CBFA

COMMISSION BANCAIRE, FINANCIÈRE ET DES ASSURANCES

Circulaire CBFA_2010_09 du 6 avril 2010

Modifiée par la circulaire CBFA_2011_09 du 1 mars 2011
Devoirs de vigilance à l'égard de la clientèle, la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, et la prévention du financement de la prolifération des armes de destruction massive
(version coordonnée)

Champ d'application:

Toutes les entreprises établies en Belgique qui relèvent des compétences de contrôle de la CBFA et qui, visées à l'article 2, § 1er, 4 à 15 , de la loi et à l'article 2 du règlement, sont assujetties aux obligations légales et réglementaires de prévention du blanchiment de capitaux et du financement du terrorisme, ci-après dénommés "organismes financiers" (cf. infra, chapitre 1)

Résumé/Objectifs:

La présente circulaire rassemble et commente les dispositions légales et réglementaires applicables aux organismes financiers en matière de prévention de l'utilisation du système financier aux fins du blanchiment des capitaux, du financement du terrorisme et du financement de la prolifération des armes de destruction massive. Elle formule en outre les recommandations de la CBFA en vue d'une application correcte et effective de ces dispositions.

Structure:

rue du Congrès 12-14 | 1000 Bruxelles
t +32 2 220 53 42| f +32 2 220 54 93 | www.cbfa.be

Introduction

Les exigences en matière de prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme ont connu d'importantes évolutions au cours des dernières années sur le plan international, particulièrement à la suite de la révision des « 40 recommandations sur le blanchiment d'argent » du Groupe d'Action Financière (GAFI) en juin 2003, et à l'adoption de ses « 9 recommandations spéciales sur le financement du terrorisme » en 2001 et 2004.

En Belgique, cette évolution a déjà été en grande partie prise en compte par la loi du 12 janvier 2004 qui a modifié la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système aux fins du blanchiment de capitaux et du financement du terrorisme.

Concernant spécifiquement le secteur financier belge, cette évolution des standards internationaux a également présidé à l'élaboration du règlement de la Commission bancaire, financière et des assurances du 27 juillet 2004 relatif à la prévention du blanchiment de capitaux et du financement du terrorisme, approuvé par arrêté royal du 8 octobre 2004 [1], et des circulaires PPB 2004/8 et D.250 du 22 novembre 2004 de la CBFA (modifiée par les circulaires PPB 2005/5 et D.258 du 12 juillet 2005) relative aux devoirs de diligence au sujet de la clientèle et à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme.

Néanmoins, de nouvelles évolutions sont intervenues depuis lors dont il importe de tenir compte.

En particulier, le Parlement européen et le Conseil ont adopté le 26 octobre 2005 la directive 2005/60/CE relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme [2]. Cette troisième directive européenne en la matière vise essentiellement à aligner le droit européen sur les 40 nouvelles recommandations du GAFI sur le blanchiment d'argent et sur ses 9 recommandations spéciales sur le financement du terrorisme. Des mesures de mise en œuvre de cette directive européenne ont en outre été définies par la Commission européenne dans sa directive 2006/70/CE du 1er août 2006 [3]. De plus, le Parlement européen et le Conseil ont adopté le règlement (CE) n° 1781/2006 du 15 novembre 2006 [4], qui définit des obligations uniformes dans tout l'Espace Economique Européen et conformes à la Recommandation spéciale VII du GAFI en ce qui concerne les informations relatives au donneur d'ordre qui doivent accompagner les virements électroniques de fonds.

Sur le plan des standards prudentiels internationaux, ceux qui étaient en vigueur lors de l'adoption par la CBFA de son règlement du 27 juillet 2004 et de ses circulaires des 22 novembre 2004 et 12 juillet 2005 (cf. supra) demeurent d'actualité [5].

Par ailleurs, les comités européens de contrôleurs (CEBS, CEIOPS et CESR) ont élaboré et publié le 16 octobre 2008 un document commun (« *common understanding* ») énonçant la compréhension commune des autorités de contrôle de certaines des obligations des organismes financiers instaurées par le règlement européen (CE) n° 1781/2006 du 15 novembre 2006 précité. De plus, en marge de la Recommandation spéciale VII du GAFI et du règlement européen qui la met en œuvre, le Comité de Bâle a publié le 12 mai 2009 un nouveau document intitulé « *Due diligence and transparency regarding cover payment messages related to cross-border wire transfers* »[6].

---

1 Moniteur Belge du 22 novembre 2004.

2 JOCE L309 du 25 novembre 2005, pp. 15 à 36.

3 Directive 2006/70/CE de la Commission du 1er août 2006 portant mesures de mise en œuvre de la directive 2005/60/CE du Parlement européen et du Conseil pour ce qui concerne la définition des «personnes politiquement exposées» et les conditions techniques de l'application d'obligations simplifiées de vigilance à l'égard de la clientèle ainsi que l'exemption au motif d'une activité financière exercée à titre occasionnel ou à une échelle très limitée, JOCE L214 du 4 août 2006, pp. 29 à 34.

4 JOCE L345 du 8 décembre 2006, pp. 1 à 9.

5 En ce qui concerne le Comité de Bâle sur le Contrôle Bancaire :
- « *Devoir de diligence des banques au sujet de la clientèle* », octobre 2001.
- « *General Guide to account opening and customer identification* », février 2003.
- « *Consolidated KYC Risk Management* », octobre 2004.

Les documents du Comité de Bâle peuvent être consultés sur le site internet de la Banque des Règlements Internationaux *http://www.bis.org*

En ce qui concerne le l'Association Internationale des Contrôleurs d'Assurance :
- « *Principes de Base en matière d'assurance et méthodologie* », Principe de Base n° 28, commenté dans sa note interprétative, octobre 2003.
- « *Guidance Paper n° 5 on Anti-Money Laundering and Combating the Financing of Terrorism* » octobre 2004

Les documents de l'AICA peuvent être consultés sur son site internet *http://www.iaisweb.org*

6 *http://www.bis.org/publ/bcbs154.pdf?noframes=1*

En Belgique, la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme (ci-après, « la loi ») a été modifiée par la loi du 18 janvier 2010 [7], essentiellement afin de transposer en droit belge la troisième directive européenne en la matière et sa directive de mise en œuvre (cf. supra). A cette occasion, le Législateur belge a également procédé à une restructuration globale de la loi du 11 janvier 1993.

En vertu de la loi ainsi modifiée, la CBFA demeure chargée de fixer par la voie d'un règlement les modalités d'application des obligations légales des entreprises qu'elle contrôle. Tenant compte des modifications apportées à la loi, la CBFA a dès lors adopté le 23 février 2010 un règlement [8] remplaçant son règlement du 27 juillet 2004 relatif à la prévention du blanchiment de capitaux et du financement du terrorisme (ci-après « le règlement »).

Complémentairement, la CBFA est également amenée à actualiser par la présente circulaire ses commentaires des dispositions légales et réglementaires applicables et ses recommandations relatives à leur mise en œuvre, tenant compte également des exigences légales et prudentielles d'organisation administrative et de contrôle interne adéquats inscrites.

En conséquence, la présente circulaire abroge et remplace la circulaire PPB 2004/8 et D.250 du 22 novembre 2004 (modifiée par la circulaire PPB 2005/5 et D.258 du 12 juillet 2005).

1. Destinataires de la circulaire

La présente circulaire s'adresse aux entreprises établies en Belgique qui relèvent des compétences de contrôle de la CBFA et qui, visées à l'article 2, § 1er, 4° à 15°, de la loi et à l'article 2 du règlement, sont assujetties aux obligations légales et réglementaires de prévention du blanchiment de capitaux et du financement du terrorisme, ci-après dénommés "organismes financiers", à savoir :

- les établissements de crédit de droit belge et les succursales en Belgique d'établissements de crédit étrangers, que ceux-ci relèvent ou non du droit d'un Etat membre de l'Espace Economique Européen;
- les entreprises d'assurances de droit belge et les succursales en Belgique d'entreprises d'assurances étrangères, que celles-ci relèvent ou non du droit d'un Etat membre de l'Espace Economique Européen, qui sont habilitées à exercer en Belgique l'activité d'assurance-vie;
- les entreprises d'investissement (sociétés de bourse ou sociétés de gestion de portefeuille et de conseil en investissement) de droit belge et les succursales en Belgique d'entreprises d'investissement étrangères, que celles-ci relèvent ou non du droit d'un Etat membre de l'Espace Economique Européen;
- les sociétés de gestion d'organismes de placement collectif de droit belge et les succursales en Belgique de sociétés étrangères de gestion d'organismes de placement collectif, que celles-ci relèvent ou non du droit d'un Etat membre de l'Espace Economique Européen, dès lors qu'elles sont autorisées de par l'étendue de leur agrément à intervenir dans la commercialisation des parts ou actions des organismes de placement collectif qu'elles gèrent;
- les organismes de placement collectifs de droit belge à forme statutaire, pour autant que et dans la mesure où ils assurent eux-mêmes la commercialisation de leurs titres sans recourir à une entité tierce;
- les organismes de liquidation visés à l'article 23 de la loi du 2 août 2002;
- les établissements de paiement de droit belge et les succursales en Belgique d'établissements de paiement étrangers, que ceux-ci relèvent ou non du droit d'un Etat membre de l'Espace Economique Européen [9];
- les bureaux de change exerçant les activités de change manuel de devises et/ou de transfert de fonds;
- les entreprises hypothécaires;
- les courtiers en services bancaires et d'investissement;
- les intermédiaires d'assurance non exclusifs exerçant leur activité professionnelle dans le groupe d'activités « vie »;
- et les entreprises de marché qui organisent les marchés réglementés belges.

7 Loi modifiant la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, et le Code des sociétés, M.B. 26 janvier 2010.

8 Règlement approuvé par arrêté royal du 16 mars 2010 - Moniteur Belge du 24 mars 2010.

9 A dater de leur assujettissement à la loi du 11 janvier 1993.

Le règlement et la présente circulaire trouvent à s'appliquer à l'ensemble de ces organismes. Leurs dispositions visent à couvrir de façon harmonisée l'ensemble des opérations et des relations d'affaires que ces organismes sont susceptibles de nouer avec leurs clients. Dans leur mise en œuvre, il y a cependant lieu de tenir compte des spécificités des activités de chacune des catégories d'organismes visés et, au sein de celles-ci, des activités de chaque organisme.

Ainsi, les organismes de placement collectifs de droit belge à forme statutaire ne sont destinataires de la présente circulaire que dans la mesure où ils sont soumis aux dispositions de la loi du 11 janvier 1993 et du règlement de la CBFA du 23 février 2010, c'est à dire, pour autant et dans la mesure où ils assurent eux-mêmes la commercialisation de tout ou partie de leurs titres sans recourir à l'intermédiation d'une autre entité tierce. Ne sont dès lors pas visés les OPC qui ne fournissent pas eux-mêmes le service de réception et transmission d'ordres de souscription de leurs titres mais recourent à cet effet à une entité tierce, même s'ils prennent en charge d'autres aspects de la commercialisation des titres (comme, par exemple, l'organisation de campagnes promotionnelles), mais sans entrer directement en contact avec les souscripteurs. Lorsque les souscriptions sont réalisées, pour partie en recourant à une entité tierce, et pour partie par l'OPC lui-même, celui-ci n'est assujetti aux dispositions légales et réglementaires, et n'est destinataire de la présente circulaire que dans le cadre des opérations des personnes qui souscrivent directement auprès de lui à ses titres, sans intervention d'une entité tierce. [10]

Lorsque l'agrément d'une entreprise d'assurances porte simultanément sur des branches du groupe d'activités "vie" et sur des branches du groupe d'activités "non-vie", les obligations légales et réglementaire de prévention du blanchiment de capitaux et de financement du terrorisme sont uniquement d'application dans le cadre de ses activités qui relèvent du groupe d'activités "vie". Il en va dès lors de même pour l'application de la présente circulaire.

En ce qui concerne les organismes de liquidation et les entreprises de marché qui organisent les marchés réglementés belges, leurs clients relèvent très fréquemment des catégories visées à l'article 11, § 1er, de la loi [11] à l'égard desquelles prévalent des dispenses d'identification. Le champ s'application de leurs obligations légales et réglementaires en matière d'identification des clients, mandataires et bénéficiaires effectifs, ainsi que leurs obligations de vigilance à l'égard des opérations et relations d'affaires s'en trouve dès lors limité en proportion. Néanmoins, l'ensemble de ces obligations trouvent à s'appliquer lorsqu'ils exercent leurs activités en relation avec d'autres clients que ceux visés à l'article 11, § 1er, de la loi, ou dans toutes les situations dans lesquelles ils ont des soupçons de blanchiment de capitaux ou de financement du terrorisme [12]. La présente circulaire leur est dès lors également applicable dans le contexte de ces activités ou dans ces circonstances. Elle clarifie également à leur intention les obligations légales et réglementaires relatives à l'organisation générales (voir en particulier les chapitres 9 à 11).

2. Champ d'application *ratione materiae* de la loi

2.1. Définition du blanchiment de capitaux

Article 5, § 1er de la loi

Aux fins de l'application de la présente loi, par blanchiment de capitaux il faut entendre :

- *la conversion ou le transfert de capitaux ou d'autres biens dans le but de dissimuler ou de déguiser leur origine illicite ou d'aider toute personne qui est impliquée dans la réalisation de l'infraction d'où proviennent ces capitaux ou ces biens, à échapper aux conséquences juridiques de ses actes;*
- *la dissimulation ou le déguisement de la nature, de l'origine, de l'emplacement, de la disposition, du mouvement ou de la propriété des capitaux ou des biens dont on connaît l'origine illicite;*
- *l'acquisition, la détention ou l'utilisation de capitaux ou de biens dont on connaît l'origine illicite;*

10 Il est à noter que ces précisions visent uniquement à clarifier les conditions de l'assujettissement des OPC, sans pour autant que l'on puisse en déduire que les obligations découlant de la loi à charge des OPC qui y sont assujettis ne s'appliqueraient qu'aux seules opérations de souscription. Ces obligations sont notamment susceptibles de s'appliquer également aux demandes de rachat qui seraient directement adressées à l'OPC assujetti, sans passer par l'intermédiaire d'une partie tierce.

11 Cf. section 4.5.2 infra.

12 Cf. section 4.2.2.3 infra.

- *la participation à l'un des actes visés aux trois points précédents, l'association pour commettre ledit acte, les tentatives de le perpétrer, le fait d'aider, d'inciter ou de conseiller quelqu'un à le commettre ou le fait d'en faciliter l'exécution.*

Ni la loi du 12 janvier 2004 ni celle du 18 janvier 2010 n'ont modifié cette définition légale du blanchiment de capitaux. De même, cette dernière loi n'a que peu modifié la liste des infractions sous-jacentes visées à l'article 5, § 3, de la loi du 11 janvier 1993 :

Article 5, § 3, de la loi

Pour l'application de la présente loi, l'origine de capitaux ou de biens est illicite lorsque ceux-ci proviennent de la réalisation:

1° d'une infraction liée:
- *au terrorisme ou au financement du terrorisme;*
- *à la criminalité organisée;*
- *au trafic illicite de stupéfiants;*
- *au trafic illicite d'armes, de biens et de marchandises, en ce compris les mines anti-personnel et/ou les sous-munitions;*
- *au trafic de main-d'œuvre clandestine;*
- *à la traite des êtres humains;*
- *à l'exploitation de la prostitution;*
- *à l'utilisation illégale chez les animaux de substances à effet hormonal ou au commerce illégal de telles substances;*
- *au trafic illicite d'organes ou de tissus humains;*
- *à la fraude au préjudice des intérêts financiers des Communautés européennes;*
- *à la fraude fiscale grave et organisée qui met en œuvre des mécanismes complexes ou qui use de procédés à dimension internationale;*
- *au détournement par des personnes exerçant une fonction publique et à la corruption;*
- *à la criminalité environnementale grave;*
- *à la contrefaçon de monnaie ou de billets de banque;*
- *à la contrefaçon de biens;*
- *à la piraterie;*

2° d'un délit boursier ou d'un appel public irrégulier à l'épargne ou de la fourniture de services d'investissement, de commerce de devises ou de transferts de fonds sans agrément;

3° d'une escroquerie, d'un abus de confiance, d'un abus de biens sociaux, d'une prise d'otages, d'un vol ou d'une extorsion, d'une infraction liée à l'état de faillite.

Compte tenu du fait que le contexte n'est pas celui d'une loi pénale, le législateur a préféré se référer, non pas à des dispositions spécifiques du droit pénal, mais à des agissements considérés comme graves dans leur signification courante.

En conséquence, il n'est pas requis des personnes et organismes assujettis à la loi qu'ils examinent si chaque élément de la définition d'une infraction pénale est présent pour déterminer si les capitaux sont vraisemblablement d'origine illicite, mais seulement s'ils pourraient trouver leur origine dans l'exercice de l'une des activités criminelles énumérées.

2.2. Définition du financement du terrorisme

Article 5, § 2, de la loi

Aux fins de l'application de la présente loi, il faut entendre par financement du terrorisme le fait de fournir ou de réunir des fonds, directement ou indirectement et par quelque moyen que ce soit, dans l'intention de les voir utilisés ou en sachant qu'ils seront utilisés, en tout ou en partie, par un terroriste ou une organisation terroriste ou pour la commission d'un ou plusieurs actes terroristes.

Cette définition a été modifiée par la loi du 18 janvier 2010. Le commentaire suivant y est consacré dans l'exposé des motifs de cette loi [13] :

« L'article 7 en projet vise à adapter la définition du financement du terrorisme à celle reprise dans la directive 2005/60/CE, laquelle est établie en conformité avec l'article 2, § 2, b) de la décision-cadre du Conseil de l'Union européenne du 13 juin 2002 relative à la lutte contre le terrorisme et avec l'article 2 de

13 Chambre des Représentants, 2008-2009, Doc 52 1988/001, p. 26.

la convention internationale pour la répression du financement du terrorisme, faite à New York, le 9 décembre 1999. Il s'agit par ailleurs de tenir compte des critères essentiels de la recommandation spéciale II du GAFI en matière d'incrimination du financement du terrorisme qui explicite les caractéristiques que doit présenter cette infraction et ce, notamment en termes de finalité à savoir la commission d'un ou plusieurs actes terroristes, par une organisation terroriste ou par un terroriste. Cette référence à ces éléments plutôt qu'à des infractions spécifiques dans la loi du 11 janvier 1993 permet de mieux rendre compte de l'esprit de cette loi qui se réfère non pas à des dispositions spécifiques du Code pénal mais plus généralement à des formes de criminalité déterminées, appréhendées dans un sens large et commun. Dans ce cadre, tous les « fonds » doivent être pris en considération et ce, sans imposer que ceux-ci aient effectivement servi à commettre ou tenter de commettre un ou plusieurs actes terroristes ni qu'ils soient liés à un ou plusieurs actes terroristes spécifiques. La Convention sur le financement du terrorisme définit ce qu'il convient d'entendre par « fonds » soit des biens de toute nature, corporels ou incorporels, mobiliers ou immobiliers, acquis par quelque moyen que ce soit et des documents ou instruments juridiques sous quelque forme que ce soit, y compris sous forme électronique ou numérique, qui attestent un droit de propriété ou un intérêt sur ces biens et notamment les crédits bancaires, les chèques de voyage, les chèques bancaires, les mandats, les actions, les titres, les obligations, les traites et les lettres de crédit, sans que cette énumération soit limitative. »

3. Principes de base de la prévention du blanchiment de capitaux et du financement du terrorisme

Article 6 de la loi

Les organismes et personnes visés aux articles 2, § 1er, 3 et 4 concourent pleinement à l'application de la présente loi par la mise en œuvre des moyens requis pour l'identification des actes de blanchiment de capitaux et de financement du terrorisme.

Cette obligation générale de coopérer à la lutte contre le blanchiment d'argent et le financement du terrorisme se décline en diverses obligations plus détaillées, notamment:

- l'obligation d'identifier et de vérifier l'identité des clients et des personnes pour lesquelles, le cas échéant, les clients agissent (« bénéficiaires effectifs »);
- l'obligation de conserver les documents liés à l'identification et aux opérations effectuées;
- l'obligation d'exercer une vigilance constante à l'égard des relations d'affaires que les organismes entretiennent avec leurs clients et des opérations conclues tant avec leurs clients habituels qu'occasionnels;
- l'obligation d'attacher une attention particulière aux opérations atypiques des clients et de les analyser afin de déterminer si elles sont entachées de soupçons de blanchiment de capitaux ou de financement du terrorisme;
- l'obligation de coopérer activement et utilement avec la Cellule de traitement des informations financières en lui communiquant toutes les opérations et tous les faits suspects détectés et en répondant à ses demandes d'informations.

Satisfaire à l'ensemble de ces obligations requiert, plus généralement:

- que les établissements disposent d'une organisation administrative et de procédures de contrôle interne adéquates, incluant la désignation d'un responsable; et
- que les membres de leur personnel ou les personnes qui les représentent en qualité d'indépendants disposent d'une honorabilité adéquate en fonction des risques liés à leurs tâches et fonctions, et qu'ils soient adéquatement sensibilisés et formés en la matière de manière à pouvoir coopérer constructivement à la prévention.

Indépendamment du respect des dispositions de la loi, la prévention du blanchiment de capitaux et du financement du terrorisme s'impose également au regard des exigences de gestion saine et prudente et, plus précisément, au regard de la gestion du risque de réputation.

4. Identification et vérification de l'identité des clients, des mandataires et des bénéficiaires effectifs

4.1. Principes généraux

4.1.1. Portée et nature juridique de l'obligation d'identifier les clients et bénéficiaires effectifs et de vérifier leur identité

L'article 7 de la loi et les articles 4 à 13 du règlement définissent l'obligation d'identifier les clients et leurs mandataires et de vérifier leur identité; l'article 8 de la loi et les articles 14 à 20 du règlement définissent ces mêmes obligations en ce qui concerne les bénéficiaires effectifs.

Au sens de ces dispositions, « identifier » le client, son mandataire ou ses bénéficiaires effectifs signifie prendre connaissance des données d'identification de ces personnes.

« Vérifier l'identité » de ces personnes consiste à confronter ces données d'identification à une source fiable d'information apte à les confirmer ou à les infirmer (un « document probant »).

L'obligation d'identifier les clients, leurs mandataires et leurs bénéficiaires effectifs est une obligation de résultat. Sauf dans le cas de dispenses d'identification prévues par ou en vertu de l'article 11 de la loi (cf. section 4.5. infra), cette obligation doit être remplie indépendamment de toute considération concernant le niveau de risque que l'organisme financier estime attaché à la personnalité du client, du mandataire ou des bénéficiaires effectifs, à la relation d'affaires à nouer ou à l'opération à réaliser. Il en va de même en ce qui concerne l'obligation de vérifier l'identité des clients et de leurs mandataires au moyen de documents probants.

L'obligation de vérifier l'identité des bénéficiaires effectifs requiert quant à elle que les organismes financiers mettent effectivement en œuvre les moyens nécessaires à cet effet, et que ces moyens soient proportionnés au niveau de risque que l'organisme financier estime attaché à la personnalité du client, de son ou ses mandataires, ou de ses bénéficiaires effectifs, à la relation d'affaires à nouer, ou à l'opération à réaliser.

