer to the request for complete /meaningful information.

---

<sup>2</sup> FIU = Financial Intelligence Unit

34. The request for complete/meaningful information should include a deadline for the PSP of the payer to answer. A maximum deadline should be set, such as 3 working days, or longer for payments from outside the EEA. However, PSPs of payees may decide to fix a shorter deadline. This deadline could be communicated through its insertion in the Terms and Conditions of the receiving PSP.
35. Once the PSP has sent its request for complete /meaningful information, it has to wait for its selected deadline, such as 3 working days, for receiving the requested information to run out.
36. Then, if it receives a satisfactory answer to the request for complete information, it should assess the suspicious character and, after having completed this assessment, decide whether to execute the transfer, reject the transfer or sending a STR to the FIU and holding the funds.
37. The PSP has to define policies and set up procedures and processes in order to complete an appropriate follow up to its requests for complete /meaningful information. This should in particular define its reaction to the absence of a valid answer in the required deadline and the processes for sending reminders to failing PSPs. In addition, the PSP should be able to demonstrate to its supervisor that those policies, processes and procedures are adequate in order to fulfil their objectives and are effectively applied.
38. For example, if it does not receive a satisfactory answer to the request for complete /meaningful information, it should proceed to the follow up to the request. This follow up could consist of sending a reminder, such as 3 working days after the first deadline has run out. The reminder should set a deadline for the sending PSP, which could be again 3 working days. The reminder could also notify that the sending PSP, in case it will not answer satisfactory within the deadline, will in future be subject to the internal high risk monitoring (cf. above 2.2.) and treated under the conditions of

Art. 9 (2) of Regulation 1781/2006. Another alternative could be that the PSP may choose to state this in its Terms and Conditions.

39. Additionally, the reminder should indicate that the respective transfer is currently pending. After that the deadline included in the reminder has run out, and whether or not it has received a satisfactory answer to its reminder, the receiving PSP should assess the suspicious character and, after having completed this assessment, decide whether to execute the transfer, reject the transfer or send a STR to the FIU and hold the funds. When it decides to execute the transfer, it has to take into account the factors that led him to hold the funds at the initial stage. For more details on "*Assessing the suspicious character*", refer to section 3.1.3.

### **3.2 The PSP becomes aware that a transfer is incomplete after having executed the transfer**

40. Where the PSP of the payee becomes aware subsequent to processing the payment that it contained meaningless or incomplete information either as a result of random checking or by any other way, it must:

- a. consider the incompleteness /meaninglessness of the information as a factor in assessing whether the transfer or any related transaction is suspicious and whether it must be reported to its FIU;
- b. consider asking for the complete /meaningful information to the PSP of the payer or, where appropriate, to the intermediary PSP. In this case, it shall also proceed to the follow up actions to the request, as above mentioned.

## **4. Common understanding on Article 9 §2**

### **4.1 The regularity of failure**

41. Recital 17 calls for a common approach on Article 9 §2, which provides that PSPs have to react towards PSPs that are regularly failing to supply the complete information.

42. However, the Regulation does not elaborate on the concept of regularity. A common approach on this point will be highly desirable as a common response by EU PSPs will enhance the credibility and effectiveness of their reaction and, thereby, international compliance with FATF Special Recommendation VII, SR VII. The PSP of the payee shall determine when the other PSP is regularly failing. This could be due to different reasons, for example regularly not inserting the full information of the payer and/or regularly not responding to requests in a timely manner. Also the level of failure may vary according to the risk based approach of the payee PSP.

43. Accordingly the PSP of the payee shall consider what criteria determine whether the PSP of the payer has regularly failed to provide the required information. Until the PSP of the payee, has sufficient data to analyse its own experience in identifying such "failure", the following criteria could, for example, be used:

- a. the level of cooperation of the PSP of the payer relating to requests for complete/meaningful information sent ;
- b. a threshold defined in a percentage of incomplete transfers or transfers with meaningless information sent by a specific PSP;
- c. a threshold defined in a percentage of still incomplete transfers in a period or with meaningless information, after that the PSP of the payer has received a certain amount of requests for complete/meaningful information;

- d. a threshold defined equating to an absolute number of incomplete transfers or transfers with meaningless information sent by a specific PSP; and
- e. a threshold defined equating to an absolute number of still incomplete transfers or transfers with meaningless information in a defined period, after that the PSP of the payer has received a certain amount of requests for complete/meaningful information.

#### **4.2 Steps to be taken**

44. Once a PSP has been assessed as regularly failing by a PSP of a payee, the PSP of the payee should issue a warning to the PSP which is failing, in order to draw its attention to the fact that, in accordance with the present common understanding, it has been identified as regularly failing.

#### **4.3 Transmission to the authorities**

45. As provided by Article 9§2, once a PSP has been identified as being regularly failing to provide the required information, the PSP of the payee shall report that fact to the "authorities responsible for combating money laundering or terrorist financing". Determination of such "authorities responsible" remains within national arrangements, and they should receive this information. These "authorities" are encouraged to exchange the information with their national supervisors.