Par ailleurs, la loi du 11 janvier 1993 est d'ordre public. Outre les obligations qu'elle énonce en ce qui concerne l'identification des clients, mandataires et bénéficiaires effectifs (art. 7 et 8), elle requiert également des organismes qui y sont assujettis qu'ils acquièrent une connaissance suffisante de leurs clients pour être en mesure de remplir de manière effective et satisfaisante leurs devoirs de vigilance constante (article 14, § 1er, alinéa 1er, de la loi *:* « *... s'assurer que [les opérations du client] sont cohérentes avec la connaissance qu'ils ont de leur client, de ses activités commerciales, de son profil de risque et, lorsque cela est nécessaire, de l'origine des fonds »).* Elle impose également aux organismes d'attacher une attention particulière aux opérations particulièrement susceptibles d'être liées au blanchiment de capitaux ou au financement du terrorisme, notamment « *de par la qualité des personnes impliquées*» (article 14, alinéa 2, de la loi). Le règlement fixe les modalités de ces obligations en vertu d'une disposition spécifique de la loi (article 38 de celle-ci). Dès lors, les organismes financiers sont légalement habilités à prendre connaissance de toutes informations adéquates et utiles concernant leurs clients, dans le respect des dispositions légales relatives à la protection de la vie privée, mais sans que ces dispositions ne constituent un empêchement à la collecte et au traitement de ces informations conformément à ce que requiert la loi du 11 janvier 1993.

4.1.2. Moment de l'identification

Article 3 du règlement

Les organismes n'entrent pas en relations d'affaires avec leurs clients ni n'exécutent des opérations occasionnelles pour lesquelles ils les sollicitent avant d'avoir satisfait à leurs obligations de vigilance conformément aux articles 7 et 8 de la loi et aux dispositions du présent règlement.

Par dérogation à l'alinéa 1er, les organismes peuvent, dans des circonstances particulières que leurs procédures internes énumèrent limitativement, et dans lesquelles il est nécessaire de ne pas interrompre l'exercice des activités, vérifier l'identité des personnes impliquées dans une relation d'affaires dans le courant de l'établissement de cette relation d'affaires, pour autant que les conditions suivantes soient réunies :

- *la relation d'affaires présente un faible risque de blanchiment d'argent ou de financement du terrorisme, compte tenu de sa nature et des qualités des personnes impliquées;*

- *la vérification de l'identité des personnes impliquées est effectuée, conformément aux articles 7 et 8 de la loi et aux dispositions du présent règlement, dans les plus brefs délais après le premier contact avec le client;*
- *les activités exercées en relation avec le client font l'objet d'une vigilance accrue jusqu'à ce que l'identité de toutes les personnes impliquées ait été vérifiée, de sorte que toute anomalie, en ce compris l'impossibilité de vérifier dans les plus brefs délais l'identité des personnes impliquées dans la relation d'affaires, fait l'objet d'un rapport interne visé à l'article 14, § 2, de la loi.*

Par dérogation à l'alinéa 1er, les établissements de crédit peuvent, dans les cas que leurs procédures internes énumèrent limitativement, ouvrir un compte bancaire au nom d'un client avant que l'identité de celui-ci ou de ses bénéficiaires effectifs ait pu être vérifiée conformément aux articles 7 et 8 de la loi, pour autant que les conditions suivantes soient réunies :

- *aucune opération de débit n'est effectuée au départ dudit compte par le client ou en son nom avant que l'identité des personnes concernées ait pu être vérifiée conformément aux articles 7 et 8 de la loi;*
- *la vérification de l'identité des personnes impliquées est effectuée, conformément aux articles 7 et 8 de la loi et aux dispositions du présent règlement, dans les plus brefs délais après le premier contact avec le client;*
- *le fonctionnement du compte bancaire et le processus de vérification de l'identité des personnes concernées conformément aux articles 7 et 8 de la loi font l'objet d'une vigilance accrue de sorte que toute anomalie, en ce compris l'impossibilité de vérifier l'identité de personnes concernées dans le délai prescrit par les règles internes, fasse l'objet d'un rapport interne visé à l'article 14, § 2, de la loi.*

Les règles internes définissent des mesures appropriées garantissant que les conditions énoncées aux alinéas 2 et 3 sont remplies.

En règle générale, l'identification et la vérification de l'identité du client, de ses mandataires et de ses bénéficiaires effectifs doivent être effectuées au plus tard au moment où la relation d'affaires est nouée ou l'opération réalisée.

Cette règle ne souffre pas d'exception en ce qui concerne l'obligation d'identifier le client souhaitant réaliser une opération occasionnelle et de vérifier son identité. Certains aménagements de la règle générale sont cependant prévus par le règlement dans le cas de l'établissement de relations d'affaires.

Ainsi, dans le cadre de la conclusion d'un contrat d'assurance-vie, l'identification et la vérification de l'identité du preneur d'assurance, de ses mandataires et de ses bénéficiaires effectifs (p.ex. ses actionnaires importants, ses administrateurs...) doivent en règle générale être effectuées au moment de la souscription. Toutefois, l'article 20, alinéa 1er, du règlement autorise que l'identification et la vérification de l'identité du bénéficiaire à qui la prestation prévue par le contrat d'assurance-vie sera payée soient reportées jusqu'à l'époque où il sollicite le paiement de la prestation (Cf. section 4.4.4.3 infra).

D'autre part, dans des situations qui ne présentent que de faibles risques de blanchiment de capitaux ou de financement du terrorisme, et dans lesquelles l'accomplissement complet des obligations de vérification de l'identité des personnes impliquées (client, mandataires et bénéficiaires effectifs) préalablement à l'exécution de toute opération serait de nature à compromettre les objectifs économiques ou commerciaux de ces opérations, la politique d'acceptation des clients de l'organisme peut prévoir, conformément à l'article 3, alinéa 2, du règlement, qui fait usage de la faculté laissée aux Etats Membres par l'article 9.2 de la Directive 2005/60/CE du 26 octobre 2005, que cette vérification peut être effectuée dans le courant de l'établissement de la relation d'affaires, pour autant que l'ensemble des conditions énumérées par cette disposition du règlement soient rencontrées.

Cette faculté pourrait par exemple trouver à s'appliquer dans le cadre d'activités financières spécifiques exercées en relation avec des clients professionnels et qui, dans la pratique, ne permettent pas que la vérification de l'identité de la contrepartie soit complètement réalisée avant que les premières opérations soient effectuées.

De même, l'article 3, alinéa 3, du règlement, qui fait usage de la faculté laissée aux Etats Membres par l'article 9.4 de la Directive 2005/60/CE du 26 octobre 2005, prévoit une possibilité de report, dans le respect de certaines conditions, de la vérification de l'identité du client et de ses bénéficiaires effectifs après l'ouverture d'un compte bancaire. Cette disposition pourrait notamment être utilisée dans le cadre de la procédure d'ouverture de comptes à distance, notamment par Internet, et permettre que l'ouverture d'un tel compte nécessite un versement initial du client au départ d'un autre compte bancaire ouvert à

son nom, sans attendre que son identité et celles de ses mandataires ou bénéficiaires effectifs aient pu être vérifiées.

Dans toutes ces hypothèses, il importe cependant de s'assurer préalablement que ces situations ne présentent que de faibles risques de blanchiment de capitaux ou de financement du terrorisme, et de veiller à l'application d'un encadrement strict qui vise à parfaire les devoirs de vigilance requis par la loi dans les plus brefs délais, d'une part, et à éviter, d'autre part, que l'absence de vérification de l'identité des personnes impliquées ne puisse faciliter l'exécution d'opérations de blanchiment de capitaux ou de financement du terrorisme.

Il appartient à chaque établissement souhaitant recourir à cette faculté d'en définir préalablement, dans le cadre de sa procédure d'acceptation des clients (cf. chapitre 5 infra), les cas admissibles d'application et les modalités précises, sous le contrôle et la responsabilité du responsable de la prévention du blanchiment de capitaux et du financement du terrorisme.

Généralement, l'encadrement spécifique de la relation d'affaires dans l'attente de la vérification de l'identité des personnes impliquées devrait comprendre un ensemble de mesures cohérentes limitant drastiquement pendant cette période les possibilités offertes au client dans le cadre de la relation d'affaires. Pourraient ainsi par exemple être prises en considération le report de la liquidation des opérations, la limitation des sources d'alimentation du compte ouvert à un seul autre compte bancaire ouvert au nom du client auprès d'un établissement de crédit établi dans l'Espace Economique Européen ou dans un pays tiers équivalent, etc.

De plus, pendant la période précédant l'achèvement des devoirs de vigilance, la relation d'affaires concernée doit faire l'objet d'une vigilance particulièrement attentive, afin que toute anomalie dans son fonctionnement ou dans le processus de vérification fasse l'objet d'un examen particulier du responsable de la lutte contre le blanchiment de capitaux et le financement du terrorisme en vue de déterminer s'il y a lieu de procéder à une déclaration de soupçons à la Cellule de traitement des informations financières, conformément aux articles 23 et suivants de la loi.

4.1.3. Impossibilité d'identifier ou de vérifier l'identité

Article 7, § 4, de la loi

Lorsque les organismes et les personnes visés aux articles 2, § 1er, et 3 ne peuvent accomplir leur devoir de vigilance conformément aux §§ 1er, 2 et 3 ci-dessus, ils ne peuvent ni nouer ou maintenir une relation d'affaires, ni effectuer une opération pour le client. Dans ce cas, ils déterminent s'il y a lieu d'en informer la Cellule de traitement des informations financières, conformément aux articles 23 à 28.

Article 8, § 4, de la loi

Lorsque les organismes et les personnes visés aux articles 2, § 1er et 3 ne peuvent accomplir leur devoir de vigilance conformément aux § 1er et 2, ils ne peuvent ni nouer ou maintenir une relation d'affaires, ni effectuer une opération pour le client. Il en va de même lorsque les clients visés au § 3 restent en défaut de leur fournir les informations requises ou leur fournissent des informations qui n'apparaissent pas pertinentes ou vraisemblables. Les organismes et personnes visés déterminent dans ces cas s'il y a lieu d'informer la Cellule de traitement des informations financières, conformément aux articles 23 à 28.

La portée des interdictions énoncées aux articles 7, § 4, et 8, § 4, de la loi ne peut pas être dissociée de celle des obligations générales d'identification et de vérification de l'identité des clients, mandataires et bénéficiaires effectifs qui constituent les devoirs de vigilance. Les obligations d'identification et de vérification de l'identité étant pour la plupart des obligations de résultat, l'interdiction légale sort généralement ses effets dès l'instant où il apparaît que l'identification ou la vérification ne peut pas être opérée. Toutefois, l'obligation de vérifier l'identité des bénéficiaires effectifs est quant à elle une obligation de moyens. Dans ce cas, l'interdiction de nouer ou de maintenir la relation d'affaires ou d'effectuer l'opération souhaitée par le client sort ses effets lorsque l'organisme financier se trouve dans l'impossibilité, pour quelque raison que ce soit, de mettre en œuvre les moyens proportionnés au risque qui sont requis par la loi (Cf. section 4.4.4.1 infra).

L'entrée en application de ces interdictions légales dépend également du moment où il est requis que les obligations d'identification et de vérification de l'identité soient satisfaites (cf. section 4.1.2 supra). Ainsi, par exemple, les devoirs d'identification et de vérification de l'identité d'un client constituant en règle générale un préalable à la relation d'affaires ou à l'opération souhaitée, l'article 7, § 4, de la loi interdit en principe de nouer cette relation d'affaires ou de réaliser cette opération tant que ces devoirs n'ont pas pu être pleinement accomplis.

Lorsqu'il apparaît qu'une mise à jour des données d'identification d'un client s'impose par application de l'article 7, § 3, de la loi, le § 4 du même article impose de mettre un terme à la relation d'affaires en cours avec ce client dès qu'il apparaît que la nouvelle identification ou la nouvelle vérification de son identité ne peuvent pas être accomplies. Il en va de même dans les cas où, conformément à l'article 3, alinéa 2 ou alinéa 3, du règlement ou à son article 20, alinéa 1er, (cf. section 4.1.2 supra), la vérification de l'identité d'un client, de ses mandataires ou de ses bénéficiaires effectifs n'a pas été complètement effectuée avant l'entrée en vigueur de la relation d'affaires, et où il apparaît par la suite que l'organisme financier se trouve dans l'impossibilité de remplir complètement ses obligations.

En ce qui concerne les entreprises d'assurance-vie, l'obligation légale de mettre fin à une relation d'affaires lorsque les devoirs de vigilance ne peuvent pas être accomplis entre en contradiction avec les dispositions de l'article 30 de la loi du 25 juin 1992 sur le contrat d'assurance terrestre, qui interdit la résiliation des contrats d'assurance-vie par ces entreprises. Toutefois, considérant notamment que la loi du 11 janvier 1993 est d'ordre public, alors que les dispositions de la loi du 25 juin 1992 sont impératives, que la loi du 12 janvier 2004 ayant introduit les dispositions concernées dans la loi du 11 janvier 1993 est postérieure à la loi du 25 juin 1992 et a donc introduit une exception aux dispositions de l'article 30 de cette dernière, et qu'enfin, la loi du 11 janvier 1993 contient une disposition spéciale dérogeant à la règle générale énoncée par la loi du 25 juin 1992, la CBFA estime que la contradiction relevée doit être résolue au profit de l'application de l'interdiction de maintenir la relation d'affaires prévue par la loi du 11 janvier 1993.

Au-delà de l'interdiction de nouer ou de maintenir une relation d'affaires ou d'effectuer une opération avec le client dans les circonstances visées, ce fait doit être porté à la connaissance du responsable de la prévention du blanchiment de capitaux afin qu'il détermine si les circonstances justifient qu'une déclaration de soupçon soit adressée à la CTIF (cf. infra, chapitre 9).

4.2. Identification et vérification de l'identité des clients

4.2.1. Notion de « client »

4.2.1.1. Définition générale

La notion de client n'est pas définie par la loi. Il convient donc de l'interpréter largement, dans le sens courant du terme. Peut dès lors être considéré comme un client au sens de la loi toute personne physique ou morale, ou toute structure juridique sans personnalité juridique faisant appel à un organisme financier pour obtenir la fourniture, généralement à titre onéreux, d'un service ou d'un produit financier.

4.2.1.2. Indivisions et droits démembrés

Article 10 du règlement

Lorsque le client est une indivision, les obligations d'identification du client et de vérification de son identité conformément à l'article 7, § 1er, de la loi portent sur chaque indivisaire. Dans le cas de droits démembrés, ces obligations portent sur les usufruitiers, emphytéotes ou superficiaires.

Ne sont pas à considérer comme indivisions au sens de cet article les trusts, associations de fait, fiducies ou autres structures juridiques sans personnalité juridique, qui sont visées, notamment, à l'article 9 du règlement [14].

4.2.1.3. Contrats d'assurance-vie

Dans le cadre de la conclusion d'un contrat d'assurance-vie, sans préjudice de l'identification du ou des bénéficiaires du contrat en qualité de bénéficiaires effectifs (cf. infra, section 4.4.4.3 infra), seul le preneur d'assurance a la qualité de client et doit être identifié en cette qualité, à l'exclusion, le cas échéant, de l'assuré sur la tête duquel le contrat est conclu.

Si, en cours de contrat, le preneur d'assurance change, le nouveau preneur d'assurance doit être dûment identifié en qualité de client.

14 Voir aussi l'article 20 du règlement et le point 5.3.1. ci-dessous.

4.2.2. Situations dans lesquelles le client doit être identifié

4.2.2.1. Relations d'affaires

4.2.2.1.1. Relations contractuelles ou factuelles

Article 7, § 1er, alinéa 1er, 1°, de la loi

Les organismes et les personnes visés aux articles 2, § 1er et 3 doivent identifier leurs clients et vérifier leur identité, au moyen d'un document probant, dont il est pris copie, sur support papier ou électronique, lorsque :

1° le client souhaite nouer des relations d'affaires qui feront de lui un client habituel ;
(...)

Article 4 du règlement

Une relation d'affaires est nouée au sens de l'article 7 § 1er, alinéa 1er, 1°, de la loi lorsqu'un organisme et un client concluent un contrat en exécution duquel plusieurs opérations successives seront réalisées entre eux pendant une durée déterminée ou indéterminée, ou qui crée des obligations continues.

Une relation d'affaires est également nouée au sens de l'article 7, § 1er, alinéa 1er, 1°, de la loi lorsqu'en dehors de la conclusion d'un contrat visé à l'alinéa 1er du présent article, un client sollicite de manière régulière et répétée l'intervention d'un même organisme pour la réalisation d'opérations financières distinctes et successives.

Le « *Level Playing Field* » de l'Association Belge des Banques du 17 juillet 2003 relatif au « système des comptes-clients individuels » prévoit l'ouverture de tels comptes pour la réalisation de toute opération pour laquelle une banque ou une société de bourse est sollicitée par un client « de passage ».

S'agissant néanmoins de réaliser avec le client une opération ponctuelle, et l'ouverture du compte-client individuel ayant pour seul objectif de rendre techniquement possible l'opération demandée par le client et non de nouer avec lui une relation durable, la CBFA estime que l'obligation d'identifier ce client repose sur les dispositions de l'article 7, § 1er, alinéa 1er, 2° de la loi, et non sur celles de l'article 7, § 1er, alinéa 1er, 1° de la loi.

Dans le secteur des assurances, une opération d'assurance est toujours une opération qui mène à la souscription d'un contrat non instantané, et donc à une relation d'affaires qui requiert l'identification et la vérification de l'identité du client conformément à l'article 7, § 1er, alinéa 1er, 1°, de la loi.

Dès lors qu'un client a été identifié à l'occasion de l'ouverture d'une relation d'affaires, cette identification couvre l'ensemble des opérations réalisées dans le cadre de cette relation.

Ainsi, par exemple, lorsqu'un client souhaite contracter simultanément un prêt hypothécaire et un contrat d'assurance-vie qui est lié au prêt hypothécaire (assurance du solde restant dû ou assurance-vie mixte affectée à la reconstitution de l'emprunt) auprès d'un même organisme financier, une relation d'affaires est nouée entre le client et l'organisme financier, de sorte que l'identification et la vérification de l'identité du client au moment de nouer cette relation d'affaires vaudra tant pour l'un que pour l'autre contrat souhaité par le client.

Cette identification unique se complète cependant des devoirs de vigilance constante de l'organisme à l'égard de ce qu'il connaît de son client (cf. section 6.1., infra).

4.2.2.1.2. Comptes anonymes et numérotés

Article 5 du règlement

En exécution de leurs obligations d'identification des clients en vertu de l'article 7, § 1er, alinéa 1er, 1°, de la loi, les organismes ne peuvent ouvrir à des clients des comptes anonymes ou sous de faux noms ou pseudonymes. Ils prennent toutes les mesures appropriées pour s'assurer du respect de cette interdiction.

L'ouverture aux clients de comptes numérotés n'est autorisée que dans le respect de règles spécifiques arrêtées par l'organisme pour fixer les conditions dans lesquelles ces comptes peuvent être ouverts et en préciser les modalités de fonctionnement, et pour autant que ces conditions et modalités ne fassent pas obstacle à l'application des dispositions des articles 7, 8, 12, 13, 14 et 15 de la loi, ni à l'application du présent règlement.

Dès lors que l'entrée en relation avec un client requiert son identification en vertu de l'article 7, § 1er, de la loi, il ne peut être admis que des comptes anonymes soient ouverts, c'est-à-dire des comptes dont l'identité du titulaire n'est pas connue. Il en va de même des comptes qui sont ouverts sous des noms ne

correspondant pas à l'identité réelle du client. Cette interdiction ne s'oppose cependant pas à l'adjonction à un nom de mentions correspondant à une réalité légitime. Ainsi en est-il notamment d'une dénomination commerciale, d'une subdivision du client ou d'un nom identifiant collectivement des clients en situation d'indivision. Toutefois, l'organisme veillera soigneusement à ce que l'adjonction soit aisément identifiable en tant que telle, et à ce qu'elle ne puisse en aucun cas induire en erreur quant à l'identité du client.

La pratique consistant, pour des raisons de confidentialité souhaitée par le client, à limiter le nombre de personnes au sein de l'organisme qui disposent des informations leur permettant de connaître l'identité du client concerné, notamment par le fait que les extraits de compte et autres documents sont uniquement établis en mentionnant le seul numéro de compte, peut être admise pour autant que cette pratique ne fasse pas obstacle à l'application des règles d'identification et aux autres dispositifs de prévention du blanchiment de capitaux et du financement du terrorisme. Dans ce cas dès lors, l'identité du client doit être connue par le responsable de la prévention du blanchiment de capitaux et du financement du terrorisme et par les personnes au sein de l'organisme pour qui cette connaissance est nécessaire pour l'exercice effectif du devoir de vigilance (cf. chapitre 6 infra).

4.2.2.2. Opérations occasionnelles

Article 7, § 1er, alinéa 1er, 2°, de la loi

Les organismes et les personnes visés aux articles 2, § 1er, et 3 doivent identifier leurs clients et vérifier leur identité, au moyen d'un document probant, dont il est pris copie, sur support papier ou électronique, lorsque :

(...)

2° le client souhaite réaliser, en dehors des relations d'affaires visées au 1° ci-dessus, une opération :

a. dont le montant atteint ou excède 10.000 euros, qu'elle soit effectuée en une seule ou en plusieurs opérations entre lesquelles semble exister un lien, ou

b. qui consiste en un virement de fonds au sens du 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;

(...)

4.2.2.2.1. Opérations dont le montant atteint ou excède 10.000 €, réalisées en dehors d'une relation d'affaires

L'article 7, § 1er, 2°, de la loi précise explicitement que les clients ne doivent être identifiés et leur identité vérifiée en vue de la réalisation d'opérations que lorsque celles-ci ne sont pas comprises dans une relation d'affaires nouée avec le même client. Dans ce cas, en effet, et sans préjudice des obligations de mise à jour des données (cf. infra, section 6.1.3), l'identification et la vérification de l'identité du client qui ont été opérées en vue de nouer ladite relation d'affaires couvrent l'ensemble des opérations effectuées dans le cadre de cette relation d'affaires.

Ainsi, par exemple, lorsqu'un client souhaite contracter auprès d'une entreprise d'assurance-vie un contrat de prêt hypothécaire, une relation d'affaires est nouée entre le client et l'entreprise, et le client doit être identifié à cette occasion. Cette identification vaudra également pour toute opération à réaliser par la suite dans le cadre de cette relation d'affaires. Le client ne doit donc plus être à nouveau identifié lorsque, dans le cadre de cette relation d'affaires, il conclut un contrat d'assurance-vie qui est lié au prêt hypothécaire (assurance du solde restant dû ou assurance-vie mixte affectée à la reconstitution de l'emprunt).

Il est à souligner par ailleurs que, d'une manière générale, la réception et la transmission d'ordres par un organisme financier en vue notamment de la souscription de titres en dehors de toute autre relation d'affaires avec le client constituent des opérations occasionnelles visées à l'article 7, § 1er, alinéa 1er, 2°, a), de la loi. Tel est également le cas lorsque ces services sont offerts directement aux souscripteurs par l'OPC lui-même, sans intervention d'une entité tierce. La CBFA est en effet d'avis que la relation entre le souscripteur et l'OPC qui résulte de la souscription ne peut pas être assimilée à une relation d'affaires entre un organisme financier et un client, dans la mesure où elle s'analyse comme une relation d'actionnariat.

Il convient aussi de préciser que doit également être identifiée, en vertu de l'article 7, § 1er, alinéa 1er, 2°, a), de la loi, la personne qui souhaite effectuer un dépôt en espèces de plus de 10.000 € sur un compte dont il n'est pas titulaire. Cette précision revêt une importance particulière dans la mesure où l'interdiction

des paiements en espèces de plus de 15.000 € prévue à l'article 20 de la loi peut conduire à la multiplication de ce type d'opérations.

4.2.2.2.2. Virements électroniques de fonds

Lorsqu'un client occasionnel sollicite un organisme financier pour réaliser un virement électronique de fonds en dehors de toute relation d'affaires (et notamment, sans que ce virement ne soit effectué au départ d'un compte ouvert au nom du client), l'organisme financier est tenu d'identifier ce client et de vérifier son identité.

Satisfaire à cette obligation légale est en outre indispensable pour que l'organisme financier soit en mesure de satisfaire à son obligation de joindre au virement des fonds les informations complètes et vérifiées concernant le donneur d'ordre, comme requis par les articles 4 et 5 du 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 [15] (cf. section 8.1., infra,).

A cet égard, il convient cependant de noter que l'article 7, § 1er, alinéa 2, de la loi fait usage de l'option prévue à l'article 3.6 de ce règlement européen :

> ***Article 7, § 1er, alinéa 2, de la loi***
>
> *Pour l'application de l'alinéa 1er, 2°, b, ne constitue pas un virement de fonds au sens du 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, le virement d'un montant inférieur ou égal à 1.000 euros, effectué en Belgique, sur le compte du destinataire du paiement, à condition :*
>
> *1° que le virement constitue un paiement effectué en exécution de la fourniture de biens ou de services entre le donneur d'ordre et le destinataire;*
>
> *2° que le compte du destinataire soit ouvert afin de permettre le paiement de la fourniture de biens ou de services ;*
>
> *3° que le prestataire de services de paiement du destinataire soit soumis aux obligations de la présente loi; et*
>
> *4° que ce prestataire de services de paiement soit capable, grâce à un code unique d'identification, de remonter jusqu'au donneur d'ordre, par l'intermédiaire du destinataire du paiement.*

Cette disposition vise à faire exception aux obligations d'identification et de vérification de l'identité des clients dans des situations particulièrement peu susceptibles de présenter des risques de blanchiment de capitaux ou de financement du terrorisme. Sont par exemple visés les paiements de factures de consommation d'eau, de gaz ou d'électricité effectués par des personnes ne disposant pas d'un compte bancaire au départ duquel effectuer un virement, et qui remettent le montant en espèces de leur facture aux guichets d'un organisme financier pour que celui-ci le vire électroniquement sur le compte ouvert par le prestataire de services concerné pour recevoir ces paiements.

4.2.2.3. Soupçons de blanchiment de capitaux ou de financement du terrorisme

> ***Article 7, § 1er, alinéa 1er, 3°, de la loi***
>
> *Les organismes et les personnes visés aux articles 2, § 1er, et 3 doivent identifier leurs clients et vérifier leur identité, au moyen d'un document probant, dont il est pris copie, sur support papier ou électronique, lorsque :*
>
> *(...)*
>
> *3° il y a soupçon de blanchiment de capitaux ou de financement du terrorisme, en dehors des cas visés aux 1° et 2° ;*
>
> *(...)*

L'article 7, § 1er, alinéa 1er, 3°, de la loi énonce une exception aux dispenses d'identification et de vérification de l'identité des clients qui sont prévues à l'article 7, § 1er, alinéa 2, (cf. section 4.2.2.2 supra) ou à l'article 11 de la loi (cf. section 4.5 infra). Ces dispenses ne peuvent en effet pas être invoquées dès l'instant où surgissent des soupçons de blanchiment de capitaux ou de financement du terrorisme. Si de tels soupçons apparaissent après que la relation d'affaires ait été nouée en faisant application d'une dispense d'identification, il appartient à l'organisme financier de prendre dans les plus brefs délais toutes

15 JOCE L345 du 8 décembre 2006, pp. 1 à 9.

les mesures requises d'identification et de vérification de l'identité de ce client et de ses éventuels mandataires et bénéficiaires effectifs.

De même, lorsqu'un organisme financier est sollicité pour la réalisation d'une opération occasionnelle d'un montant inférieur à 10.000 €, il s'impose d'identifier et de vérifier l'identité de ce client et de ses éventuels mandataires et bénéficiaires effectifs, quel que soit le montant de l'opération souhaitée, si l'organisme financier soupçonne qu'elle pourrait être liée au blanchiment de capitaux ou au financement du terrorisme.

Si l'organisme financier ne peut accomplir ses devoirs de vigilance, il ne peut maintenir la relation d'affaires avec le client ni effectuer l'opération (articles 7, § 4, et 8, § 4, de la loi - cf. section 4.1.3., supra).

De plus, puisqu'il existe par hypothèse des soupçons de blanchiment de capitaux ou de financement du terrorisme, les dispositions relatives à la déclaration des opérations ou des faits suspects trouvent à s'appliquer (cf. chapitre 7, infra).

4.2.2.4. Doutes quant à la véracité ou à l'exactitude des données d'identification d'un client existant

Article 7, § 1er, alinéa 1er, 4°, de la loi

Les organismes et les personnes visés aux articles 2, § 1er, et 3 doivent identifier leurs clients et vérifier leur identité au moyen d'un document probant dont il est pris copie, sur support papier ou électronique, lorsque :

(...)

4° il existe des doutes quant à la véracité ou à l'exactitude des données d'identification au sujet d'un client déjà identifié.

Article 6 du règlement

L'identification d'un client est requise en vertu de l'article 7, § 1er, alinéa 1er, 4°, de la loi lorsque :

1° postérieurement à l'identification du client concerné en vue de nouer avec lui une relation d'affaires, apparaissent des raisons de croire que les données d'identification qu'il a fournies à cette occasion étaient inexactes ou mensongères;

2° il existe des raisons de douter que la personne qui souhaite réaliser une opération dans le cadre d'une relation d'affaires antérieurement nouée est effectivement le client identifié en vue de cette relation d'affaires ou son mandataire autorisé et identifié.

Dans les hypothèses visées par ces dispositions, une nouvelle identification et une nouvelle vérification de l'identité du client et de ses éventuels mandataires et bénéficiaires effectifs doivent être immédiatement effectuées.

L'urgence d'y procéder dans ces hypothèses constitue une différence notable par rapport aux mesures de mise à jour des données d'identification des clients qui sont requises par l'article 7, § 3 de la loi, et dont le degré d'urgence peut être défini en fonction du risque (Cf. section 4.8., infra).

Dès lors, si le client refuse de se soumettre à la nouvelle identification requise par application de l'article 7, § 1er, alinéa 1er, 4°, de la loi, ou s'il tarde excessivement ou de manière suspecte à s'y soumettre, il y a lieu d'appliquer l'article 7, § 4, de la loi, qui interdit de maintenir la relation d'affaires lorsque les devoirs de vigilance ne peuvent être accomplis.

Dans ces cas, de même que lorsque les soupçons d'informations mensongères ou de substitution de personne semblent fondés, il y a lieu d'établir un rapport écrit tel que requis par l'article 14, § 2, de la loi et, le cas échéant, de procéder à une communication à la Cellule de traitement des informations financières par application des articles 23 à 25 de la loi.

Une attitude identique est également requise si, au cours de l'identification initiale d'un client demandant à nouer une relation d'affaires ou souhaitant réaliser une opération occasionnelle, il existe des raisons de douter de l'exactitude ou de la véracité des données d'identification fournies par le client et si celui-ci n'apparaît pas de bonne foi. Il en va de même si, postérieurement à la réalisation d'une opération occasionnelle, l'établissement a des raisons de croire que les éléments d'identification qui lui ont été fournis par le client concerné sont inexacts ou mensongers.

4.2.3. Données d'identification

4.2.3.1. Données relatives aux personnes physiques

Article 7, § 1er, alinéa 3, de la loi

Pour les personnes physiques, l'identification et la vérification portent sur le nom, le prénom, le lieu et la date de naissance. (...)

Afin de renforcer la fiabilité de l'identification des personnes physiques, la loi du 18 janvier 2010 a modifié la liste des données d'identification les concernant en y incluant le lieu et la date de naissance, ces informations pouvant de plus être aisément vérifiées au moyen de documents probants (carte d'identité, passeport ou Registre national : cf. section 4.2.4., infra).

En ce qui concerne les clients avec lesquels les organismes financiers entretiennent des relations d'affaires à la date d'entrée en vigueur de la loi du 18 janvier 2010, l'article 43, § 1er de celle-ci prévoit une disposition transitoire en vertu de laquelle le lieu et la date de naissance doit être identifiée et vérifiée au moyen d'un document probant dans un délai déterminé en fonction du risque, et au plus tard cinq ans après l'entrée en vigueur de la loi. Cette obligation de compléter l'identification et la vérification de l'identité des clients existants ne s'applique pas lorsque l'organisme financier dispose d'ores et déjà des informations relatives au lieu et à la date de naissance d'un client existant, du fait qu'elles sont mentionnées sur la copie, qu'il a conservée, du document probant au moyen duquel il a vérifié l'identité dudit client avant l'entrée en vigueur de la loi du 18 janvier 2010.

4.2.3.2. Données relatives aux personnes morales et aux constructions juridiques

Article 7, § 1er, alinéa 4, de la loi

Pour les personnes morales, les trusts, les fiducies et les constructions juridiques similaires, l'identification et la vérification portent sur la dénomination sociale, le siège social, les administrateurs et la connaissance des dispositions régissant le pouvoir d'engager la personne morale, le trust, la fiducie ou la construction juridique similaire.

Article 9 du règlement

Lors de l'identification des clients qui sont des trusts, des associations de fait, des fiducies, ou toutes autres structures juridiques dénuées de personnalité juridique, les organismes prennent connaissance de l'existence, de la nature, des finalités poursuivies et des modalités de gestion et de représentation de la structure juridique concernée, et les vérifient au moyen de tous documents susceptibles de faire preuve, dont ils prennent copie.

Cette identification inclut la prise de connaissance et la vérification de la liste des personnes autorisées à exercer la gestion de ces clients, au moyen d'un document susceptible de faire preuve.

4.2.3.3. Objet et nature de la relation d'affaires

Article 7, § 1er, alinéa 5 de la loi

L'identification porte également sur l'objet et la nature envisagée de la relation d'affaires.

Article 11 du règlement

En vue de l'identification de l'objet et de la nature envisagée de la relation d'affaires, les organismes prennent connaissance et enregistrent les types d'opérations pour lesquelles le client les sollicite, ainsi que toute information adéquate permettant de déterminer la finalité de la relation d'affaires envisagée dans le chef du client.

Lorsqu'un client souhaite nouer une relation d'affaires, qu'il s'agisse d'une personne physique, d'une personne morale ou d'une construction juridique, l'identification de ce client requiert en outre que l'organisme identifie l'objet et la nature envisagée de la relation d'affaires. Il convient à cet égard de prendre connaissance des intentions du client concernant le type de relation d'affaires qu'il souhaite nouer avec l'organisme, et le type d'opérations qu'il souhaite nouer avec l'organisme dans le cadre de cette relation, ainsi que toutes informations utiles et pertinentes permettant de connaître la finalité de cette relation dans le chef du client.

L'objet et la nature d'une relation d'affaires peuvent être déterminés en se basant sur les informations préalables ou précontractuelles relatives au produit ou au service financier proposé qui sont effectivement transmises au client, pour autant que l'objet et la nature de la relation d'affaires à nouer puissent en être déduits de façon certaine, précise et univoque. Ainsi, par exemple, les entreprises d'assurance-vie et les intermédiaires non exclusifs en assurance-vie peuvent déterminer l'objet et la

nature de la relation d'affaires qu'ils nouent avec le souscripteur d'une assurance-vie en se fondant sur l'information précontractuelle comprenant la proposition d'assurance ou tout autre formulaire de souscription. De même, un établissement de crédit proposant à un client la souscription d'un produit d'épargne ne présentant aucune ambigüité quant à son objet et à sa nature peut fonder l'identification de l'objet et de la nature de la relation d'affaires à nouer avec le client sur la description du produit qui lui a été préalablement fournie. En revanche, lorsque le produit ou le service financier offert permet d'effectuer des opérations susceptibles de présenter des caractéristiques diverses, l'identification de l'objet et de la nature de la relation d'affaires requerra de recueillir auprès du client des informations plus précises et personnalisées sur ses intentions quant à l'utilisation qu'il fera de la relation d'affaires. Ces informations devront permettre à l'organisme financier d'exercer une vigilance constante effective à l'égard du client. Tel sera généralement le cas, par exemple, lors de l'ouverture de comptes courants.

4.2.4. Documents probants

Les articles 7 à 10 du règlement visent à préciser les documents probants au moyen desquels les organismes sont tenus de vérifier l'identité de leurs clients conformément à l'article 7, § 1er de la loi.

4.2.4.1. Vérification face à face de l'identité d'un client personne physique

4.2.4.1.1. Carte d'identité et passeport

Article 7, § 1er, alinéa 1er, du règlement

Lors de l'identification face-à-face des clients qui sont des personnes physiques, la vérification de leur identité conformément à l'article 7, § 1er, de la loi, doit être opérée au moyen de leur carte d'identité. S'il s'agit de personnes physiques qui résident à l'étranger, la vérification peut également être opérée au moyen de leur passeport.

Lorsque le client est une personne physique faisant l'objet d'une identification face à face, la vérification de son identité doit être effectuée, en règle générale, au moyen de ses documents officiels d'identité en cours de validité, à savoir sa carte d'identité ou, le cas échéant, son passeport s'il ne dispose pas d'une carte d'identité [16].

En ce qui concerne les personnes ayant leur domicile en Belgique, seule la carte d'identité peut en principe être acceptée. Cette règle s'applique également aux personnes résidant en Belgique qui sont titulaires d'une carte d'identité électronique. Dans des cas exceptionnels, notamment lorsque la carte d'identité du client est en cours d'émission par les autorités belges compétentes, d'autres documents émis par des autorités belges ou étrangères pourraient être admis comme documents probants dans l'attente que la vérification puisse être à nouveau opérée ultérieurement au moyen de la carte d'identité du client. Lorsque le client est un enfant mineur âgé de moins de 12 ans qui ne dispose pas encore obligatoirement d'une carte d'identité, il peut être admis de ne vérifier son identité qu'à l'époque de son 12ème anniversaire, lorsqu'une carte d'identité lui est délivrée. Cette tolérance ne fait cependant pas exception à l'obligation d'identifier le mineur d'âge concerné, ni à celle d'identifier et de vérifier l'identité de la ou des personnes autorisées à agir en son nom et pour son compte, conformément aux dispositions légales et réglementaires.

Lorsque les organismes financiers procèdent à la vérification de l'identité du client par la lecture électronique des données enregistrées sur le microprocesseur de sa carte d'identité, il s'impose de procéder également à une vérification électronique simultanée que les données figurant sur la puce sont signées électroniquement par le Registre National. A cet égard, il est recommandé que les procédures informatiques mises en œuvre soient conçues en manière telle que cette vérification soit opérée systématiquement et automatiquement, sans requérir d'intervention du préposé qui procède à l'identification, et sans qu'il ne dispose de la faculté de désactiver ce contrôle. De plus un contrôle de la conformité des données enregistrées sur la puce avec celles lisiblement mentionnées sur la carte d'identité peut s'avérer utile pour détecter d'éventuelles falsifications. Enfin, il convient de s'assurer que le certificat n'a pas été révoqué par le Registre National.

16 De plus amples informations relatives aux documents d'identité dont doivent être porteurs les étrangers sur le territoire belge peuvent être consultées sur le site internet de l'Office des Etrangers : http://www.dofi.fgov.be. Concernant les ressortissants d'autres Etats Membres de l'Espace Economique Européen, il est également renvoyé à la directive 2004/38/CE du Parlement européen et du Conseil du 29 avril 2004 relative au droit des citoyens de l'Union et des membres de leurs familles de circuler et de séjourner librement sur le territoire des États membres, modifiant le règlement (CEE) n° 1612/68 et abrogeant les directives 64/221/CEE, 68/360/CEE, 72/194/CEE, 73/148/CEE, 75/34/CEE, 75/35/CEE, 90/364/CEE, 90/365/CEE et 93/96/CEE].

4.2.4.1.2. Personnes de nationalité étrangères établies en Belgique

Article 7, § 1er, alinéa 2, du règlement

Lors de l'identification de personnes de nationalité étrangère établies en Belgique qui, en raison de leur statut légal sur le territoire belge, ne disposent pas d'une carte d'identité délivrée par les autorités belges, la vérification de leur identité peut être opérée au moyen de leur certificat d'inscription au registre des étrangers en cours de validité, ou, lorsqu'ils n'en disposent pas en raison de leur statut, au moyen d'un document en cours de validité émis par les autorités publiques belges.

En vertu de l'article 7, § 1er, alinéa 2, du règlement, l'identité des personnes de nationalité étrangère peut être valablement vérifiées au moyen du document qui leur est délivré par les autorités belges en fonction de leur statut sur le territoire belge (carte d'identité, certificat d'inscription au registre des étrangers, ainsi que les différentes annexes à l'AR du 8 octobre 1981).Cette disposition vise notamment à ne pas exclure les personnes en situation précaire sur le territoire belge de l'accès aux services financiers.

4.2.4.2. Vérification à distance de l'identité d'un client personne physique

Article 7, § 2, du règlement

Lors de l'identification à distance des clients qui sont des personnes physiques, la vérification de leur identité conformément à l'article 7, § 1er, de la loi doit être opérée:

1° au moyen de la carte d'identité électronique du client;

2° au moyen d'un certificat qualifié au sens de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification et au sens de la directive 1999/93/CE du Parlement européen et du Conseil du 13 décembre 1999 sur un cadre communautaire pour les signatures électroniques, pour autant que;

a. le certificat qualifié présenté ait été émis:
- *par un prestataire de service de certification qui est établi dans un Etat membre de l'Espace Economique Européen et qui y est accrédité conformément aux dispositions de la directive européenne relative à la signature électronique;*
- *ou par un autre prestataire service de certification qui est établi dans un Etat membre de l'Espace Economique Européen, et dont l'organisme concerné a préalablement décidé d'accepter les certificats au titre de documents probants, sur la base d'une analyse préalable et documentée de sa réputation et de ses procédures de certification;*
- *ou par un autre prestataire de service de certification établi dans un pays tiers, qui remplit les conditions fixées à l'article 16, § 2, de la loi du 9 juillet 2001 précitée, et dont l'organisme concerné a préalablement décidé d'accepter les certificats au titre de documents probants, sur la base d'une analyse préalable et documentée de sa réputation et de ses procédures de certification;*

b. la délivrance du certificat qualifié d'identification ait eu lieu sur la base d'une procédure requérant une identification face-à-face du client par le prestataire de service de certification lui-même ou, dans le respect des procédures qu'il définit, par des personnes qu'il mandate à cet effet;

c. le certificat n'ait pas été émis sous un pseudonyme;

d. l'organisme procède instantanément, systématiquement et automatiquement à la vérification de la non péremption du certificat produit et de sa non révocation par le prestataire de service de certification émetteur;

3° ou au moyen d'une copie de la carte d'identité du client dont la véracité est vérifiée par la consultation du Registre national conformément à l'article 16, § 3, de la loi.

Lorsque la vérification de l'identité du client n'est pas opérée conformément à l'alinéa précédent, elle peut être effectuée au moyen d'une copie d'un document probant adressée par le client à l'organisme pour autant que l'identification soit opérée en vue de nouer une relation d'affaires, et pour autant que ni le client, ni la relation d'affaire ne présentent de risques particuliers de blanchiment de capitaux ou de financement du terrorisme.

Les organismes procèdent à un réexamen périodique, sur la base d'une actualisation des informations dont ils disposent, de leur décision d'accepter au titre de documents probants les certificats émis par les prestataires de service de certification visés à l'alinéa 1er, 2°, a, 2ème et 3ème tirets.

4.2.4.2.1. Principes - Prise en considération des risques particuliers

L'article 7, § 2, du règlement énumère quatre types de documents probants auxquels les organismes peuvent recourir pour procéder à la vérification de l'identité d'un client qui est identifié à distance, à savoir, sa carte d'identité électronique (belge ou étrangère), un certificat qualifié au sens de la directive européenne relative à la signature électronique, la copie d'une carte d'identité dont la véracité est vérifiée par la consultation du Registre national, ou une copie d'un document probant.

Cette diversité des documents probants admis vise à ne pas entraver outre mesure le développement des relations d'affaires et des opérations conclues à distance, notamment par le recours à l'internet.

Il convient cependant de souligner que, conformément à l'article 12, § 2, de la loi, l'identification à distance d'un client impose dans tous les cas de prendre des mesures complémentaires afin de réduire le risque de blanchiment de capitaux et de financement du terrorisme. Ces mesures sont précisées à l'article 29 du règlement et commentées plus complètement à la section 5.2.2.1 de la présente circulaire.

D'autre part, les quatre types de documents admis par cette disposition du règlement ne présentent pas des degrés égaux de fiabilité. Ainsi, notamment, si le règlement prévoit que la copie d'un document probant peut être admise sans vérification auprès du Registre national lorsque l'organisme financier ne peut ou ne souhaite pas vérifier l'identité du client au moyen de l'un des trois autres documents énumérés, la photocopie ou l'image électronique de la carte d'identité ou du passeport du client ne pourra pas être considérée comme présentant la même fiabilité que les autres documents probants. Dès lors, les mesures précitées d'encadrement complémentaires doivent se différencier pour tenir compte des niveaux différents de risque qui découlent de la nature du document probant au moyen duquel l'identité du client a été vérifiée. C'est dans cette perspective notamment qu'une copie de document probant non vérifiée au Registre national ne peut être admise que dans l'hypothèse où l'identification est opérée dans le but de nouer avec le client une relation d'affaires, dans le courant de laquelle des mesures pourront être prises pour raffermir la qualité de la connaissance de ce client. En revanche, il ne peut être admis de vérifier l'identité d'un client au moyen d'une simple copie de document probant lorsque l'identification est opérée en vue de réaliser une opération occasionnelle avec le client. L'on soulignera aussi tout particulièrement que, dans cette hypothèse, la relation d'affaires à conclure ne peut impliquer aucune manipulation d'espèces, pas même par le biais de retraits aux ATM (cf. art. 29, 5ème tiret, du règlement).

De plus, il appartient à l'organisme financier qui entend recourir à de simples copies de documents probants pour vérifier l'identité de certains clients de justifier au préalable que ni le client concerné, ni la relation d'affaires à nouer avec lui ne présentent de risques particuliers de blanchiment de capitaux ou de financement du terrorisme (cf. art. 7, § 2, alinéa 2, du règlement). La CBFA estime dès lors que cet organisme financier ne peut pas accepter la simple copie d'un document probant pour vérifier l'identité d'un client sans que sa politique d'acceptation des clients ne précise préalablement, d'une part, les catégories de relations d'affaires concernées qui ne présentent en principe pas de risques particuliers de blanchiment de capitaux ou de financement du terrorisme, et, d'autre part, les devoirs de vigilance à accomplir préalablement à l'ouverture de chaque relation d'affaire concernée pour justifier qu'aucun risque particulier de blanchiment de capitaux ou de financement du terrorisme n'est associé au client considéré.