46. This transmission of such information should be clearly distinguished from a Suspicious Transaction Report, STR. Indeed, the purpose of this transmission is to signal that a specific PSP meets the criteria defining the regular failure in this common understanding, which indicates a difficulty to comply with SR VII. This transmission does not imply that the PSP of the payer is suspected of money laundering or terrorism financing. It implies that it might be failing to respect its obligations under SR VII. Some countries have chosen to develop a specific format for "Article 9 §2

reporting". This seems to enhance the perception of this distinction by PSPs.

#### **4.4 Decision as to restrict or terminate the business relationship with a PSP reported as being regularly failing**

47. The Regulation states that the PSP of the payee decides whether or not to restrict or terminate its business relationship with regularly failing PSPs.

48. For the PSP of the payee to act alone against a failing PSP may prove commercially disruptive, particularly where that PSP is an important counterparty.

49. In addition, we would also expect supervisors to share views about failing PSPs and consider what action they may take.

50. It should be stressed that, when the regularly failing PSP is also a correspondent bank from a third country, the decision taken according to the present section and the enhanced due diligence performed according to Article 13 §3 of the Third Anti Money Laundering Directive could all be included as part of the process of managing the cross-border correspondent bank's relationship.

#### **5. Internal data collecting and reporting**

51. PSPs should be able to demonstrate to their supervisory authority that there are effective policies and procedures in place related to data collection and internal reporting that are appropriate to meeting the requirements of the Regulation. Further, PSPs' internal control and audit policies and procedures for Anti Money Laundering and Combat of Financing of Terrorism should be subject to appropriate senior management oversight.

## **6. Threshold**

52. It should be born in mind, when applying the Regulation and the present common understanding, that some countries outside the EU may have framed their own Regulation to incorporate a threshold of €/US\$ 1,000 below which the provision of complete information on out-going payments is not required. This is permitted by the Interpretative Note to SR VII. This does not preclude European PSPs from calling for the complete information where it has not been provided. The existence of such a threshold, although relevant for the risk-based decision whether to carry out, to hold or to reject the transaction as well as for the determination of the regularity of failures, does not exclude the application of the procedures under points 3 and 4 above.

53. Any threshold of a higher amount would be non compliant with the SR VII and any related transfer will have to be considered as incomplete.

## **7. Review of the common understanding**

54. Considering the fact that the common understanding takes into account the current level of compliance with SR VII at international level and the current functioning of payment, settlement, and supporting systems, it should be revised subject to the compliance level attained by the Industry with the regulations, and not later than when the Regulation 1781/2006 is reviewed.

## **Annex 1**

### **Existing industry practice**

This annex describes some existing practice that our liaison with the financial services industry has identified. It outlines some measures that are currently being employed by payment service providers.

- Bank N is a large bank based in an EU member state. It handles tens of thousands of electronic transfers every day. It sends and receives payments between EU member states, and countries outside of the EU, using the SWIFT message system. The SWIFT system prevents messages with blank fields from being processed. However, meaningless data can still be attached to payments: the SWIFT messaging systems are not able to prevent this. As such, Bank N undertakes post-event sampling of incoming payments traffic to identify where data is likely to be incomplete or meaningless. Sampling is focused on certain areas that are regarded to present a higher risk. Examples of higher-risk payments identified by Bank N include a) those that originate from payment service providers outside the EU, particularly those from jurisdictions that the bank has identified to be of a higher risk b) those from payment service providers that have previously failed to meet their obligations and c) payments that are collected by the payee in cash on a "pay on application and identification basis".
- Bank P is a small private bank based in a European capital that predominantly deals with customers from certain countries outside the EU. It receives very few electronic payments on behalf of its customers. When these payments are received it is not unusual for these to have originated from outside the EU, and to represent large sums of money. Bank P is able to subject each payment to scrutiny by a member of staff. The staff member's knowledge of the countries in question allows

them to quickly identify where, for example, the payer's address appear to not correspond with what might be expected.

- Bank Q is a medium-sized bank in an EU state. Bank Q seeks to identify incorrect data by performing post-event sample checks. As such, the payment has already been made by the time that Bank Q has become aware that information is incorrect. Aside from the practical issues, Bank Q is unsure whether it would be desirable to reject a transaction "in-flight": this could lead to civil claims for breach of contract, and also risk prosecution under national legislation that outlaws "tipping off" criminals. The next step that the bank takes is to seek complete information on the payer. It also considers whether there is anything suspicious about the transaction, although it is difficult to form suspicions based on this information alone. Bank Q is recording where payment service providers are failing to provide information, and considering which institutions are being sufficiently unreliable or unco-operative to warrant further action. Bank Q has not ruled out ending relationships with some payment service providers outside of the EU.
- For intermediaries, many view that the Payee PSP should address a request for missing information direct to the Payer PSP. It should not be necessary to involve the intermediary PSP, other than on occasions where their help is needed to provide a payer PSP transaction reference number in order to trace the payment.
- Some banks view that is sufficient to have information in Field 20 in the Swift standard message and that this meets the obligation according to the Regulation for a "unique identifier". However, in non EU payments there must be information on the banks account in Field 50 in the Swift message.