De plus, l'article 29, 3ème tiret, impose de procéder à une nouvelle vérification de l'identité du client au moyen d'un autre document probant qu'une simple copie de carte d'identité ou de passeport, dès lors que le risque le justifie. Les procédures internes doivent dès lors imposer cette nouvelle vérification dès l'instant où, dans le courant de la relation d'affaire, l'exercice de la vigilance constante à l'égard de celle-ci fait apparaître qu'un risque particulier de blanchiment de capitaux ou de financement du terrorisme est associé au client ou à la relation d'affaires.

4.2.4.2.2. Les cartes d'identités électroniques

Les mêmes observations que celles formulées précédemment concernant l'identification face à face des clients au moyen des informations enregistrées sur le microprocesseur de leur carte d'identité électronique sont a fortiori d'application lors de la vérification à distance des clients au moyen du même document probant.

Dans ce cas également, la vérification correcte des données d'identification au départ du microprocesseur des cartes d'identité électroniques belges requiert une vérification électronique simultanée que les données figurant sur la puce sont signées électroniquement par le Registre National. Il convient en outre de s'assurer que le certificat n'a pas été révoqué par celui-ci. Il est également recommandé dans ce cas que les procédures informatiques mises en œuvre soient conçues en manière telle que cette vérification soit opérée systématiquement et automatiquement, sans requérir d'intervention du préposé qui procède à l'identification, et sans qu'il ne dispose de la faculté de désactiver ce contrôle.

4.2.4.2.3. Les certificats d'identification

L'admissibilité des certificats d'identification au sens de la directive européenne relative à la signature électronique est soumise à diverses conditions liées aux caractéristiques du certificat : ne peuvent être admis que des certificats qualifiés requérant, pour être obtenus, une identification physique du titulaire, et qui n'ont pas été émis sous un pseudonyme.

D'autres conditions d'admissibilité sont liées aux qualités du prestataire de service de certification qui a émis le certificat. À cet égard, les certificats émis par des prestataires accrédités dans l'Etat membre de l'Espace économique européen où ils sont établis peuvent être admis sans opérer d'autre vérification que celle de l'existence de l'accréditation. En ce qui concerne les certificats émis par d'autres prestataires de service de certification en revanche, il appartient à chaque organisme qui souhaite pouvoir admettre leurs certificats au titre de document probant de procéder au préalable aux vérifications suivantes. Il s'agit, d'une part, de s'assurer qu'il s'agit de prestataires de service de certification établis dans un Etat membre de l'Espace économique européen ou, si ce n'est pas le cas, qu'ils rencontrent les conditions fixées à l'article 16, § 2, de la loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques. D'autre part, l'organisme doit apprécier préalablement la qualité des certificats émis par le prestataire de service de certification concerné sur la base d'une analyse documentée de sa réputation et de ses procédures de certification, et la décision d'accepter les certificats émis par ce prestataire doit faire l'objet d'un réexamen périodique.

La CBFA estime dès lors que le recours à cette faculté requiert que l'organisme concerné dispose d'une organisation adéquate, s'appuyant sur les compétences requises, pour procéder à cet examen et à ce réexamen périodique.

En cas de recours à de tels certificats pour vérifier l'identité d'un client, les recommandations formulées à la section 4.2.4.2.2., alinéas 2 et 3, ci-dessus sont également applicables, *mutatis mutandis.*

4.2.4.2.4. Consultation du Registre national

Article 16, § 3, de la loi

Les associations professionnelles désignées par le Roi se voient accorder l'autorisation :

1° d'utiliser le numéro d'identification du Registre national ;

2° d'accéder aux données du Registre national des personnes physiques, visées à l'article 3 de la loi du 8 août 1983 organisant un Registre national des personnes physiques ;

3° de prendre copie sur support papier ou électronique des informations consultées dans le Registre national et de communiquer ces informations aux personnes et organismes visés à l'article 2, § 1er, 4° à 15° ;

et ce aux seules fins de la vérification par les personnes et organismes visés à l'article 2, § 1er, 4° à 15°, conformément à l'article 7, § 1er et § 2, de l'identité des clients et des mandataires de ceux-ci, qui sont des personnes physiques et ne sont pas présents lors de leur identification, de même qu'aux fins de la vérification de l'identité des bénéficiaires effectifs des clients, conformément à l'article 8, § 1er, et de la mise à jour des données d'identification relatives aux clients et aux mandataires et bénéficiaires effectifs des clients, conformément aux articles 7, § 3, et 8, § 2.

Les associations professionnelles désignées par le Roi n'ont accès aux données visées à l'alinéa 1er qu'à condition d'avoir reçu une demande motivée dans ce sens de la part d'une personne ou d'un organisme visé à l'article 2, § 1er, 4° à 15°. L'association professionnelle consultée communiquera à cette personne ou à cet organisme les données que celle-ci ou celui-ci doit nécessairement connaître pour exécuter ses obligations visées à l'alinéa 1er.

Les associations professionnelles désignées par le Roi peuvent ensemble ou chacune séparément créer une institution qui, à leur place :

1° reçoit l'autorisation d'utiliser le numéro d'identification du Registre national aux fins visé es à l'alinéa 1er ;

2° reçoit l'accès aux données du Registre national des personnes physiques, visées à l'article 3 de la loi du 8 août 1983 organisant un Registre national des personnes physiques, aux fins visées à l'alinéa 1er ;

3° reçoit l'autorisation de prendre copie sur support papier ou électronique des informations consultées dans le Registre national et de communiquer ces informations aux personnes et organismes visés à l'article 2, § 1er, 4° à 15°, aux fins visées à l'alinéa 1er.

Les institutions visées à l'alinéa 3 jouissent de la personnalité juridique. Leur siège et leur direction générale sont établis en Belgique. Sans préjudice des dispositions d'autres lois,

elles limitent leur objet social aux activités visées à l'alinéa 3. Sans préjudice des dispositions d'autres lois, ces institutions sont toujours détenues exclusivement par les associations professionnelles désignées par le Roi.

Les personnes et organismes visés à l'article 2, § 1er, 4° à 15°, peuvent, aux fins du respect de leurs obligations visées à l'alinéa 1er, utiliser toutes les informations du Registre national qu'elles ont reçues par l'intermédiaire des associations professionnelles ou des institutions précitées, les traiter, les conserver et en prendre copie sur support papier ou électronique.

Le recours au Registre national est uniquement autorisé pour vérifier, par application de la loi du 11 janvier 1993, l'identité des personnes qu'elle vise (à savoir, les clients, leurs mandataires et leurs bénéficiaires effectifs). De plus, il n'est autorisé que lorsque les personnes dont l'identité doit être vérifiée ne sont pas physiquement présentes. Tel est le cas lorsque des relations d'affaires ou des opérations sont nouées à distance avec un client, lorsque l'identification et la vérification porte sur des bénéficiaires effectifs du client, ou lors de la mise à jour des données d'identification de clients ou de bénéficiaires effectifs qui ne sont pas présents au moment d'y procéder. Ces situations comportent par nature des risques particuliers. Dès lors, indépendamment de la valeur probante du recours au Registre national dans ces hypothèses, cette modalité de vérification de l'identité du client ne dispense pas les organismes financiers de mettre en œuvre les mesures de vigilance particulière qui sont requises en vertu de l'article 12, § 2, de la loi (cf. sections 4.6 et 5.2.2.1, infra).

Sur le plan de la procédure, le Législateur a défini les modalités de la consultation du Registre national de manière cohérente avec les dispositions légales analogues visant à faciliter la recherche des titulaires des comptes, coffres et contrats d'assurance dormants [17]. L'accès aux données du Registre national ainsi accordé par la loi aux organismes financiers est indirect et requiert l'intervention des associations professionnelles désignées par le Roi ou des institutions créées par elles pour offrir ce service. Le parallélisme établi avec les dispositions légales relatives aux comptes, coffres et contrats d'assurance dormants vise à permettre que les mêmes outils et procédures mis en œuvres par les associations professionnelles puissent être mis à la disposition des organismes financiers pour leur permettre de satisfaire à leurs obligations, indifféremment, dans le cadre de l'une ou de l'autre de ces législations.

Il convient cependant de souligner que les données pouvant être consultées auprès du Registre National dans le cadre de l'une et de l'autre de ces législations pourront être différentes. Par application de la loi du 11 janvier 1993, cette procédure de consultation des données du Registre National ne peut être utilisée, dans les circonstances précitées, que pour la seule vérification des données d'identification visées à l'article 7, § 1er, alinéa 3, et à l'article 8, § 1er, alinéa 4, de la loi. De plus, le recours indirect aux données du Registre National pour vérifier l'identité des clients ou de leurs mandataires ou bénéficiaires effectifs conformément à la loi du 11 janvier 1993 demeure soumis par ailleurs aux dispositions de la loi du 8 août 1983 organisant un registre national des personnes physiques, ainsi qu'à la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. Pour la correcte application de ces législations, il y a lieu de se référer aux décisions, avis et recommandations de la Commission de la Protection de la Vie Privée en la matière [18]. L'attention est notamment attirée sur le fait que la CPVP estime qu'il est préférable, lorsque cela est possible, d'effectuer le contrôle à distance de l'identité en recourant aux fonctionnalités de la carte d'identité électronique plutôt que par recours au Registre National.

4.2.4.3. Vérification de l'identité d'une personne morale, d'un trust, d'une association de fait ou d'une autre structure juridique dénuée de personnalité juridique

Article 8 du règlement

§ 1er. Lors de l'identification des clients qui sont des personnes morales de droit belge, la vérification de leur identité conformément à l'article 7, § 1er, de la loi, doit être opérée au moyen des documents probants suivants:

17 Loi du 24 juillet 2008 portant des dispositions diverses (I), Chapitre V (MB 7 août 2008).

18 Il est notamment renvoyé à cet égard :

- à l'avis n° 16/2008 de la CPVP du 9 avril 2008, relatif à l'avant-projet de loi modifiant la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme : http://www.privacycommission.be/fr/docs/Commission/2008/avis_16_2008.pdf.
- et à l'avis n° 31/2008 de la CPVP du 24 septembre 2008, de la CPVP, relatif à l'avant-projet d'Arrêté royal portant application des articles 26 à 28, 31 et 36 de la loi du 24 juillet 2008 portant dispositions diverses (I) - Utilisation du Registre national et des données d'identification du registre Banque carrefour de la sécurité sociale : http://www.privacycommission.be/fr/docs/Commission/2008/avis_31_2008.pdf.

1° les derniers statuts coordonnés ou les statuts à jour de la personne morale cliente déposés au Greffe du Tribunal de commerce ou publiés aux annexes du Moniteur Belge;

2° la liste des administrateurs de la personne morale cliente et la publication de leurs nominations au Moniteur Belge, ou tout autre document probant permettant d'établir leur qualité d'administrateurs, tels que toute publication au Moniteur Belge faisant mention de ces personnes en tant qu'administrateurs, ou les comptes annuels déposés à la Banque Nationale de Belgique;

3° la dernière publication au Moniteur Belge des pouvoirs de représentation de la personne morale cliente.

§ 2. Lors de l'identification des clients qui sont des personnes morales de droit étranger, la vérification de leur identité conformément à l'article 7, § 1er, de la loi, doit être opérée au moyen des documents probants équivalents à ceux énumérés au § 1er du présent article et, si nécessaire pour l'organisme, de leur traduction dans une des langues nationales ou en anglais.

Article 9 du règlement

Lors de l'identification des clients qui sont des trusts, des associations de fait, des fiducies, ou toutes autres structures juridiques dénuées de personnalité juridique, les organismes prennent connaissance de l'existence, de la nature, des finalités poursuivies et des modalités de gestion et de représentation de la structure juridique concernée, et les vérifient au moyen de tous documents susceptibles de faire preuve, dont ils prennent copie.

Cette identification inclut la prise de connaissance et la vérification de la liste des personnes autorisées à exercer la gestion de ces clients, au moyen d'un document susceptible de faire preuve.

Dans l'ensemble des cas ici visés, la vérification des informations d'identification doit être opérée au moyen de documents ayant valeur de preuve dans le droit qui est applicable à la personne morale, au trust, à l'association de fait ou à la structure juridique considérée.

Ces documents probants peuvent être obtenus soit auprès du client lui-même, soit auprès de sources officielles telles que le Moniteur Belge ou auprès de toutes autres sources d'information pouvant être considérés comme fiables. A cet égard il conviendra également de tenir compte à court ou moyen terme de l'existence de la Banque-Carrefour des Entreprises et du principe selon lequel les « services ou instances » habilités à consulter la BCE, ne pourront plus réclamer aux entreprises ou aux mandataires de celles-ci les données accessibles publiquement (article 22 de la loi portant création d'une Banque-Carrefour des Entreprises [19]). A cet effet, il est cependant nécessaire que l'enregistrement de toutes les données visées à l'article 17 de la loi BCE soit concrètement réalisé et que certaines adaptations en projet de cette législation et de l'arrêté royal portant sur les modalités d'accès soient effectives.

4.2.5. Copie des documents probants

L'article 7, § 1er, alinéa 1er, de la loi précise que la copie du document probant que les organismes sont tenus de prendre peut l'être tant sur support papier qu'électronique. Cette alternative s'applique à tous les documents probants utilisés.

Toutefois, la CBFA encourage également ces organismes à évoluer rapidement d'un enregistrement des données d'identification des clients par photocopie de leurs cartes d'identité vers un enregistrement électronique systématique de ces données, dans un environnement adéquatement sécurisé, au départ des microprocesseurs incorporés aux nouvelles cartes d'identité. En effet, les performances de ces nouvelles modalités d'enregistrement sont susceptibles d'être incomparablement plus élevées, tant sur le plan du coût économique de la gestion de ces informations par les établissements, que sur celui de la rapidité de la reconstitution des opérations à la demande de la Cellule de traitement des informations financières.

Lorsque l'identité du client a été vérifiée électroniquement au moyen de sa carte d'identité électronique ou d'un certificat visé à l'article 7, § 2, 2°, du règlement, les données d'identification lues, ainsi que leur signature électronique par le Registre National ou par le prestataire de service de certification, doivent être conservées solidairement afin de permettre toute vérification ultérieure de la signature.

19 Loi du 16 janvier 2003 portant création d'une Banque-Carrefour des Entreprises, modernisation du registre de commerce, création de guichets-entreprises agréés et portant diverses dispositions, MB 5 février 2003

Article 38, § 2, alinéa 2, de la loi

Par dérogation aux dispositions de l'article 7, § 1er, alinéa 1er et de l'article 13, les autorités visées au § 1er peuvent autoriser, par voie de règlement, les organismes et les personnes soumis à leur contrôle et visés aux articles 2, § 1er, 3 et 4, à conserver les références des documents probants exigés lors de l'identification du client en lieu et place d'une copie de ceux-ci, dans les cas et sous les conditions qu'elles déterminent.

Article 25 du règlement

Par dérogation aux articles 7, § 1er, 8, § 1er, et 13 de la loi, les organismes sont autorisés, par application de l'article 38, § 2, alinéa 2 de la loi, à substituer à la prise et à la conservation d'une copie des documents probants au moyen desquels ils ont vérifié l'identité du client, et, le cas échéant, de ses mandataires et bénéficiaires effectifs, l'enregistrement et la conservation des références de ces documents probants, pour autant que, de par leur nature et leurs modalités de conservation, les références de ces documents permettent avec certitude à l'organisme de les produire immédiatement, à la demande des autorités compétentes, au cours de la période de conservation des informations fixée à l'article 13 de la loi, sans que ces documents n'aient pu entretemps être modifiés ou altérés.

Les organismes qui envisagent de recourir à cette autorisation précisent au préalable dans leurs procédures d'acceptation des clients, sous le contrôle et la responsabilité du responsable de la prévention du blanchiment de capitaux et du financement du terrorisme, les catégories de documents probants dont les références peuvent être enregistrées et conservées en lieu et place d'une copie, ainsi que les modalités de récupération des documents probants concernés permettant de les produire à la demande conformément à l'alinéa précédent.

L'article 25 du règlement, pris par application de l'article 38, § 2, alinéa 2, de la loi, vise à alléger la charge administrative que représente pour les organismes financiers la prise de copie des documents probants et leur conservation, lorsque l'enregistrement et la conservation des références de ces documents probants permet d'atteindre des résultats équivalents.

Ceci suppose que l'organisme qui a recours à cette faculté puisse avoir la certitude qu'il sera à même, grâce à ces références, de retrouver et de produire rapidement, sur demande des autorités compétentes (notamment la CTIF et la CBFA) le document probant sur lequel il s'est basé pour procéder à la vérification de l'identité d'un client, mandataire ou bénéficiaire effectif, sans que ce document n'ait entre-temps pu être modifié, altéré ou perdu. Pourraient notamment être visées par cette mesure les publications au Moniteur belge ou dans d'autres publications officielles qui peuvent être retrouvées avec certitude à tout instant auprès de l'organe qui les a publiés. En revanche, la copie des cartes d'identité et des passeports ne peut pas être remplacée par l'enregistrement et la conservation de leurs références, dans la mesure où celles-ci ne permettront pas avec certitude à l'organisme de retrouver a posteriori et de produire dans le délai imparti le document probant, sans modification ni altération, qu'il a utilisé pour satisfaire à son obligation de vérification.

Par ailleurs, la décision de recourir à cette faculté relève de la politique de conformité de l'organisme à la législation et à la réglementation de lutte contre le blanchiment de capitaux et du financement du terrorisme. Cette faculté ne peut dès lors être utilisée qu'à la condition qu'elle soit prévue et modalisée de façon précise par la procédure écrite d'acceptation des clients, sous la responsabilité du responsable de la prévention du blanchiment de capitaux et du financement du terrorisme.

4.2.6. Autres informations requises

4.2.6.1. L'adresse du client, personne physique

Article 7, § 1er, alinéa 3, de la loi

(...) Des informations pertinentes doivent en outre être recueillies, dans la mesure du possible, concernant l'adresse des personnes identifiées.

Comme indiqué plus haut, les données d'identification des clients, personnes physiques, dont les organismes financiers sont tenus de prendre connaissance et qu'ils doivent vérifier au moyen d'un document probant sont le nom, le prénom, et le lieu et la date de naissance. Néanmoins, l'article 7, § 1er, alinéa 3, de la loi impose complémentairement d'obtenir, dans la mesure du possible, des informations relatives à l'adresse du client.

A cet effet, la CBFA estime que les procédures internes des organismes financiers devraient déterminer de manière suffisamment précise les mesures à prendre pour satisfaire à cette obligation légale.

Lorsque les informations pertinentes concernant l'adresse du client sont fournies par le document probant utilisé pour vérifier l'identité du client, ce document devrait logiquement aussi constituer la source des informations pertinentes concernant son adresse.

Si cela n'est pas possible (notamment lorsque l'adresse du client n'est pas mentionnée par ce document probant), les procédures internes devraient déterminer de quelle manière cette information peut être obtenue. Dès lors qu'en vertu de l'article 7, § 1er, de la loi, l'adresse ne doit pas être vérifiée au moyen d'un document probant [20], la simple déclaration signée du client concernant son adresse peut en règle générale être satisfaisante lorsque le client, la relation d'affaires ou l'opération ne présente pas de risques particuliers de blanchiment de capitaux ou de financement du terrorisme.

Néanmoins, lorsque les caractéristiques de la relation d'affaires à nouer ou de l'opération à effectuer font apparaître des risques particuliers de blanchiment de capitaux ou de financement du terrorisme, les organismes financiers devraient renforcer leur vigilance également en ce qui concerne leur connaissance de l'adresse du client. Ainsi par exemple, dans le cas de l'ouverture d'une relation d'affaires à distance qui peut présenter des risques plus élevés de méconnaissance du client par l'organisme financier, celui-ci devrait envisager, dans le cadre des mesures de vigilance renforcée qui sont requises (voir section 5.2.2.1 infra) de mettre en œuvre des mesures permettant de confirmer l'exactitude de l'adresse communiquée par le client. Ces mesures pourraient par exemple consister dans l'envoi d'un courrier à l'adresse indiquée par le client, conditionnant l'entrée en vigueur de la relation d'affaires ou l'exécution de l'opération au renvoi par le client d'un accusé de réception attaché au courrier.

4.2.6.2. Informations requises pour la mise en œuvre de la politique d'acceptation des clients et l'exercice des devoirs de vigilance

Article 12 du règlement

Lors de l'identification de clients visés à l'article 7, § 1er, alinéa 1er, 1° et 2° de la loi, les organismes recueillent et enregistrent toutes informations nécessaires pour permettre la mise en application de la politique d'acceptation des clients conformément au chapitre 8 et le devoir de vigilance à l'égard des relations d'affaires et des opérations conformément au chapitre 9.

L'article 12 du règlement précise également qu'il y a lieu de recueillir auprès du client toutes les informations qui sont nécessaires pour mettre en œuvre la politique d'acceptation des clients et les devoirs de vigilance à l'égard des relations d'affaires et des opérations. Ces informations, à préciser également en fonction des critères définis par chaque organisme dans le cadre de sa politique d'acceptation des clients et de ses devoirs de vigilance (voir chapitres 5 et 6, infra), peuvent notamment concerner les activités professionnelles et le secteur économique d'activité du client, ses sources de revenus ou l'origine des fonds. Il importe néanmoins que les organismes financiers veillent à ce que les informations à caractère personnel qu'ils collectent auprès de leurs clients soient proportionnées aux finalités poursuivies par la loi et le règlement, afin d'éviter que cette collecte d'informations constitue une intrusion excessive dans la vie privé des clients.

A cet égard, l'attention est attirée en particulier sur l'article 12, § 3, alinéa 6, 1°, de la loi qui impose aux organismes de « *mettre en œuvre des procédures adéquates et adaptées, en fonction du risque, de manière à pouvoir déterminer si le client ou un bénéficiaire effectif du client est une personne politiquement exposée* » [21], ainsi que sur le 3° de la même disposition qui impose de « *prendre toute mesure appropriée, en fonction du risque, pour établir l'origine du patrimoine et l'origine des fonds impliqués dans la relation d'affaires ou la transaction* ».

L'ensemble des informations ainsi recueillies, de même que celles relatives à l'adresse du client, devraient être enregistrées selon des modalités qui en permettent une exploitation adéquate dans le cadre la politique d'acceptation des clients et du système vigilance de l'organisme. En revanche, il est à noter qu'il s'agit le plus souvent d'éléments d'information non vérifiables au moyen d'un document probant. Vu leur finalité, les organismes financiers devraient néanmoins s'efforcer de s'assurer que ces informations leur sont fournies de bonne foi par le client.

---

20 Toutefois, l'adresse du client doit être vérifiée au moyen d'un document probant, conformément au Règlement (CE) n° 1781/2006 du Parlement européen et du Conseil du 15 novembre 2006, si, pour satisfaire à son obligation qui en résulte de transmettre, en même temps que les fonds, les informations complètes à propos du donneur d'ordre d'un virements de fonds, l'organisme financier décide de communiquer les informations relatives à l'adresse du client, sans recourir à la faculté laissée par le Règlement d'y substituer le lieu et la date de naissance du client. (cf. section 8.1.1, infra.)

21 Pour plus de précisions concernant les devoirs de vigilance accrue à l'égard des personnes politiquement exposées, il est renvoyé à la section 5.2.2.2 de la présente circulaire

Les dispositions de l'article 12 du règlement s'appliquent également, *mutatis mutandis*, lors de l'identification d'un client souhaitant réaliser une opération occasionnelle visée à l'article 7, § 1er, alinéa 1er, 2°, de la loi. Dans ce cas, outre que les informations à recueillir doivent permettre la mise en œuvre de la politique d'acceptation des clients, elles doivent également permettre aux préposés chargés de la surveillance de première ligne d'exercer adéquatement leurs responsabilités de détection des « opérations atypiques » (cf. section 6.1., infra). Ces informations doivent notamment leur permettre de se forger une opinion quant à la justification économique et à la légitimité apparentes de l'opération à la réalisation de laquelle leur concours est demandé.

4.3. Identification et vérification de l'identité des mandataires

4.3.1. Règles générales

Article 7, § 2, de la loi

Les organismes et les personnes visés aux articles 2, § 1er et 3 doivent identifier les mandataires de leurs clients et vérifier leur identité, au moyen d'un document probant dont il est pris copie, sur support papier ou électronique et ce, préalablement à l'exercice par ces mandataires de leur pouvoir d'engager le client qu'ils représentent dans le cadre de relations d'affaires ou d'opérations visées au § 1er, alinéa 1er. Les alinéas 3 et 4 du §1er sont d'application.

Article 13 § 1er, du règlement

La vérification de l'identité des mandataires des clients conformément à l'article 7, § 2, de la loi est soumise aux dispositions des articles 7 et 8 du présent règlement.

Les organismes prennent en outre connaissance des pouvoirs de représentation de la personne agissant au nom du client et procèdent à leur vérification au moyen de documents susceptibles de faire preuve dont ils prennent copie.

Sont notamment visés au présent article:

- *les représentants légaux de clients incapables;*
- *les personnes autorisées à agir au nom des clients en vertu d'un mandat général ou spécial;*
- *les personnes autorisées à représenter les clients qui sont des personnes morales, des associations de fait, des trusts, des fiducies, ou toutes autres structures juridiques dénuées de personnalité juridique, dans leurs relations avec l'organisme.*

Dans le prolongement de l'article 7, § 2, de la loi qui étend les obligations d'identification et de vérification de l'identité des clients à leurs mandataires, l'article 13 du règlement précise qu'il s'impose également de recourir aux mêmes modalités de vérification de leur identité. Tout comme les obligations d'identification et de vérification de l'identité des clients, les obligations d'identifier leurs mandataires et de vérifier l'identité de ceux-ci au moyen de documents probants sont des obligations de résultat (cf. section 4.1.1., supra).

Sont visées par ces dispositions toutes les personnes qui sont habilitées en vertu de la loi, de la fonction qu'elles exercent ou d'un contrat, à agir au nom et pour le compte du client.

En ce qui concerne les clients qui sont des personnes morales, associations de fait, trusts ou autres structures juridiques dénuées de personnalité juridique, cette obligation d'identification ne porte pas sur toutes les personnes qui exercent un mandat d'administration ou participent à la gestion du patrimoine du client - et qui sont à ce titres ses bénéficiaires effectifs (cf. sections 4.4.2.2., et 4.4.2.3., infra), mais sur les personnes qui, dans le cadre d'un tel mandat d'administration ou en vertu de tout autre mandat spécial ou général, représentent effectivement le client dans ses relations avec l'organisme.

L'article 7, § 2, de la loi précise également que l'identification et la vérification de l'identité des mandataires ne doit pas obligatoirement être effectuées préalablement à l'ouverture d'une relation d'affaires avec le client, mais au plus tard lorsque les mandataires entendent exercer pour la première fois de manière effective leur pouvoir de représenter le client.

Il est aussi à souligner que l'obligation d'identification et de vérification de l'identité des mandataires est subsidiaire par rapport à l'obligation d'identification et de vérification de l'identité du client. Dès lors, dans les cas où la loi prévoit une dispense d'identifier le client (cf. section 4.5., infra), cette dispense inclut aussi celle d'identifier les mandataires du client.

4.3.2. Cas particulier : employés de contreparties professionnelles

Article 1er, 11°, du règlement

Pour l'application du présent règlement, l'on entend par :

(...)

11° « contrepartie professionnelle » : un client qui ne relève pas d'une catégorie visée à l'article 11, § 1er, de la loi et qui est un client professionnel au sens de l'article 2, alinéa 1er, 28° de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers, tel que précisé à la section I, alinéa 1er, de l'annexe A de l'arrêté royal du 3 juin 2007 portant les règles et modalités visant à transposer la Directive concernant les marchés d'instruments financiers, ou qui est une contrepartie éligible au sens de l'article 2, alinéa 1er, 30° de la loi précitée du 2 août 2002, tel que précisé à l'article 3, § 1er, alinéa 1er, de l'arrêté royal précité du 3 juin 2007.

Article 13, § 2, du règlement

Sans préjudice de l'identification et de la vérification de l'identité des clients qui sont des contreparties professionnelles, ainsi que de leurs bénéficiaires effectifs, conformément aux articles 7 et 8 de la loi et au présent règlement, et pour autant que les organismes qui entrent en relation avec eux ou qui effectuent des opérations avec eux s'assurent que ces contreparties et leurs opérations ne présentent pas de risques particuliers de blanchiment de capitaux ou de financement du terrorisme, les organismes peuvent faire porter l'identification des employés du client autorisés à conclure les opérations en son nom sur le nom, le prénom, et le grade hiérarchique ou les fonctions de ces employés dans l'organigramme du client.

La vérification de ces données d'identification des employés concernés du client peut être effectuée au moyen des documents habituellement échangés dans le cadre de relations d'affaires ou de l'exécution d'opérations de cette nature avec ces contreparties.

Dans ces cas également, les organismes sont dispensés de recueillir des informations concernant l'adresse privée des employés concernés du client.

Les règles internes des organismes qui recourent à la faculté prévue aux alinéas précédents énumèrent limitativement les catégories de clients professionnels, ainsi que les catégories de relations d'affaires ou d'opérations, auxquelles ces modalités particulières d'identification et de vérification de l'identité des mandataires des clients peuvent être appliquées.

Les organismes établissent par écrit, pour chacun des clients auxquels ces modalités particulières sont appliquées, la justification que lesdites modalités sont adéquates et appropriées compte tenu des risques de blanchiment de capitaux et de financement du terrorisme. Ils tiennent cette justification écrite à la disposition de la CBFA.

L'article 13, § 2, du règlement fait usage de la faculté que l'article 38, § 2, alinéa 1er, de la loi attribue aux autorités de contrôle d'autoriser les organismes à ajuster la portée de leurs obligations d'identification en fonction du risque associé au type concerné de client, de relation d'affaires, de produit ou d'opération. Cet article du règlement met ainsi en application le principe de proportionnalité dans des situations dans lesquelles l'application des modalités normales d'identification et de vérification de l'identité des mandataires peut ne pas être adaptée, compte tenu des particularités des activités financières concernées et de leurs modalités usuelles d'exercice.

Sont notamment visées les relations d'affaires et les opérations des salles de marché des organismes avec des contreparties professionnelles auxquelles les dispenses d'identification prévues à l'article 11, § 1er, de la loi ne trouvent pas à s'appliquer. Pour déterminer les contreparties professionnelles concernées, il est fait référence aux clients qui relèvent des "*catégories de clients considérés comme professionnels*", conformément à la section I, alinéa 1er, de l'annexe A de l'arrêté royal du 3 juin 2007 portant les règles et modalités visant à transposer la Directive concernant les marchés d'instruments financiers, ainsi qu'aux "*contreparties éligibles*" visées à l'article 3, § 1er, alinéa 1er, du même arrêté royal. L'on notera que ne sont pas visés les clients qui, bien que ne relevant pas d'une catégorie d'entreprises ainsi visées, font usage du droit que leur reconnait cet arrêté royal de demander d'être traité comme des clients professionnels ou comme des contreparties éligibles.

Dès lors que, dans le cadre de ce type d'activités, les employés de la contrepartie ne peuvent en principe conclure d'opérations qu'au nom et pour le compte de la contrepartie, sans avoir la possibilité de conclure de telles opérations en leur propre nom ou au nom d'un tiers, il peut ainsi apparaître plus opportun que leur identification porte sur leur grade hiérarchique ou leur position dans l'organigramme de la contrepartie, plutôt que sur le lieu et la date de leur naissance. De plus, l'adresse privée de ces employés

n'apparaît pas revêtir en l'occurrence un degré de pertinence suffisant pour imposer que des informations à ce sujet soient recueillies.

Dès lors qu'en outre ce type de relations d'affaires donne lieu à des échanges de documents tels que les listes de signatures autorisées, auxquelles il est donné foi dans le cadre de la relation d'affaire, l'article 13, § 2, alinéa 2, du règlement prévoit une dérogation au § 1er, alinéa 1er, du même article, en autorisant que la vérification de l'identité de ces employés soient effectuée au moyen de ces documents usuels, en lieu et place des documents probants visés à l'article 8 du règlement.

Toutefois, le recours à la faculté ainsi laissée par le règlement d'appliquer des modalités plus adaptées aux circonstances en matière d'identification et de vérification de l'identité des employés de leurs contreparties professionnelles requiert que les règles internes de l'organisme concerné énumèrent limitativement les situations dans lesquelles ces modalités spécifiques peuvent être appliquées (article 13, § 2, alinéa 4) et, d'autre part, que leur mise en application effective fasse l'objet d'une analyse préalable permettant de justifier, au cas par cas, que ces modalités spécifiques sont adéquates et appropriées pour tenir compte du niveau de risque de blanchiment de capitaux et de financement du terrorisme qui est associé au client concerné, à la relation d'affaires nouée avec lui, aux produits à lui fournir et aux opérations à effectuer avec lui.

4.4. Identification et vérification de l'identité des bénéficiaires effectifs

4.4.1. Principes de base

Article 8, § 1er, alinéa 1er, de la loi

Le cas échéant, les organismes et les personnes visés aux articles 2, § 1er et 3 doivent identifier le ou les bénéficiaires effectifs du client et prendre des mesures adéquates et adaptées au risque pour vérifier leur identité.

Afin d'être en mesure de satisfaire à cette obligation, il appartient en premier lieu aux organismes financiers de définir des mesures appropriées, notamment sur le plan de la collecte des informations visées à l'article 12 du règlement, afin de déterminer, dans les cas qui ne sont pas visés aux sections 4.4.2.2 à 4.4.2.4 ci-dessous, si le client agit exclusivement pour son propre compte ou pour le compte d'un ou plusieurs bénéficiaires effectifs.

Comme indiqué à la section 4.1.1., supra, si l'obligation d'identifier les bénéficiaires effectifs est une obligation de résultat tout comme l'obligation d'identifier les clients et leurs mandataires, l'obligation de vérifier l'identité des bénéficiaires effectifs est une obligation de moyens.

De plus, ces mesures prises en vue de vérifier l'identité des bénéficiaires effectifs doivent être définies en fonction du niveau de risque de blanchiment de capitaux ou de financement du terrorisme que l'organisme financier estime associé au profil du client ou à la nature de la relation d'affaires ou de l'opération souhaitée par le client. Le degré d'exigence quant aux mesures prises en vue de vérifier l'identité des bénéficiaires effectifs doit dès lors être déterminé sur la base d'une analyse des autres informations dont dispose l'organisme financier concernant le client, la relation d'affaire à nouer ou l'opération à effectuer. Ainsi, notamment, la vérification de l'identité des bénéficiaires effectifs requerra une attention accrue dans les situations énumérées à l'article 12 de la loi (cf. sections 4.6 et 5.2.2., infra).

4.4.2. Notion de bénéficiaire effectif

4.4.2.1. Règle générale

Article 8, § 1er, alinéa 2, de la loi

Au sens de la présente loi, il faut entendre par bénéficiaires effectifs, la ou les personnes physiques pour le compte ou au bénéfice de laquelle ou desquelles une transaction est exécutée ou une relation d'affaires nouée ou encore la ou les personnes physiques qui possèdent ou contrôlent en dernier ressort le client.

Il importe de souligner que seules des personnes physiques peuvent être considérées comme bénéficiaires effectifs au sens de la loi. Par conséquent, lorsqu'il apparaît que le client souhaite nouer une relation d'affaires ou effectuer une opération occasionnelle en son propre nom mais pour le compte ou au bénéfice d'une société, d'une autre personne morale ou d'une construction juridique, il s'impose d'identifier, en qualité de bénéficiaires effectifs du client, les personnes physiques qui possèdent ou contrôlent en dernier ressort ladite société, personne morale ou construction juridique, comme indiqué aux sections 4.4.2.2. à 4.4.2.4. ci-après.

Quant à la portée de la notion de bénéficiaire effectif, en ce qu'elle vise les personnes pour le compte desquelles ou au bénéfice desquelles une transaction est exécutée ou une relation d'affaires nouée, l'exposé des motifs de la loi du 18 janvier 2010 comporte les précisions importantes reproduites ci-après [22]:

« (…) sans préjudice des situations dans lesquelles une vigilance simplifiée peut être mise en œuvre conformément au projet d'article 11, § 1er de la loi du 11 janvier 1993, il convient de s'intéresser à la nature des opérations effectuées par un établissement financier. Lorsque ces opérations ont pour but de permettre à l'établissement financier de fournir effectivement à sa propre clientèle les produits et services qu'il lui propose, ces transactions sont à considérer comme des opérations pour le compte propre de l'établissement financier et non pour le compte de ses clients. Dans ce cas en effet, ceux-ci n'ont pas la possibilité de déterminer quelque modalité que ce soit de ces opérations. Ainsi en est-il par exemple lorsqu'un établissement de crédit contracte des emprunts interbancaires pour financer son portefeuille de crédits ou lorsqu'il recourt aux services de compensation/liquidation prestés par un autre établissement financier pour assurer la bonne exécution des services qu'il propose à ses clients en matière de paiements ou d'opérations sur titres.

Par contre, lorsqu'un client réalise une opération financière (dépôt, emprunt, opération sur titres, etc.) auprès d'un établissement financier tout en disposant du pouvoir de déterminer tout ou partie des modalités des opérations financières subséquentes que cet établissement réalisera en son propre nom, mais pour le compte du client, auprès d'autres contreparties financières, ces dernières doivent considérer le client de l'établissement financier comme le bénéficiaire effectif des opérations que cet établissement réalise dans ce contexte auprès d'elles. »

Il est de plus à noter qu'un même client peut simultanément avoir des bénéficiaires effectifs relevant de l'une et de l'autre des catégories définies par l'article 8, § 1er, alinéa 2, de la loi. Ainsi par exemple, lorsque le souscripteur d'une assurance-vie est une société, il s'impose d'identifier en qualité de bénéficiaires effectifs, non seulement la personne à qui la prestation sera payée au terme du contrat, en sa qualité de « personne au bénéfice de laquelle le contrat est conclu » (cf. section 4.4.4.3., infra), mais aussi les actionnaires et dirigeants de la société cliente, en qualité de « personnes qui possèdent ou contrôlent le client ».

4.4.2.2. Bénéficiaires effectifs des sociétés

Article 8, § 1er, alinéa 3, 1°, de la loi

Sont des bénéficiaires effectifs au sens de la présente loi, notamment :

1° lorsque le client est une société:
- *a. la ou les personnes physiques qui, en dernier ressort, possèdent ou contrôlent directement ou indirectement plus de 25% des actions ou des droits de vote ;*
- *b. la ou les personnes physiques qui exercent autrement le pouvoir de contrôle sur la direction de la société.*

(...)

Article 15, du règlement

Lorsque le client est une société commerciale ou à forme commerciale, il faut entendre par "personnes physiques qui exercent autrement le pouvoir de contrôle sur la direction de la société" au sens de l'article 8, § 1er, alinéa 3, 1°, b) de la loi :

- *les personnes physiques visées aux articles 5 à 9 du code des sociétés qui, sans posséder ou contrôler plus de 25 % des actions ou des droits de vote, exercent directement ou indirectement, le contrôle de fait la société*
- *ainsi que les personnes qui, sans disposer du pouvoir de représenter le client dans ses relations avec l'organisme, exercent des mandats dans son organe d'administration.*

Lorsque le client est une société, les dispositions rappelées ci-dessus de la loi et du règlement distinguent deux catégories de bénéficiaires effectifs :

- les actionnaires ou associés importants au profit desquels la société est gérée;
- les personnes qui exercent un mandat au sein de l'organe d'administration de la société et qui influencent à ce titre sa gestion.

Il convient de considérer comme des personnes qui possèdent ou contrôlent indirectement plus de 25 % des actions ou des droits de vote, au sens de l'article 8, § 1er, alinéa 3, 1°, a, de la loi, les personnes

22 Chambre des Représentants, 2008-2009, Doc 52 1988/001, p. 34

physiques qui exercent directement ou indirectement, en fait ou en droit, le contrôle sur une société qui détient directement plus de 25 % des actions ou des droits de vote.

Concernant les personnes qui exercent un mandat au sein de l'organe d'administration de la société et qui interviennent en outre effectivement pour représenter la société dans ses relations avec l'organisme financier, l'on rappellera que ces personnes doivent en outre être identifiées en raison de leur qualité de mandataires du client (cf. supra, section 4.3.1.).

En ce qui concerne les bénéficiaires effectifs des clients visés à l'article 8, § 1er, alinéa 3, de la loi, l'attention est également attirée sur la disposition transitoire prévue par l'article 44, § 2, de la loi. Dans la mesure où la notion de bénéficiaires effectifs de ces clients a été modifiée par la loi du 18 janvier 2010, cette disposition transitoire laisse aux organismes et personnes visées un délai de deux ans à dater de l'entrée en vigueur des nouvelles dispositions légales pour procéder à la mise à jour de l'identification et de la vérification de l'identité de ces bénéficiaires effectifs. Ce délai est porté à cinq ans en ce qui concerne l'identification de leur lieu et de leur date de naissance.

4.4.2.3. Bénéficiaires effectifs des autres personnes morales et des constructions juridiques dénuées de personnalité juridique

Article 8, § 1er, alinéa 3, 2°, de la loi

Sont des bénéficiaires effectifs au sens de la présente loi, notamment :

(...)

2° lorsque le client est une personne morale, autre qu'une société, telle qu'une fondation et une association sans but lucratif, ou est un trust, une fiducie ou une construction juridique similaire, qui gère ou distribue des fonds :

a. lorsque les futurs bénéficiaires ont déjà été désignés, la ou les personnes physiques qui sont bénéficiaires d'au moins 25 % des biens de la personne morale ou de la construction juridique;

b. lorsque les personnes physiques qui sont les bénéficiaires de la personne morale ou de la construction juridique n'ont pas encore été désignées, le groupe de personnes, défini in abstracto, dans l'intérêt duquel la personne morale ou la construction juridique a été principalement constituée ou a principalement produit ses effets;

c. la ou les personnes physiques qui exercent un contrôle sur au moins 25 % des biens d'une personne morale ou d'une construction juridique.

Article 16 du règlement

Lorsque le client est une personne morale autre qu'une société commerciale ou à forme commerciale visée à l'article 15, il faut notamment entendre par "personnes physiques qui exercent un contrôle sur au moins 25 % des biens d'une personne morale" au sens de l'article 8, § 1er, alinéa 3, 2°, c) de la loi les personnes qui, sans disposer du pouvoir de représenter le client dans ses relations avec l'organisme, exercent des mandats dans son organe d'administration.

Article 17 du règlement

Lorsque le client est une association de fait ou toute autre structure juridique dénuée de personnalité juridique, telle qu'un trust ou une fiducie, sont notamment à considérer comme "personnes physiques qui exercent un contrôle sur au moins 25 % des biens de la construction juridique" au sens de l'article 8, § 1er, alinéa 3, 2°, c) de la loi les personnes autres que celles qui disposent du pouvoir de représenter l'association auprès de l'organisme et qui sont visées à l'article 13 du présent règlement, mais qui disposent du pouvoir d'influer notablement sur sa gestion.

En ce qui concerne les trusts, la CBFA estime que doivent par exemple être considérés comme bénéficiaires effectifs en raison de leur pouvoir d'influence sur la gestion les *«charities commissioners»* des *«charitable trusts»,* compétents pour nommer, révoquer ou remplacer le trustee, lui demander des comptes et procéder à des enquêtes sur sa gestion du trust.

Concernant les bénéficiaires effectifs visés à l'article 8, alinéa 3, 2°, b, de la loi, l'exposé des motifs de la loi contient le commentaire explicatif suivant [23] : "*Dans les cas où les individus qui sont les bénéficiaires d'une personne morale ou d'une construction juridique tels une fondation ou un trust, doivent encore être désignés et où il n'est donc pas possible d'identifier un ou plusieurs individus comme bénéficiaires effectifs, il est suffisant de déterminer le groupe de personnes qui est désigné comme bénéficiaire de la*

23 Chambre des Représentants, 2008-2009, Doc 52 1988/001, p. 35

fondation ou du trust. Cette exigence n'implique pas l'identification des individus formant ce groupe de personnes." Tel serait par exemple le cas d'un "charitable trust" dont l'acte de constitution désigne comme bénéficiaires "les pensionnaires de tel orphelinat".

En ce qui concerne les personnes morales autres que des sociétés (les associations sans but lucratif, les fondations, etc.) et les associations de fait, les articles 16 et 17 du règlement précisent que leurs bénéficiaires effectifs sont les personnes qui exercent une influence notable sur leur gestion. Dans le cas de personnes morales, sont visées à ce titre les personnes qui exercent des mandats dans leurs organes d'administration. Comme le précisent le 12ème considérant de la 3ème directive européenne, ainsi que les travaux préparatoires de la loi du 18 janvier 2010 [24], lorsque des personnes apportent des biens à une personne morale ou à une construction juridique et exercent un contrôle sur l'utilisation de ces biens, elles doivent être également identifies comme bénéficiaires effectifs.

Il est à noter également que ces catégories de bénéficiaires effectifs sont complémentaires à celle des personnes physiques auxquelles le patrimoine des personnes morales ou les biens logés dans la construction juridique sont destinés.

4.4.2.4. Droits démembrés

Article 19 du règlement

Dans les cas de droits démembrés, l'obligation d'identification des bénéficiaires effectifs et de vérification de leur identité conformément à l'article 8 § 1er, alinéa 1er, de la loi porte sur les nus-propriétaires, sur les propriétaires dans le cas de contrats d'emphytéose, et sur les tréfonciers dans le cas de contrats de superficie.

4.4.3. Données d'identification

Article 8, § 1er, alinéa 4, de la loi

L'identification du bénéficiaire effectif porte sur son nom et son prénom, ainsi que, dans la mesure du possible, sur la date et le lieu de sa naissance. Des informations pertinentes doivent en outre être recueillies, dans la mesure du possible, concernant son adresse. (...) Toutefois, dans le cas visé à l'alinéa 3, 2°, b), l'identification porte sur la définition in abstracto du groupe concerné de personnes.

Comme dans le cas des clients, personnes physiques, l'obligation d'identification des bénéficiaires effectifs porte sur leur nom, leur prénom, et le lieu et la date de leur naissance. Toutefois, compte tenu du fait qu'il n'existe pas de relations directes entre les organismes financiers et les bénéficiaires effectifs de leurs clients, l'identification du lieu et de la date de naissance des bénéficiaires effectifs ne sont requises que dans la mesure du possible, et constitue ainsi une obligation de moyens, contrairement à l'identification du nom et du prénom du bénéficiaire effectif, qui est définie par la loi comme une obligation de résultat.