## Annex 2

**Summary of Industry workshop on Anti Money Laundering in relation  
to the European regulation on the information on the payer  
accompanying funds transfers  
*London, 9<sup>th</sup> January 2008***

1. A workshop was held with industry participants and the Anti Money Laundering Task Force (“AMLTF”) on obligations imposed by the EU Regulation 1781/2006, implemented in December 2007. The AMLTF Chair, Andrea Enria, Secretary General of CEBS, provided background on the AMLTF, which was established in the second half of 2006 by CEBS, CESR and CEIOPS (- the three Level Three committees, 3L3), with a view to providing a supervisory contribution in anti-money laundering (AML) and Counter Terrorism Finance issues, with a specific focus on the Third Anti-Money Laundering Directive. In particular, its mandate is focused on the developments of risk-based approaches to Customer Due Diligence (CDD) and the “know your customer principle” (KYC) and their impact on the internal organisation and controls of intermediaries. The AMLTF provides a forum for exchange of experiences and networking between supervisory authorities, to help identifying practical issues that supervisors face in their day-to-day work and, when possible find common practical answers.
2. The workshop had been convened as the AMLTF wishes to find practical solutions to deal with payments that lack the required information in respect of the Regulation 1781/2006.
3. Further the Committee for the Prevention of Money Laundering and Terrorist Financing (CPMLTF), chaired by the European Commission and comprises of representatives from all Member States, asked the AMLTF to work on this topic, interacting with market participants. Also, the Commission is ensuring appropriate contacts with the bodies working on payments issues too.
4. The CBFA AMLTF member presented the AMLTF’s (draft) paper AMLTF 2007 22 rev2, relating to information on the payer of accompanying

fund transfers to payment service providers of payees, and sought to gather industry views on the nature and relevance of the problem, to assist in AMLTF finalising this paper and discussing the issues at the CPLMTF. In particular the CBFA AMLTF member presented issues relating to the general principles for common understanding on Articles 8, 9, 10 and 16 of Reg. 1781/2006. In adherence to standard 3L3 practices for public consultation, the AMLTF intends to finalise this paper, and subject it to formal consultation, and hence workshop attendees' comments were sought informally on the current draft.

5. Discussion focussed on incomplete incoming transactions messages, both inter EEA and from 3<sup>rd</sup> countries. Market participants agreed that the problem is indeed relevant and expressed their availability to provide information on the amount and distribution (including, in terms of country of origin and Payment Service Providers) of the transactions with incomplete information.
6. The industry representatives also presented their approaches to dealing with the issue. Some differences emerged both in the timing of the assessment of the completeness of information as per Art 9.1 and in the interpretation of Art 9.2. An issue relating to Art 6 was also raised, calling for further investigation: it was pointed out that a reference number might be sufficient for funds transfer inter EEA, yet from a practical perspective, might not be sufficient for many competent authorities, in relation to their domestic AML/financial crime requirements.
7. Some concerns were expressed as to the compliance burden of some of the options presented in the draft AMLTF paper (i.e. under Art 9.1 and Art 10) where the AMLTF proposed i) PSP execute the transfer first and then ask for complete information. PSP wait for deadline for receiving the complete information to run out and then assess the suspicious character of the transaction; and ii) PSP define risk criteria in order to allow their systems to distinguish between those incomplete transfers that can be executed before assessing their suspicious character and those incomplete transfers for which the assessment of their suspicious character and the request for complete information should be done

before executing the transfer. Some also suggested that there may be an additional option, or that a mix of options should be sought that better reflects current market practices.

8. Although the urgency of the subject matter was acknowledged, several market participants invited the AMLTF not to rush to conclusions, especially in some areas.
9. The AMLTF Chair committed to come back to the industry group with:
  - a. a request for some information by early February, and
  - b. to submit, for an informal feedback, a revised version of the paper as soon as available; and
10. Further in adherence to standard 3L3 practices for public consultation, the AMLTF aims to subject its proposals for a 3 month public consultation, relatively soon, although there may be more flexibility in the consultation period so as to respect the urgency of finding a solution to the problem, having taken into account the informal pre consultation with industry.

## ANNEXE VI

### **Adresses internet utiles en matière de lutte contre le blanchiment et le financement du terrorisme**

Site du Comité de Bâle :

[www.bis.org](http://www.bis.org)

- Devoir de diligence des banques au sujet de la clientèle Octobre 2001 ;
- Guide général pour l'ouverture de compte et l'identification de la clientèle février 2003.

Site du Groupement d'Action Financière (GAFI – FATF) :

[www.fatf-gafi.org](http://www.fatf-gafi.org)

- Le site internet du GAFI comporte des informations et des documents importants contenant des précisions sur les méthodes et techniques et les risques en matière de lutte contre le blanchiment et le financement du terrorisme