L'absence de relations directes entre les organismes financiers et les bénéficiaires effectifs justifie que l'obligation d'identification de ceux-ci ne porte pas sur l'objet et la nature de la relation d'affaires.

Tout comme à l'égard des clients, l'obligation d'identification et de vérification de l'identité des bénéficiaires effectifs est complétée par une obligation de recueillir des informations pertinentes concernant leur adresse. Cette obligation ne doit cependant être remplie que dans la mesure du possible.

Lorsqu'un organisme n'a pas pu identifier le lieu et la date de naissance d'un ou plusieurs bénéficiaires effectifs d'un client, ou lorsqu'il n'a pas pu satisfaire à son obligation de recueillir des informations sur l'adresse de ces personnes, il est de bonne gestion de tenir compte de cette circonstance particulière dans la mise en œuvre de sa politique d'acceptation des clients, et d'examiner si, tenant compte également des éventuels autres facteurs de risque qui sont relevés, cette connaissance imparfaite des bénéficiaires effectifs du client nécessite de soumettre la relation d'affaires à nouer avec lui à un degré accru de vigilance.

4.4.4. Modalités de vérification de l'identité

4.4.4.1. Modalités générales

Article 8, § 1er, alinéa 4, de la loi

(...) En outre, des mesures adéquates et adaptées au risque doivent être prises afin de vérifier ces données. (...)

24 Idem, p. 36

Article 14 du règlement

Les procédures internes des organismes définissent les mesures requises pour vérifier l'identité des bénéficiaires effectifs, conformément à l'article 8, § 1er, alinéa 4, de la loi, en fonction du risque de blanchiment de capitaux ou de financement du terrorisme associé au profil du client et à la nature de la relation d'affaires ou de l'opération souhaitée par le client.

Lorsque la vérification de l'identité des bénéficiaires effectifs ne peut pas être raisonnablement opérée par application des mesures définies conformément à l'alinéa précédent, les organismes consignent par écrit les mesures qui ont effectivement été mises en œuvre à cette fin et conservent cette justification dans le dossier d'identification du client. Ils tiennent compte de l'absence de vérification de l'identité des bénéficiaires effectifs dans l'application de leur politique d'acceptation des clients visée au chapitre 8. Ils refusent de nouer la relation d'affaires ou d'effectuer l'opération souhaitée par le client lorsque l'absence de vérification de l'identité des bénéficiaires effectifs est de nature à aggraver déraisonnablement le risque de blanchiment de capitaux ou de financement du terrorisme.

Dès lors que les mesures définies par les procédures internes pour vérifier l'identité des bénéficiaires effectifs doivent être proportionnées au risque de blanchiment de capitaux ou de financement du terrorisme associé au profil du client et à la nature de la relation d'affaires ou de l'opération souhaitée par le client, la CBFA recommande que ces mesures soient définies en fonction des critères de risques appliqués par l'organisme en application de sa politique d'acceptation des clients (cf. chapitre 5 infra). Ces procédures internes devraient prévoir que, dans la mesure du possible, la vérification de l'identité des bénéficiaires effectifs sera effectuée avec la même attention, et dès lors, en se fondant sur les mêmes documents probants que la vérification de l'identité du client.

A ce dernier égard, il pourra être fait usage, chaque fois que cela sera possible, de l'accès indirect au Registre national, qui est également octroyé par l'article 16, § 3, de la loi pour vérifier l'identité des bénéficiaires effectifs. Quant aux modalités de cette méthode de vérification de l'identité, il est renvoyé à la section 4.2.4.2.4 de la présente circulaire. Toutefois, les procédures internes peuvent prévoir que la vérification de l'identité d'un bénéficiaire effectif peut être opérée auprès du Registre national sans disposer d'une copie de la carte d'identité de cette personne.

A défaut de pouvoir vérifier l'identité des bénéficiaires effectifs au moyen d'un document probant tel que requis pour vérifier l'identité d'un client, les procédures internes des organismes devraient désigner les autres documents ou sources d'information auxquels il est raisonnable de donner foi et au moyen desquelles il convient de s'efforcer de procéder à la vérification. Peuvent ainsi être pris en considération des documents pour l'établissement desquels des contrôles d'identité appropriés sont effectués, tels que, par exemple, les actes notariés.

Lorsque, bien que mises en œuvre, ces mesures n'ont pas permis de vérifier l'identité des bénéficiaires effectifs d'un client, le règlement de la CBFA requiert que l'organisme consigne par écrit les mesures qui ont effectivement été mises en œuvre, afin de pouvoir justifier a posteriori qu'elles étaient adéquates et adaptées au risque.

Cette hypothèse doit être distinguée de celle où les mesures requises par les procédures internes n'ont pas pu être effectivement mises en œuvre, quelle qu'en soit la raison. Dans ce cas en effet, l'organisme financier est tenu de se conformer à l'interdiction de nouer ou de maintenir la relation d'affaires ou de réaliser l'opération, qui est énoncée à l'article 8, § 4, de la loi (voir aussi section 4.1.3 supra).

4.4.4.2. Bénéficiaires effectifs des sociétés, personnes morales et constructions juridiques

Article 8, § 3, de la loi

Les sociétés, personnes morales et constructions juridiques visées au § 1er, alinéa 3, sont tenues de communiquer l'identité de leurs bénéficiaires effectifs aux organismes ou aux personnes visés aux articles 2, § 1er et 3 avec lesquels ces sociétés, personnes morales et constructions juridiques souhaitent nouer une relation d'affaires visée à l'article 7, § 1er, alinéa 1er, 1°, ou réaliser une opération visée à l'article 7, § 1er, alinéa 1er, 2°. Elles sont également tenues de leur fournir, sur demande, une mise à jour de ces informations, en vue de leur permettre de satisfaire à l'obligation visée au § 2.

Article 18 du règlement

§ 1er. Lorsque l'examen des informations que le client a communiquées concernant l'identité de ses bénéficiaires effectifs, conformément à l'article 8, § 3, de la loi lui permet de conclure à leur pertinence et à leur vraisemblance, il procède à la vérification de l'identité de ces bénéficiaires effectifs conformément à l'article 14.

§ 2. Lorsqu'il existe des raisons de douter de la pertinence ou de la vraisemblance des informations communiquées par le client conformément à l'article 8, § 3, de la loi, l'organisme prend toutes autres mesures raisonnables adéquates pour identifier les bénéficiaires effectifs du client, et toutes les mesures raisonnables pour vérifier leur identité, conformément à l'article 14.

L'organisme refuse de nouer la relation d'affaires ou d'effectuer l'opération souhaitée par le client lorsqu'il existe des raisons de croire que l'inexactitude ou le caractère incomplet des informations fournies par le client vise à dissimuler l'identité d'un ou plusieurs bénéficiaires effectifs. Il détermine en outre s'il y a lieu de procéder à une déclaration à la Cellule de traitement des informations financières par application de l'article 25 de la loi.

En ce qui concerne les clients qui sont des sociétés, d'autres personnes morales ou des constructions juridiques, le Législateur a facilité l'identification de leurs bénéficiaires effectifs par les personnes et organismes assujettis à la loi en instaurant une obligation à charge de ces clients de communiquer à ces personnes et organismes l'identité de leurs bénéficiaires effectifs. Cette obligation couvre les diverses catégories de bénéficiaires effectifs énumérées aux sections 4.4.2.2 et 4.4.2.3 ci-dessus. Cette déclaration du client pourra se fonder, selon le cas, sur l'acte de constitution, le registre des actionnaires nominatifs ou des associés ou les listes de présence aux assemblées générales, etc. En ce qui concerne les clients qui sont des sociétés ayant émis des actions au porteur ou dématérialisées, le Législateur a veillé à ce qu'ils disposent des informations nécessaires pour satisfaire à leur obligation, en assujettissant les actionnaires eux-mêmes à une obligation de déclaration auprès de la société lorsqu'ils franchissent le seuil de 25 % du capital et des droits de vote. L'article 56 de la loi du 18 janvier 2010 a inséré à cet effet un nouvel article 515*bis* dans le Code des Sociétés afin de prévoir cette obligation selon des modalités très largement inspirées des articles 514 et 515 du même code.

L'attention est attirée sur le fait que cette déclaration du client vise uniquement à faciliter les devoirs d'identification des bénéficiaires effectifs.

D'une part, les organismes financiers doivent soumettre les déclarations qu'ils reçoivent à un examen critique afin de s'assurer que les informations qu'elles contiennent sont pertinentes et vraisemblables. L'article 18, § 2, du règlement indique les mesures à prendre dans le cas où cet examen conduirait à considérer qu'une déclaration d'un client ne remplit pas ces qualités, ces mesures pouvant aller, en fonction des circonstances, jusqu'à un refus de nouer la relation d'affaires ou d'effectuer l'opération, et, le cas échéant, à la transmission d'une déclaration à la CTIF.

D'autre part, cette déclaration du client ne dispense pas l'organisme qui la reçoit de prendre des mesures adéquates et adaptées au risque afin de vérifier l'identité des personnes renseignées comme bénéficiaires effectifs, conformément à l'article 8, § 1er, alinéa 4, de la loi, selon les modalités précisées à l'article 14 du règlement. Il est renvoyé à cet égard à la section 4.4.4.1 ci-dessus.

Lorsque le client est un trust ou une fiducie dont ni l'acte constitutif, ni aucun autre document officiel ne désigne nominativement les personnes au profit desquelles ils sont gérés, les organismes sont invités à faire preuve d'une vigilance particulière s'ils ont des raisons de soupçonner, sur la base des informations disponibles concernant ce trust ou cette fiducie, ou sur la base de toute circonstance, que les modalités de désignation in abstracto des bénéficiaires effectifs ont notamment pour objectif de dissimuler leur identité. Le cas échéant, l'interdiction de nouer la relation d'affaires ou de réaliser l'opération prévue à l'article 8, § 4, de la loi pourra trouver à s'appliquer dans ce cas. Il peut de plus y avoir lieu d'examiner dans cette hypothèse s'il s'impose de procéder à une déclaration de faits suspects par application de l'article 25 de la loi.

4.4.4.3. Bénéficiaires des contrats d'assurance-vie

Article 20 du règlement

L'identification et la vérification de l'identité des bénéficiaires effectifs des contrats d'assurances vie conformément à l'article 8, § 1er, alinéa 1er, de la loi doivent être opérées au plus tard lorsqu'ils font valoir leur droit au paiement de la prestation résultant du contrat, et préalablement au paiement de celle-ci.

Lorsque le bénéficiaire effectif d'un contrat d'assurance vie s'adresse directement à l'entreprise d'assurances en vue d'obtenir le paiement de la prestation prévue par le contrat, sans recourir à l'intermédiaire en assurances par l'intermédiation duquel ce contrat a été conclu, l'entreprise d'assurances procède elle-même à son identification et à la vérification de son identité. Elle n'est pas tenue de transmettre à l'intermédiaire en assurances les données d'identification et les copies des documents probants.

Si l'article 20 du règlement permet de reporter l'identification des bénéficiaires d'un contrat d'assurance-vie jusqu'au paiement de la prestation prévue par le contrat, les devoirs d'identification et de vérification

de l'identité des personnes qui possèdent ou contrôlent le preneur d'assurance doivent en revanche être accomplis dès l'entrée en relation avec le preneur d'assurances.

4.4.5. Copie des documents utilisés pour la vérification de l'identité

Contrairement à l'article 7, § 1er de la loi, en ce qui concerne l'identification des clients, l'article 8, § 1er, de la loi n'impose pas explicitement de prendre une copie du document probant au moyen duquel l'identité des bénéficiaires effectifs a été vérifiée. Cette obligation découle cependant indirectement de l'article 13 de la loi, qui impose de conserver pendant 5 ans une copie des documents probants ayant servi à la vérification de l'identité du client et, le cas échéant, de ses mandataires et de ses bénéficiaires effectifs conformément aux articles 7 à 9 de la loi.

4.5. Dispenses légales d'identification

4.5.1. Principes et portée des dispenses d'identification

Outre le cas visé à l'article 7, § 1er, alinéa 2, de la loi, déjà évoqué plus haut (cf. section 4.2.2.2.2., supra), l'article 11 de la loi prévoit divers cas de dispense d'identification des clients, soit en raison du profil personnel de ces clients (article 11, § 1er), soit en raison du faible risque attaché aux produits pour lesquels ils sollicitent un organisme financier (article 11, § 2). Ces dispenses ne sont toutefois pas absolues, mais soumises aux limitations fixées par l'article 11, § 3, de la loi :

> ***Article 11, § 3, de la loi***
>
> *Les organismes et les personnes visés aux articles 2, § 1er et 3 recueillent, dans chaque cas, des informations suffisantes pour établir si le client remplit les conditions requises pour bénéficier d'une dérogation visée au § 1er.*
>
> *Les dérogations aux obligations de vigilance prévues aux § 1er et 2 ci-dessus ne s'appliquent pas s'il y a soupçon de blanchiment de capitaux ou de financement du terrorisme.*

D'une part, la CBFA recommande que les organismes financiers qui font application des dispenses visées à l'article 11, § 1er, de la loi consignent par écrit et conservent les informations sur lesquelles ils se sont fondés pour décider d'appliquer lesdites dispenses, afin d'être en mesure de les produire à tout instant à la demande des autorités compétentes pour justifier l'application de ces dispenses. Ces informations devraient concerner, outre l'identification du client, les éléments d'information sur lesquels l'organisme s'est fondé pour décider de l'application de l'article 11, § 1er de la loi, ainsi que leur source.

D'autre part, dès l'instant où des circonstances quelconques font naître des soupçons de blanchiment de capitaux ou de financement du terrorisme, que ce soit lors de l'entrée en relation avec le client ou postérieurement, l'organisme financier ne peut plus invoquer l'application d'une dispense d'identification prévue à l'article 11, § 1er ou § 2, de la loi. Il est tenu de procéder immédiatement à l'identification du client et de ses bénéficiaires effectifs conformément aux articles 7 et 8 de la loi. (Cf. aussi à ce sujet, l'article 7, § 1er, alinéa 1er, 3°, de la loi). De plus, l'existence de soupçons requiert qu'un rapport écrit soit établi conformément à l'article 14, § 2, de la loi et transmis au responsable de la prévention du blanchiment de capitaux, afin de permettre à ce dernier de déterminer s'il y a lieu de procéder à une déclaration d'opération ou de fait suspects conformément aux articles 23 à 25 de la loi. (cf. section 6.1.1., infra).

La CBFA attire en outre l'attention sur le fait qu'en vertu de l'article 12, § 1er de la loi, une vigilance accrue est requise dans toutes les situations présentant un risque élevé de blanchiment de capitaux ou de financement du terrorisme. Dans ces situations, il appartient aux organismes financiers d'exercer une vigilance accrue dès le stade de l'identification et de la vérification de l'identité du client, de ses mandataires et de ses bénéficiaires effectifs (cf. infra, section 4.6). Cette disposition légale s'oppose, par nature, à l'application dans ces circonstances des mesures de vigilance simplifiée autorisées par l'article 11 de la loi. Tel est notamment le cas si l'organisme financier reçoit, au moment de l'opération occasionnelle ou de l'entrée en relation, ou dans le cours de la relation d'affaires, des informations crédibles de nature à infirmer le faible risque de blanchiment de capitaux ou de financement du terrorisme associé au client, à l'opération ou à la relation d'affaires. Tel sera notamment le cas si ces informations crédibles font état de déficiences importantes des mesures de prévention du blanchiment de capitaux ou du financement du terrorisme mises en œuvre par un client visé à l'article 11, § 1er, 1° de la loi. Tel serait aussi le cas si ces informations crédibles font état de déficiences graves des dispositions légales ou réglementaires auxquelles le client est assujetti dans son pays d'origine en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, en ce compris les dispositions qui définissent les mécanismes de contrôle et de sanction qui sont applicables au client,

4.5.2. Dispenses fondées sur le profil personnel du client

4.5.2.1. Etablissements de crédit ou établissements financiers

Article 11, § 1er, 1°, de la loi

Les organismes et personnes visés aux articles 2, § 1er et 3 ne sont pas soumis aux obligations d'identification et de vérification visées aux articles 7 et 8 à l'égard des personnes suivantes:

1° le client ou le bénéficiaire effectif qui est un établissement de crédit ou un établissement financier visé à l'article 2 de la directive 2005/60/CE établi en Belgique ou dans un autre pays de l'Espace économique européen ou un établissement équivalent établi dans un pays tiers désigné par le Roi en vertu de l'article 37, § 2, alinéa 1er, 2°, qui impose des obligations et un contrôle équivalents à ceux prévus par la directive 2005/60/CE;

Les établissements de crédit et les établissements financiers établis en Belgique sont réputés de plein droit être soumis à un régime conforme à la 3ème directive européenne, et ne représenter qu'un faible risque justifiant la dispense légale d'identification. Il en va de même, par application du principe de reconnaissance mutuelle, des établissements de crédit et des établissements financiers qui sont établis dans un autre pays de l'Espace économique européen.

Lorsque ces établissements sont établis dans des pays tiers, ils peuvent également ne représenter qu'un faible risque, pour autant que le pays où ils sont établis leur impose des obligations et un contrôle équivalents à ceux prévus par la 3ème directive. Les pays tiers remplissant cette condition seront énumérés limitativement par un arrêté royal à prendre en exécution de l'article 37, § 2, alinéa 2, 2°, de la loi. Dans l'attente de l'entrée en vigueur de cet arrêté royal, l'article 44, § 4, de la loi prévoit que les pays membres du GAFI sont transitoirement considérés comme des pays tiers équivalents au sens de l'article 11, § 1er, 1° de la loi. L'on soulignera que cette liste est établie en tenant compte de la concertation régulière à ce sujet au sein du Comité de prévention du blanchiment de capitaux et du financement du terrorisme ("CPMLTF") créé par la 3ème Directive. Dans le souci de maintenir une égalité des conditions de concurrence au sein de l'Espace Economique Européen, cette concertation vise à établir et à tenir à jour une liste de pays tiers que l'ensemble des Etats membres considèrent "équivalents", en se fondant essentiellement à cet effet sur les résultats des évaluations internationales de la conformité des dispositifs nationaux des pays considérés avec les recommandations du GAFI. Il est toutefois rappelé qu'il ne peut pas être fait usage de la faculté de réduire le niveau de vigilance lorsque l'organisme financier reçoit des informations crédibles de nature à infirmer le faible risque de blanchiment de capitaux ou du financement du terrorisme associé au client, soit en raison de ses propres déficiences, soit en raisons de celles du cadre juridique auquel il est soumis (cf. supra).

4.5.2.2. Sociétés cotées

Article 11, § 1er, 2°, de la loi

Les organismes et personnes visés aux articles 2, § 1er et 3 ne sont pas soumis aux obligations d'identification et de vérification visées aux articles 7 et 8 à l'égard des personnes suivantes:

(...)

2° le client ou le bénéficiaire effectif qui est une société cotée dont les valeurs sont admises à la négociation sur un marché réglementé au sens de la directive 2004/39/CE dans un pays de l'Espace économique européen ou une société cotée dans un pays tiers désigné par le Roi en vertu de l'article 37, § 2, alinéa 1er, 3°, où elle est soumise à des exigences de publicité compatibles avec la législation communautaire;

(...)

Art. 8, § 1er, alinéa 3, 1°, b, de la loi :

(...)

Lorsque le client ou le détenteur d'une participation de contrôle est une société cotée sur un marché réglementé au sens de la directive 2004/39/CE dans un pays de l'Espace économique européen ou dans un pays tiers désigné par le Roi en vertu de l'article 37, § 2, alinéa 1er, 3°, où elle est soumise à des exigences de publicité compatibles avec la législation communautaire, il n'est pas requis d'identifier ses actionnaires, ni de vérifier leur identité.

Les pays tiers dont il est présumé, pour l'application de l'article 8, § 1er, alinéa 3, 1°, b, et de l'article 11, § 1er, 2°, de la loi, que leur législation impose des exigences de publicité compatibles avec la législation

communautaire seront énumérés limitativement par un arrêté royal à prendre en exécution de l'article 37, § 2, alinéa 2, 3°, de la loi.

4.5.2.3. Comptes groupés

Article 11, § 1er, 3°, de la loi

Les organismes et personnes visés aux articles 2, § 1er et 3 ne sont pas soumis aux obligations d'identification et de vérification visées aux articles 7 et 8 à l'égard des personnes suivantes:

(...)

3° les bénéficiaires effectifs de comptes groupés tenus par des notaires ou des membres d'une autre profession juridique indépendante établis en Belgique, dans un autre pays de l'Espace économique européen ou dans un pays tiers désigné par le Roi en vertu de l'article 37, § 2, alinéa 1er, 4°, où ils sont soumis à des exigences conformes aux normes internationales en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, et où le respect de ces obligations est contrôlé, pour autant que les informations relatives à l'identité des bénéficiaires effectifs soient mises à la disposition des établissements agissant en qualité de dépositaires pour les comptes groupés, lorsqu'ils en font la demande; lorsque le client est une personne visée à l'article 3, 5°, qui ne peut fournir les informations demandées en raison de son obligation de secret professionnel, l'article 8, § 4, ne s'applique pas s'il atteste par écrit à l'établissement dépositaire que les bénéficiaires effectifs du compte groupé considéré sont uniquement et exclusivement des clients avec lesquels il est en relation pour évaluer leur situation juridique, ou au profit desquels il exerce sa mission de défense ou de représentation dans une procédure judiciaire ou concernant une telle procédure, y compris dans le cadre de conseils relatifs à la manière d'engager ou d'éviter une procédure ;

(...)

La dispense d'identifier les bénéficiaires des comptes groupés ouverts à des notaires, avocats et titulaires de professions juridiques indépendantes tient compte de ce que ces personnes sont elles-mêmes légalement assujetties à l'obligation de coopérer à la lutte contre le blanchiment d'argent et le financement du terrorisme. Toutefois, le titulaire du compte doit fournir à l'organisme financier les informations relatives à l'identité de ses clients dont il détient les fonds sur son compte concernés lorsqu'il lui en adresse la demande. Une telle demande pourra résulter, soit de ce que la surveillance du fonctionnement de ce compte fait apparaître des doutes quant à la cohérence des opérations effectuées par rapport aux finalités du compte, de sorte qu'il s'impose à l'établissement financier de s'interroger sur la nécessité de procéder à une déclaration d'opérations suspectes auprès de la CTIF conformément aux articles 23 et suivants de la loi, soit d'une demande d'information que la CTIF a adressée à l'établissement financier en vertu de l'article 33, alinéa 1er de la loi. Toutefois, si en réponse à une telle demande, un avocat atteste par écrit que toutes les personnes dont il détient des fonds sur ce compte sont des clients avec lesquels il est en relation pour évaluer leur situation juridique ou assurer la défense en justice, et s'il refuse pour ce motif de fournir l'information demandée, l'établissement financier n'est pas tenu de mettre fin pour ce motif à la relation d'affaire. Ces circonstances sont en effet celles dans lesquelles l'avocat lui-même n'est pas légalement tenu de refuser ou de rompre la relation d'affaires lorsqu'il n'a pas pu accomplir ses obligations d'identification de son client ou des bénéficiaires effectifs de celui-ci (articles 7, § 5, et 8, § 5, de la loi).

Ces règles s'appliquent non seulement aux notaires et titulaires de professions juridiques indépendantes établis en Belgique, mais également à ceux qui relèvent du droit d'un autre pays membre de l'Espace économique européen, ou du droit d'un pays tiers "équivalent". Les pays tiers remplissant cette condition seront énumérés limitativement par un arrêté royal à prendre en exécution de l'article 37, § 2, alinéa 2, 4°, de la loi.

4.5.2.4. Autorités publiques belges

Article 11, § 1er, 4°, de la loi

Les organismes et personnes visés aux articles 2, § 1er et 3 ne sont pas soumis aux obligations d'identification et de vérification visées aux articles 7 et 8 à l'égard des personnes suivantes:

(...)

4° le client ou le bénéficiaire effectif qui est une autorité publique belge;

(...)

La portée de la notion d'autorité publique belge au sens de cette disposition légale est précisée comme suit par l'exposé des motifs de la loi du 18 janvier 2010 : « *La notion d'autorité publique belge peut être comprise au sens de la notion « d'autorité administrative » prévue à l'article 14, § 1er, des lois coordonnées du 12 janvier 1973 sur le Conseil d'Etat. La description de cette notion a été amplement développée par la doctrine et la jurisprudence du Conseil d'Etat. (« Overzicht van het Belgisch Administratief Recht », A. MAST et J. DUJARDIN, 2006, Kluwer, p. 972 et ss.).»* [25]

4.5.2.5. Autorités ou organismes publics européens

Article 11, § 1er, 5°, de la loi

Les organismes et personnes visés aux articles 2, § 1er et 3 ne sont pas soumis aux obligations d'identification et de vérification visées aux articles 7 et 8 à l'égard des personnes suivantes:

(...)

5° les clients qui sont des autorités ou des organismes publics européens dont la liste est établie par le Roi, conformément à l'article 37, § 2, alinéa 1er, 5°.

(...)

Les autorités ou organismes publics européens visés par cette disposition seront énumérés limitativement par un arrêté royal à prendre en exécution de l'article 37, § 2, alinéa 2, 5°, de la loi.

4.5.2.6. Autres personnes désignées par le Roi

Article 11, § 1er, 6°, de la loi

Les organismes et personnes visés aux articles 2, § 1er et 3 ne sont pas soumis aux obligations d'identification et de vérification visées aux articles 7 et 8 à l'égard des personnes suivantes:

(...)

6° les clients qui relèvent des catégories de personnes ou d'organismes désignés par le Roi en vertu de l'article 37, § 2, alinéa 1er, 6°.

(...)

Actuellement, aucune catégorie de clients n'a été désignée, complémentairement à celles énumérées à l'article 11, § 1er, 1° à 5°, de la loi, comme ne représentant qu'un faible risque et pouvant dès lors bénéficier de la dispense légale d'identification.

4.5.3. Dispenses fondées sur le faible risque lié aux produits

4.5.3.1. Polices d'assurance vie, contrats d'assurance retraite ou régimes de retraite

Article 11, § 2, de la loi

Les organismes et personnes visés aux articles 2, § 1er et 3 ne sont pas soumis aux obligations d'identification et de vérification visées aux articles 7 et 8 en ce qui concerne les produits ou transactions suivants:

1° 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;

2° les contrats d'assurance retraite qui ne comportent pas de clause de rachat et qui ne peuvent être utilisés en garantie;

3° les régimes de retraite ou dispositifs similaires versant des prestations de retraite aux salariés, pour lesquels les cotisations sont prélevées par déduction du salaire et dont les règles ne permettent pas aux participants de transférer leurs droits;

(...)

Ces dispositions de la loi, qui transposent l'article 11, § 5, a), b) et c), de la 3ème Directive, identifient trois catégories de contrats d'assurance-vie ou d'assurances retraites qui peuvent être en principe considérées comme présentant un faible niveau de risque, de sorte qu'il est généralement fait exception aux obligations d'identification et de vérification du souscripteur (le client) ainsi que de ses bénéficiaires effectifs éventuels (actionnaires ou dirigeants) et du ou des bénéficiaires du contrat. Par application de

25 Chambre des Représentants, 2008-2009, Doc 52 1988/001, p. 40.

l'article 7, § 1er, alinéa 1er, 3°, cette dispense cesse de pouvoir être appliquée dès l'instant où il existe un soupçon de blanchiment des capitaux ou de financement du terrorisme (voir section 4.2.2.3 supra).

La CBFA considère que :

- l'article 11, § 2, 1°, de la loi peut trouver à s'appliquer à toute forme d'assurance-vie ou d'assurance décès, individuelle ou collective, qui ne présente qu'un faible risque en raison du montant très limité de la prime unique ou périodique payée par le preneur d'assurance et, par conséquent, de la prestation prévue par le contrat ;
- l'article 11, § 2, 2°, de la loi peut trouver à s'appliquer à toute forme d'assurance-retraite, individuelle ou collective, qui ne présente qu'un faible risque en raison du fait que le contrat ne permet pas au souscripteur ou au bénéficiaire de jouir effectivement de la valeur économique du contrat avant son échéance par la voie d'un rachat ou d'une mise en garantie ;
- l'article 11, § 2, 3°, de la loi peut trouver à s'appliquer, par exemple, aux assurances de pensions complémentaires pour travailleurs salariés qui relèvent du "2ème pilier", qui ne présentent qu'un faible risque en raison du fait que leurs modalités sont fixées de façon impérative par la loi du 28 avril 2003 relative aux pensions complémentaires et au régime fiscal de celles-ci et de certains avantages complémentaires en matière de sécurité sociale, que les primes sont prélevées sur la rémunération du bénéficiaire ou constitue un élément contractuel de son coût salarial, et que le travailleur salarié reste obligatoirement le seul bénéficiaire du droit à la pension complémentaire.

4.5.3.2. Monnaie électronique

Article 11, § 2, de la loi

Les organismes et personnes visés aux articles 2, § 1er et 3 ne sont pas soumis aux obligations d'identification et de vérification visées aux articles 7 et 8 en ce qui concerne les produits ou transactions suivants:

(...)

4° la monnaie électronique au sens de l'article 3, alinéa 1er, 7° de la loi du 22 mars 1993 relative au statut et au contrôle des établissements de crédit pour autant que la capacité maximale de chargement du support ne soit pas supérieure à 150 euros si le support ne peut pas être rechargé ou, si le support peut être rechargé, pour autant qu'une limite de 2.500 euros soit fixée pour le montant total des transactions sur une année civile. Toutefois, les articles 7 et 8 s'appliquent lorsque le porteur demande le remboursement d'un montant d'au moins 1.000 euros au cours de la même année civile et ce, en application de l'article 5quater de la loi du 22 mars 1993 précitée;

(...)

4.5.3.3. Autres produits désignés par le Roi

Article 11, § 2, de la loi

Les organismes et personnes visés aux articles 2, § 1er et 3 ne sont pas soumis aux obligations d'identification et de vérification visées aux articles 7 et 8 en ce qui concerne les produits ou transactions suivants:

(...)

5° les produits et transactions présentant un faible risque de blanchiment de capitaux ou de financement du terrorisme, dont la liste est établie par le Roi conformément à l'article 37, § 2, alinéa 1er, 7°.

Actuellement, aucune catégorie de produits n'a été désignée, complémentairement à celles énumérées à l'article 11, § 2, 1° à 4°, de la loi, comme ne représentant qu'un faible risque de sorte que les clients qui y souscrivent ou les acquièrent pourraient dès lors bénéficier de la dispense légale d'identification.

4.6. Vigilance renforcée lors de l'identification

Article 12, § 1er, de la loi

Sans préjudice des obligations prévues aux articles 7 à 9, les organismes et les personnes visés aux articles 2, § 1er, 3 et 4 appliquent, en fonction de leur appréciation du risque, des mesures de vigilance renforcées à l'égard de la clientèle, dans les situations qui, de par leur nature, peuvent présenter un risque élevé de blanchiment de capitaux et de financement du terrorisme et, à tout le moins, dans les cas visés ci-dessous.

L'article 12 de la loi définit diverses situations qui doivent être obligatoirement considérées comme présentant des risques accrus de blanchiment de capitaux ou de financement du terrorisme, et qui requièrent dès lors que les organismes assujettis à la loi exercent une vigilance accrue à l'égard de ces clients.

Sont notamment visées les situations [[26]] dans lesquelles :

- l'identification et la vérification de l'identité du client sont effectuées à distance (article 12, § 2, de la loi);
- le client, son mandataire, l'un de ses bénéficiaires effectifs ou l'un de ses proches est une "personne politiquement exposée" résidant à l'étranger au sens de la loi (article 12, § 3, de la loi);
- le client est une banque correspondante qui est établie dans un pays tiers et à laquelle la dispense d'identification prévue à l'article 11, § 1er, 1°, de la loi ne trouve pas à s'appliquer (article 12, § 4, de la loi).

Cette énumération n'est cependant pas limitative : une vigilance accrue est également requise dans toutes autres situations présentant un risque élevé de blanchiment de capitaux ou de financement du terrorisme. L'article 12, § 1er, de la loi confie aux organismes financiers eux-mêmes la responsabilité de définir ces situations («... *en fonction de leur appréciation du risque...*»)

Dans l'ensemble de ces situations, il appartient aux organismes d'exercer une vigilance accrue dès le stade de l'identification et de la vérification de l'identité du client, de ses mandataires et de ses bénéficiaires effectifs et/ou de la mise en application de la politique d'acceptation des clients (cf. section 5.2.2 ci-après), et de la prolonger par la suite, dans le cadre de la vigilance constante à l'égard de la relation d'affaires et des opérations du client (cf. section 6.1.5 ci-après).

En premier lieu, il appartient dès lors aux organismes financiers de définir leurs procédures internes relatives à l'entrée en relation avec les clients de manière telle que les situations visées à l'article 12 de la loi soient détectées le plus précocement possible, afin qu'ils puissent en tenir compte au plus tôt dans le processus d'identification et de vérification de l'identité des personnes concernées.

Dans ces mêmes situations, il s'impose en outre que les procédures d'identification et de vérification de l'identité des personnes concernées soient appliquées avec le plus grand soin et que leur mise en œuvre fasse l'objet d'un contrôle renforcé. De plus, il importe que ces procédures prévoient dans ces situations des mesures renforcées en vue de l'identification et de la vérification de l'identité des bénéficiaires effectifs, en ce compris leurs lieux et dates de naissance, et des mesures renforcées en vue de recueillir des informations pertinentes concernant l'adresse exacte du client, de ses mandataires et de ses bénéficiaires effectifs.

4.7. Intervention de tiers pour l'identification et la vérification de l'identité des clients, mandataires et bénéficiaires effectifs

Il convient de distinguer deux types de situations, soumises à des règles différentes, dans lesquelles les organismes financiers peuvent recourir à un tiers pour remplir leurs obligations d'identification et de vérification de l'identité d'un client, de ses mandataires et de ses bénéficiaires effectifs :

- le recours à un agent ou mandataire;
- et le recours à un «tiers introducteur».

4.7.1. Recours à un agent ou mandataire

Article 21 du règlement

Les organismes qui recourent à l'intervention d'agents délégués ou de mandataires pour nouer ou entretenir des relations d'affaires avec les clients ou pour réaliser avec eux des opérations occasionnelles précisent par écrit à ces intervenants les procédures d'identification et de vérification à mettre en œuvre, dans le respect de la loi et du présent règlement, et assurent un contrôle adéquat du respect de ces procédures.

Le recours à de tels intervenants est sans effet sur la responsabilité personnelle de l'organisme quant au respect des dispositions de la loi et du règlement.

Dans le cas ou un organisme recourt à un agent ou à un mandataire, celui-ci effectue l'identification et la vérification de l'identité au nom et pour le compte de l'organisme. Il appartient dès lors à celui-ci de préciser par écrit les procédures à mettre en application par l'agent ou le mandataire, et d'en assurer un contrôle adéquat. L'article 21, alinéa 2, du règlement précise également, pour autant que de besoin, que

[26] Pour un examen détaillé de ces situations, il est renvoyé à la section 5.2.2 ci-après.

le recours à un agent ou à un mandataire n'exonère d'aucune façon l'organisme financier de sa responsabilité propre quant à l'exécution correcte et complète de ses obligations d'identification et de vérification.

4.7.2. Recours à un tiers introducteur

Article 10 de la loi

§ 1er. *Sans préjudice du recours aux mandataires ou sous-traitants agissant sur leurs instructions ainsi que sous leur contrôle et leur responsabilité, les organismes et personnes visés aux articles 2, § 1er, 3 et 4 sont autorisés à faire exécuter les devoirs de vigilance visés à l'article 7, § 1er, 2 et 3, à l'article 8, § 1er et 2 et à l'article 9 par un tiers introducteur d'affaires pour autant que celui-ci soit:*

1° un établissement de crédit ou un établissement financier visé à l'article 2, § 1er, 1) et 2) de la directive 2005/60/CE qui est établi en Belgique ou dans un autre pays de l'Espace économique européen, ou un établissement équivalent établi dans un pays tiers désigné par le Roi en vertu de l'article 37, § 2, alinéa 1er, 2°, dont la législation impose des obligations et un contrôle équivalents à ceux prévus par la directive 2005/60/CE et qui sont soumis à une obligation d'enregistrement professionnel reconnu par la loi ;

2° un commissaire aux comptes, un expert-comptable externe, un conseil fiscal, un notaire ou un membre d'une profession juridique indépendante visé à l'article 2, § 1er, 3), a) et b) de la directive 2005/60/CE établi en Belgique, dans un autre pays de l'Espace économique européen ou dans un pays tiers désigné par le Roi en vertu de l'article 37, § 2, alinéa 1er, 4°, dont la législation impose des obligations et un contrôle équivalents à ceux prévus par la directive 2005/60/CE et qui sont soumis à une obligation d'enregistrement professionnel, reconnu par la loi.

Les organismes et les personnes visés aux articles 2, § 1er, 3 et 4 qui recourent à un tiers introducteur d'affaires conformément à l'alinéa 1er, requièrent de celui-ci qu'il leur transmette immédiatement les informations dont il dispose concernant l'identité du client et, le cas échéant, celle des mandataires et des bénéficiaires effectifs de ce client. Ils exigent également que le tiers introducteur s'engage à leur transmettre sans délai, à première demande, une copie des documents probants au moyen desquels il a vérifié l'identité de ces personnes.

Dans les conditions définies à l'alinéa 1er, les organismes et les personnes visés aux articles 2, § 1er, 3 et 4 peuvent accepter les résultats des devoirs de vigilance qui sont exécutés par un tiers introducteur d'affaires situé dans un pays de l'Espace économique européen ou dans un pays tiers et ce, même si les données ou documents probants sur lesquels portent l'identification ou la vérification de celle-ci diffèrent de ceux requis par la présente loi ou par les mesures prises en exécution de la présente loi.

La responsabilité finale de l'exécution des devoirs de vigilance continue d'incomber aux organismes et personnes visés aux articles 2, § 1er, 3 et 4 qui recourent pour ce faire à un tiers introducteur tel que visé à l'alinéa 1er.

§ 2. *Lorsque les organismes et personnes visés au § 1er, alinéa 1er, 1° et 2° agissent en tant que tiers introducteurs d'affaires, ils mettent immédiatement à la disposition des organismes ou des personnes auprès desquels le client est introduit, les informations dont ils disposent en application des articles 7 et 8 de la présente loi.*

Si les organismes et personnes, établis en Belgique ou à l'étranger, auprès desquels le client est introduit, demandent une copie des documents d'identification et de vérification de celle-ci, les organismes et personnes visés à l'alinéa 1er la leur transmettent sans délai.

Article 22 du règlement

L'intervention d'un tiers introducteur conformément à l'article 10 § 1er, de la loi et à l'article 24 du présent règlement est soumise aux conditions suivantes:

1° l'organisme vérifie préalablement et conserve la documentation sur laquelle il s'est fondé pour vérifier que le tiers introducteur répond aux conditions fixées par l'article 10, § 1er, alinéa 1er, de la loi;

2° le tiers introducteur s'engage préalablement, par écrit, à fournir sans délai à l'organisme les informations d'identification des clients ou des bénéficiaires effectifs qu'il introduira et, à la demande, une copie des documents au moyen desquels il aura vérifié leur identité.

Article 23 du règlement

§ 1er. Les organismes peuvent faire exécuter par un tiers introducteur répondant aux conditions fixées à l'article 10, § 1er, alinéa 1er, de la loi leur obligation de collecte des autres informations visées à l'article 12 du présent règlement et de mise à jour de ces informations, conformément à l'article 30.

§ 2. La faculté de faire exécuter par un tiers introducteur les obligations énumérées à l'article 10, § 1er, alinéa 1er de la loi et au § 1er est néanmoins soumise à la condition que ce dernier ait procédé personnellement à l'identification face-à-face du client.

Article 24 du règlement

Par application de l'article 10, § 1er, alinéa 4, de la loi, l'organisme qui a recours à un tiers introducteur s'assure que l'identification du client introduit et de ses mandataires et bénéficiaires effectifs et la vérification de leur identité ont été complètement et correctement opérées par le tiers introducteur, conformément à la législation qui est applicable à celui-ci. Au besoin, il procède lui-même aux compléments nécessaires d'identification et de vérification, voire à une nouvelle identification et à une nouvelle vérification de l'identité du client introduit, de ses mandataires ou de ses bénéficiaires effectifs, conformément aux dispositions de la loi et du présent règlement.

Le recours à un tiers introducteur se distingue du recours à un agent ou mandataire dans la mesure où le tiers introducteur est lui-même assujetti à des obligations identiques ou équivalentes en matière d'identification, et où il procède à l'identification et à la vérification de l'identité du client, de ses mandataires et de ses bénéficiaires effectifs conformément à la législation nationale à laquelle il est assujetti, et par application de ses propres procédures. Ainsi, par exemple, lorsqu'un client sollicite un prêt hypothécaire auprès d'un établissement de crédit dans le cadre duquel un contrat d'assurance-vie doit être contracté et donné en garantie, l'entreprise d'assurance peut exécuter ses propres obligations d'identification et de vérification de l'identité de son client, ainsi que des éventuels mandataires et bénéficiaires effectifs de celui-ci, en recourant à l'identification et à la vérification d'identité effectuée par l'établissement de crédit pour ses propres besoins. Ce dernier agit alors en qualité de «tiers introducteur» pour l'entreprise d'assurance.

L'on notera que, conformément à ce qu'autorise la 3ème Directive, la loi du 18 janvier 2010 a élargi les catégories de personnes pouvant intervenir en qualité de tiers introducteurs. Ainsi, notamment, les intermédiaires d'assurances non exclusifs visés à l'article 2, § 1er, 7°, de la loi peuvent désormais intervenir en qualité de tiers introducteur au profit d'une entreprise d'assurances.

Les obligations que les organismes sont autorisés à exécuter en recourant à un tiers introducteur sont celles relatives à l'identification et à la vérification de l'identité des clients (art. 7, § 1er, de la loi), de leurs mandataires (art. 7, § 2, de la loi) et de leurs bénéficiaires effectifs (art. 8, § 1er, de la loi), mais également leur obligation de mise à jour, en cas de nécessité, des données d'identification relatives à ces personnes (art. 7, § 3, et 8, § 2, de la loi - voir aussi section 4.8., infra). De plus, l'article 23, § 1er du règlement les autorise également à recourir à un tiers introducteur afin de recueillir les autres informations visées à l'article 12 du règlement et pour la mise à jour des données d'identification de leurs clients, conformément à l'article 30 du règlement.

Sur le plan des modalités concrètes du recours à un tiers introducteur, les conditions fixées à l'article 22, 2°, du Règlement ne doivent pas être vérifiées lorsque le tiers introducteur transmet immédiatement à l'organisme financier auprès duquel le client est introduit tant les données d'identification de ce client que la copie des documents probants au moyen desquels il a vérifié son identité, de sorte que l'organisme financier en dispose effectivement préalablement à la conclusion de la relation d'affaires ou à la réalisation de l'opération avec le client concerné. Cette condition doit en revanche être respectée, soit en vue d'organiser au préalable les introductions de clients prévues pour le futur entre parties, soit lorsqu'à l'occasion de l'introduction d'un client, il est décidé que les copies des documents du client ne seront transmis par le tiers introducteur à l'organisme financier qu'à la demande de celui-ci. Ainsi, par exemple, lorsqu'un courtier en assurances intervient pour la souscription d'une assurance-vie par un client, il n'est requis qu'il adresse à l'entreprise d'assurances concernée un engagement préalable tel que visé à l'article 22, 2°, du règlement que lorsqu'il entre dans les intentions des parties que la copie des documents probants ne soit pas immédiatement transmise par le courtier à l'entreprise d'assurances.

Lorsqu'un tiers introducteur transmet à un organisme financier les données et documents probants d'identification de son client, il les lui transmet avec toutes leurs caractéristiques, sans que celles-ci ne soient altérées. Ainsi, le tiers introducteur ayant procédé par hypothèse à l'identification face à face du client pour remplir ses propres obligations (cf. infra), l'organisme financier auprès duquel il introduit son client est autorisé à considérer qu'il a lui-même procédé, à l'intervention du tiers introducteur, à une identification face à face de ce client. Il n'est dès lors pas tenu de mettre en œuvre les mesures de

vigilance accrue requises dans le cas de relations à distance. De même, le tiers introducteur ayant par hypothèse vérifié l'identité du client au moyen d'un document probant original (par exemple, la carte d'identité ou le passeport du client), l'organisme financier auprès duquel le tiers introducteur introduit le même client et auquel il transmet une copie du document probant utilisé pour la vérification de l'identité est également autorisé à considérer que la vérification a été opérée au moyen de l'original d'un document probant, bien qu'il ne puisse recevoir du tiers introducteur qu'une copie de ce document probant.

Dans la logique de l'approche rappelée ci-dessus, l'article 10, § 1er, alinéa 3, de la loi applique en outre dans cette hypothèse le principe de reconnaissance mutuelle des législations au sein de l'Espace Economique Européenne, ainsi que l'équivalence des législations des pays tiers dont la liste sera fixée par arrêté royal (cf. section 4.5.2.1., supra). Il s'ensuit que les organismes soumis à la loi du 11 janvier 1993 peuvent considérer comme satisfaisants au regard de celle-ci les résultats de l'identification et de la vérification de l'identité des personnes concernées qui ont été effectuées par le tiers introducteur conformément à la législation ou à la réglementation qui lui est applicable même si les modalités d'exécution de ces obligations diffèrent de celles prévues en droit belge.

Cependant, afin de conserver un degré élevé de fiabilité des données d'identification recueillies par les organismes à l'intervention d'un tiers introducteur, cette intervention n'est autorisée, en vertu de l'article 23, § 2, du règlement, que si le tiers introducteur a procédé personnellement à une identification face-à-face du client. Il apparaît en effet qu'un recours en chaîne à des identifications à l'intervention de tiers introducteurs successifs ou l'identification à distance du client par le tiers introducteur seraient de nature à amoindrir la confiance dont les organismes peuvent créditer les informations d'identification reçues.

Il convient également de souligner que lorsqu'un client a été identifié à l'intervention du tiers introducteur, celui-ci doit transmettre sans retard les données d'identification à l'organisme. En revanche, la copie des documents au moyen desquels l'identité a été vérifiée ne doit être communiquée qu'à la demande de l'organisme. Une telle demande doit être adressée au tiers introducteur, soit si l'organisme a des raisons de douter de l'identité du client, soit en vue de répondre à une question des autorités. Dans ce cas, le tiers doit être à même de fournir sans retard la copie du document demandé.

Il importe également de souligner que le recours à un tiers introducteur ne reporte pas sur celui-ci la responsabilité de l'organisme qui a recours à lui (art. 10, § 1er, alinéa 4, de la loi). L'article 24 du règlement précise par conséquent que lorsque le résultat de l'identification et de la vérification apparaît incomplet ou insatisfaisant, il appartient à l'organisme financier de compléter, de corriger, voire de recommencer l'identification et la vérification de l'identité du client, de ses mandataires et/ou de ses bénéficiaires effectifs.

5. Politique d'acceptation des clients

5.1. Objectifs de la politique d'acceptation des clients

Article 26, alinéa 1er du règlement

Les organismes arrêtent et mettent en œuvre une politique d'acceptation des clients appropriée aux activités qu'ils exercent, permettant de soumettre l'entrée en relations d'affaires ou la conclusion d'opérations avec les clients à une évaluation préalable des risques de réputation associés au profil du client et à la nature de la relation d'affaire ou de l'opération souhaitée. La politique d'acceptation des clients doit prévoir une attribution des compétences de décision au niveau hiérarchique adéquat pour tenir compte de l'importance de ces risques. La politique d'acceptation des clients doit également permettre à l'organisme de concourir pleinement à la prévention du blanchiment de capitaux et du financement du terrorisme par une prise de connaissance et un examen appropriés des caractéristiques des nouveaux clients et/ou des services ou opérations pour lesquels ils les sollicitent.

D'une manière générale, la politique d'acceptation des clients telle que définie à l'article 26, alinéa 1er, du règlement constitue un outil essentiel de la gestion des risques de réputation susceptibles d'être associés aux relations d'affaires ou des opérations avec de nouveaux clients.

Elle se concrétise essentiellement dans :

- une évaluation préalable de ces risques, et
- l'attribution du pouvoir de décider de nouer la relation d'affaires ou d'effectuer l'opération souhaitée par le client à des personnes d'un niveau hiérarchique adéquat au regard du niveau évalué de ces risques.

La politique d'acceptation des clients constitue l'un des éléments de la « politique d'intégrité » que l'organe de direction effective doit élaborer et actualiser régulièrement, sous la surveillance du conseil d'administration, conformément aux principes énoncés par la CBFA dans les circulaires relatives à la « fonction de compliance » qu'elle a adressées aux établissements de crédit, entreprises d'investissement et entreprises d'assurances [27].

Indépendamment du respect des obligations légales en matière de prévention du blanchiment de capitaux et du financement du terrorisme, cette prévention apparaît en effet également capitale au regard des exigences d'une gestion saine et prudente du risque de réputation. De ce point de vue, le respect purement formel, notamment, des obligations d'identification des clients, mandataires et bénéficiaires effectifs, et de communication à la CTIF des opérations ou des faits visés aux articles 23 à 25 et 28 de la loi apparaît insuffisant. En effet, la réputation d'un organisme pourrait être gravement entachée du fait de relations ou d'opérations importantes qu'il aurait nouées avec un client convaincu de blanchiment de capitaux ou de financement du terrorisme, si, par son comportement, cet organisme n'a pas effectivement concouru pleinement à l'application de la loi et, plus généralement, à la prévention effective du blanchiment de capitaux et du financement du terrorisme.

Dans cette perspective, la « politique d'acceptation des clients » que les organismes sont tenus de mettre en application complémentairement au respect des règles relatives à l'identification des clients et aux devoirs de vigilance à l'égard des opérations et des relations d'affaires, doit leur permettre effectivement de concourir pleinement à la prévention du blanchiment de capitaux et du financement du terrorisme par une prise de connaissance et un examen appropriés des caractéristiques des nouveaux clients qui les sollicitent et/ou des services ou opérations pour lesquels ils les sollicitent, notamment au regard du risque de blanchiment de capitaux ou de financement du terrorisme.

La politique d'acceptation des clients doit également permettre à chaque organisme de s'assurer qu'il satisfait à ses obligations en matière d'embargo financier, en ce compris en matière de gel des avoirs de certaines personnes et entités dans le cadre de la lutte contre le terrorisme, conformément aux arrêtés royaux et arrêtés ministériels pris en vertu de l'arrêté-loi du 6 octobre 1944 organisant le contrôle de tous transferts quelconques de biens et valeurs entre la Belgique et l'étranger [28], de la loi du 11 mai 1995 relative à la mise en œuvre des décisions du Conseil de Sécurité de l'Organisation des Nations Unies [29], ou de la loi du 13 mai 2003 relative à la mise en œuvre des mesures restrictives adoptées par le Conseil de l'Union européenne à l'encontre d'Etats, de certaines personnes et entités [30]. La politique d'acceptation des clients doit dès lors permettre aux organismes financiers de mettre effectivement en œuvre les mesures restrictives adoptées par le Conseil européen par la voie de règlements tels que, notamment, et de façon non exhaustive:

- le règlement (CE) nº 1081/2000 du Conseil du 22 mai 2000 concernant l'interdiction de la vente, de la fourniture et de l'exportation à la Birmanie/au Myanmar de matériel susceptible d'être utilisé à des fins de répression interne ou de terrorisme, et le gel des fonds appartenant à certaines personnes ayant un lien avec d'importantes fonctions gouvernementales dans ce pays [31],
- le règlement (CE) n° 2580/2001 du Conseil du 27 décembre 2001 concernant l'adoption de mesures restrictives spécifiques à l'encontre de certaines personnes et entités dans le cadre de la lutte contre le terrorisme [32],
- le règlement (CE) n° 881/2002 du Conseil du 27 mai 2002 instituant certaines mesures restrictives spécifiques à l'encontre de certaines personnes et entités liées à Oussama Ben Laden, au réseau Al-Qaïda et aux talibans [33],
- le règlement (CE) n° 305/2006 du Conseil du 21 février 2006 instituant des mesures restrictives spécifiques à l'encontre de certaines personnes soupçonnées d'être impliquées dans l'assassinat de l'ancien Premier Ministre libanais M. Rafiq Hariri [34],

---

27 - Circulaire D1 2001/13 du 18 décembre 2001 aux établissements de crédit.
- Circulaire D1/EB/2002/6 du 14 novembre 2002 aux entreprises d'investissement.
- Circulaire PPB/D.255 du 10 mars 2005 aux entreprises d'assurances.

28 *M.B.*, 7 octobre 1944, modifié par la loi du 28 février 2002 organisant l'établissement de la balance des paiements et de la position extérieure globale de la Belgique et portant modification de l'arrêté-loi du 6 octobre 1944 relatif au contrôle des changes et de diverses dispositions légales, *M.B.*, 3 mai 2002, éd. 2, p. 18700.

29 *M.B.*, 29 juillet 1995, p. 20444.

30 *M.B.*, 13 juin 2003, p. 31923 + errata *M.B.*, 20 juin 2003, p. 33191.

31 JO n° L 122 du 24 mai 2000, p. 29.

32 JO n° L 344 du 28 décembre 2001 p. 70.

33 JO n° L 139 du 29 mai 2002, p. 9.

34 JO n° L 51 du 22 février 2006, p. 1.

- le règlement (CE) n° 329/2007 du Conseil du 27 mars 2007 concernant l'adoption de mesures restrictives à l'encontre de la République populaire démocratique de Corée [35],
- le règlement (UE) n° 961/2010 du Conseil du 25 octobre 2010 concernant l'adoption de mesures restrictives à l'encontre de l'Iran et abrogeant le règlement (CE) n° 423/2007 [36],
- etc.

Ceci suppose notamment qu'une vérification soit opérée pour s'assurer que le client, ses mandataires éventuels et ses bénéficiaires effectifs ne sont pas des personnes reprises dans les listes d'embargo qui sont d'application [37].

Dans l'hypothèse où les avoirs d'une personne concernée devraient être gelés, il y a lieu de prendre contact au plus vite avec le SPF Finance - Département de la Trésorerie [38].

L'attention est également attirée sur le fait que les infractions aux embargos financiers sont pénalement sanctionnées (cf. notamment l'article 6 de la loi précitée du 13 mai 2003 en ce qui concerne les infractions aux mesures restrictives édictées par le Conseil européen).

5.2. Echelle de risques

5.2.1. Combinaison de critères de risque obligatoires et spécifiques

Article 26, alinéas 2 et 3, du règlement

Par application de leur politique d'acceptation, les organismes répartissent leurs clients en différentes catégories de risques auxquelles s'appliquent des exigences de niveaux différents. Ces catégories sont définies sur la base de critères objectifs de risque qui sont combinés de manière cohérente entre eux pour définir une échelle appropriée des risques. Celle-ci tient pleinement compte :

- *des situations de risque accru de blanchiment des capitaux ou de financement du terrorisme définies à l'article 12, §§ 2, 3 et 4, de la loi et à l'article 27 du présent règlement, et*
- *des critères de risque définis par chaque organisme en tenant compte, notamment, des caractéristiques des services et produits qu'il offre et de celles de la clientèle à laquelle il s'adresse.*

La politique d'acceptation des clients peut également tenir compte des situations de risque faible de blanchiment des capitaux ou de financement du terrorisme définies à l'article 11, §§ 1er et 2, de la loi.

La politique d'acceptation doit s'appuyer sur une échelle des risques constituée par la combinaison de critères de risques objectifs et pertinents. Certains de ces critères résultent des dispositions-mêmes de la loi ou du règlement ("critères obligatoires"). D'autres doivent être définis par chaque organisme afin de tenir pleinement compte de ses caractéristiques propres ("critères spécifiques").

5.2.2. Critères de risque obligatoires

L'échelle de risque sur laquelle se fonde la politique d'acceptation des clients doit logiquement tenir pleinement compte des situations que la loi ou le règlement identifient comme objectivement risquées. Ainsi en est-il des situations visées par l'article 12 de la loi. L'article 27 du règlement identifie également plusieurs situations de risque accru dont la politique d'acceptation des clients doit tenir compte.

5.2.2.1. Identification et vérification de l'identité à distance

Article 12, § 2, de la loi

Sans préjudice des obligations prévues aux articles 7 à 9, les organismes et personnes visés aux articles 2, § 1er, 3 et 4 prennent les dispositions spécifiques et adéquates qui sont nécessaires pour faire face au risque accru de blanchiment de capitaux et de financement

35 JO n° L 88 du 29 mars 2007, p. 1. - voir aussi sections 6.1.2, 7.2 et 9 infra.
36 JO n° L 281 du 27 octobre 2010, p. 1. - voir aussi section 6.1.2, 7.2 et 9 infra.
37 Un relevé des embargos qui sont d'application peut être consulté sur le site de Febelfin : http://www.febelfin.be/febelfin/fr/Embargos_financiers/
38 Fax : n° + 32 2 233 74 65; e-mail : quesfinvragen.tf@minfin.fed.be. De plus amples informations peuvent aussi être obtenues sur le site internet : http://iefa.fgov.be/fr/Topics_Sanctions.htm

du terrorisme qui existe lorsqu'ils nouent une relation d'affaires ou effectuent une transaction avec un client qui n'est pas physiquement présent lors de l'identification.

Article 29 du règlement

Sans préjudice des dispositions de l'article 7, § 2, et du chapitre 10 du présent règlement, les organismes qui nouent des relations d'affaires ou réalisent des opérations occasionnelles avec des clients, personnes physiques, qu'ils ont identifiés à distance mettent en œuvre, par application de l'article 12, § 2, de la loi, des procédures qui :

- *interdisent de nouer une relation d'affaires ou de réaliser une opération occasionnelle avec un client identifié à distance, lorsqu'il existe des raisons de croire que le client cherche à éviter un contact face-à-face afin de dissimuler plus aisément sa véritable identité, ou qu'il a l'intention de procéder à des opérations de blanchiment de capitaux ou de financement du terrorisme;*
- *imposent, en fonction du risque, des mesures spécifiques complémentaires visant à corroborer les informations d'identification obtenues sur la base du document probant visé à l'article 7, § 2;*
- *imposent, en fonction du risque, de procéder dans un délai raisonnable à la vérification de l'identité des clients ayant été identifiés au moyen d'un document visé l'article 7, § 2, alinéa 2, au moyen d'un autre document probant visé à l'article 7, § 1er, ou § 2, alinéa 1er ;*
- *permettent d'améliorer progressivement la connaissance du client;*
- *excluent les opérations impliquant ou permettant le maniement d'argent liquide, à l'exception des opérations de retraits d'espèces au moyen d'un automate sur le compte courant ouvert au nom d'un client identifié au moyen d'un document visé à l'article 7, § 2, alinéa 1er;*
- *excluent les opérations impliquant le maniement d'instruments financiers incorporés dans des titres au porteur.*

L'article 12, § 2, de la loi énonce le principe selon lequel les organismes sont tenus de prendre des mesures spécifiques et adéquates nécessaires pour faire face au risque accru qui doit obligatoirement être reconnu lorsque le client est identifié à distance. L'article 29 du règlement précise la portée des mesures requises pour limiter ce risque, sans que cet encadrement spécifique ne porte préjudice à l'application des autres aspects de la politique d'acceptation des clients, ni à l'exercice des devoirs de vigilance commentés au chapitre 6 ci-après.

Ces mesures visent, d'une part, à tendre vers une identification plus fiable et une meilleure connaissance du client et, d'autre part, à limiter le risque que des opérations de blanchiment de capitaux ou de financement du terrorisme soient réalisées.

Dans tous les cas, le premier devoir qui s'impose aux organismes lorsqu'une identification est réalisée à distance consiste à s'interroger si le client ne recourt pas à cette procédure d'identification pour dissimuler plus aisément sa véritable identité. Si tel devait être le cas, l'article 7, § 3, de la loi interdirait à l'organisme de nouer la relation d'affaires ou de réaliser l'opération souhaitée par le client et, le cas échéant, une information pourrait devoir être communiquée à la CTIF.

Par ailleurs, les mesures à arrêter par chaque organisme doivent être définies en fonction du niveau de risque lié à la procédure d'identification.

Ainsi, par exemple, une identification à distance en vue de nouer une relation d'affaires, dans le cadre de laquelle des contacts réguliers avec le client seront entretenus, peut être considérée comme moins risquée qu'une identification à distance en vue de réaliser une opération occasionnelle. De même, une identification à distance au moyen d'une carte d'identité électronique peut être considérée comme générant moins de risques d'erreur qu'au moyen d'un certificat d'identification et, a fortiori, qu'au moyen d'une copie de document probant.

S'agissant de clients identifiés au moyen d'une copie de document probant, le règlement prévoit certaines règles spécifiques renforcées. D'une part, son article 7, § 2, alinéa 2, exclut que la vérification à distance de l'identité du client soit opérée au moyen d'une copie de document probant non vérifiée auprès du Registre national lorsque le client souhaite effectuer une opération occasionnelle. D'autre part, l'article 29, 3ème tiret, du règlement requiert qu'en fonction du risque, l'identité du client soit vérifiée dans un délai raisonnable au moyen d'un autre document probant. Si la nature du risque l'exige, l'acceptation d'une copie de document probant visée à l'article 7, § 2, alinéa 2, du règlement peut donc n'être que provisoire. Les procédures internes doivent imposer une nouvelle vérification au moyen d'un autre document probant dès l'instant où, dans le courant de la relation d'affaire, l'exercice de la vigilance

constante fait apparaître qu'un risque particulier de blanchiment de capitaux ou de financement du terrorisme est associé au client ou à la relation d'affaires.

Dans le même sens, les règles spécifiques arrêtées par les organismes par application de l'article 12, § 2, de la loi doivent également soumettre à une vigilance toute particulière les relations nouées avec des clients identifiés à distance au moyen de tels documents.

Dans le but de corroborer les données d'identification du client et d'améliorer la connaissance que l'organisme a de son client, les mesures spécifiques complémentaires peuvent notamment consister:
- à requérir du client la production de documents complémentaires corroborant son identification;
- à procéder à des recoupements avec les informations pouvant être obtenues auprès de sources dignes de foi étrangères au client;
- à mettre en place une procédure d'identification face-à-face ultérieure dès que cela s'avère possible;
- à exiger que le client indique l'identité de son organisme financier habituel établi dans un Etat membre de l'Espace économique européen ou dans un pays tiers équivalent, et qu'il autorise la collecte directe d'informations auprès de cet établissement;
- à exiger que le client procède à un premier versement sur le compte ouvert à distance au départ d'un compte ouvert à son nom auprès d'un autre établissement financier établi dans un Etat membre de l'Espace économique européen ou dans un pays tiers équivalent;
- à prévoir des envois réguliers de courriers nominatifs à l'adresse du client et à mettre en œuvre un suivi attentif des retours de courrier;
- etc.

Par ailleurs, afin de réduire le risque d'opérations de blanchiment de capitaux ou de financement du terrorisme, les règles internes doivent au minimum exclure les opérations impliquant le maniement d'argent liquide ou d'instruments financiers incorporés dans des titres au porteur. Toutefois, une exception est prévue à cette exclusion pour les retraits d'espèces opérés au moyen d'un automate par le client sur le compte ouvert à son nom, pour autant que la vérification de son identité n'ait pas été effectuée au moyen d'une simple copie de document probant non vérifiée auprès du Registre National. Ces limitations se justifient dans la mesure où, à défaut d'une identification suffisamment fiable du client, ces opérations apparaissent particulièrement susceptibles d'être utilisées à des fins de blanchiment de capitaux ou de financement du terrorisme. En outre, à l'exception des retraits aux automates, ces opérations requièrent par nature la présence physique du client, et elles fournissent donc nécessairement l'occasion de confirmer l'identification opérée à distance par une identification face-à-face permettant de lever ces limitations. S'agissant de l'ouverture d'un compte bancaire à distance à un client dont l'identité a été vérifiée au moyen d'une simple copie de document probant dont la véracité n'a pas été, ou n'a pas pu être vérifiée par la consultation du Registre national, il convient de considérer comme exclu par application de l'article 29, 5ème tiret, du règlement l'octroi au client d'une carte de débit, d'une carte de crédit ou de tout autre instrument de paiement lié au compte et permettant d'effectuer de quelque manière que ce soit des retraits ou des dépôts en espèces.

5.2.2.2. Personnes politiquement exposées

5.2.2.2.1. Principes et personnes visées

Article 12, § 3, alinéas 1 à 5, de la loi

Sans préjudice des obligations prévues aux articles 7 à 9, les organismes et personnes visés aux articles 2, § 1er, 3 et 4 prennent les mesures spécifiques visées ci-après lorsqu'ils nouent des relations d'affaires ou lorsqu'ils effectuent des transactions avec ou pour le compte:
1° de personnes politiquement exposées résidant à l'étranger, à savoir des personnes physiques qui occupent ou ont exercé une fonction publique importante;
2° de membres directs de la famille des personnes visées au 1°;
3° ou des personnes connues pour être étroitement associées aux personnes visées au 1°.
Aux fins de l'application du présent paragraphe on entend par «des personnes physiques qui occupent ou ont exercé une fonction publique importante»:
1° les chefs d'État, les chefs de gouvernement, les ministres, ministres délégués et secrétaires d'État;
2° les parlementaires;
3° les membres des cours suprêmes, des cours constitutionnelles ou d'autres hautes juridictions dont les décisions ne sont habituellement pas susceptibles de recours;
4° les membres des cours des comptes et la direction des banques centrales;
5° les ambassadeurs, les chargés d'affaires et les officiers supérieurs des forces armées;

6° les membres des organes d'administration, de direction ou de surveillance des entreprises publiques.

Aucune des catégories citées à l'alinéa 2 n'est réputée comprendre des personnes occupant une fonction de niveau intermédiaire ou subalterne. Les catégories visées à l'alinéa 2 comprennent, le cas échéant, les fonctions exercées au niveau européen ou international. Sous réserve de l'application de mesures de vigilance renforcées en fonction d'une appréciation du risque lié à la clientèle, les organismes et les personnes visés aux articles 2, § 1er, 3 et 4 ne sont pas tenus de considérer comme politiquement exposée, une personne qui n'a pas occupé de fonction publique importante, au sens de l'alinéa 2, pendant une période d'au moins un an.

Aux fins de l'application du présent paragraphe, on entend par «les membres directs de la famille des personnes visées à l'alinéa 1er, 1° »:

1° le conjoint;
2° tout partenaire considéré par le droit national de la personne visée à l'alinéa 1er, 1°, comme l'équivalent d'un conjoint;
3° les enfants et leurs conjoints ou partenaires;
4° les parents.

Aux fins de l'application du présent paragraphe, on entend par « des personnes étroitement associées aux personnes visées à l'alinéa 1er, 1° »:

1° toute personne physique connue pour être, conjointement avec une personne visée à l'alinéa 1er, 1°, le bénéficiaire effectif d'une personne morale ou d'une construction juridique ou pour entretenir toute autre relation d'affaires étroite avec une telle personne;
2° toute personne physique qui est le seul bénéficiaire effectif d'une personne morale ou d'une construction juridique connue pour avoir été, de facto, créée au profit d'une personne visée à l'alinéa 1er, 1°.

L'article 12, § 3, de la loi transpose en droit belge l'article 13.4 de la directive 2005/60/CE du 26 octobre 2005 (3ème directive) et l'article 2 de la directive 2006/70/CE du 1er août 2006 (directive de mise en œuvre) qui établissent un régime harmonisé de vigilance accrue à l'égard des "personnes politiquement exposées", en conformité avec la recommandation 6 du GAFI [39].

Ce régime comprend une définition précise des critères qui déterminent si une personne doit être considérée comme « politiquement exposée », soit en raison des fonctions publiques importantes qu'elle-même exerce ou a exercé (article 12, § 3, alinéa 1er, 1°, et alinéas 2 et 3), soit en raison du fait qu'elle est un proche parent d'une personne exerçant ou ayant exercé de telles fonctions (article 12, § 3, alinéa 1er, 2°, et alinéa 4), soit en raison du fait qu'elle est connue pour être étroitement associée à une personne exerçant ou ayant exercé de telles fonctions (article 12, § 3, alinéa 1er, 3°, et alinéa 5). Cette énumération des personnes visées à l'article 12, § 3, de la loi est limitative.

Ces nouvelles dispositions légales appellent les commentaires suivants.

Par rapport au régime spécifique qui était antérieurement prévu par le règlement, il est à souligner que seules sont désormais visées les personnes politiquement exposées qui résident à l'étranger. L'on relèvera en revanche que la condition de résidence à l'étranger n'est pas prévue en ce qui concerne les membres de la famille proche des personnes politiquement exposées et les personnes qui leur sont étroitement associées.

Par ailleurs, la notion de « personnes étroitement associées à des personnes politiquement exposées » ne vise désormais plus que des personnes physiques (cf. article 12, § 3, alinéa 5). Néanmoins, l'article 12, § 3, alinéa 1er impose également l'exercice de la vigilance accrue lorsque des relations d'affaires sont nouées ou des opérations effectuées pour le compte de personnes politiquement exposées. L'exigence de vigilance accrue trouve dès lors également à s'appliquer aux clients - le cas échéant, des personnes morales - dont un ou plusieurs bénéficiaires effectifs sont des personnes politiquement exposées. Tel serait par exemple le cas des sociétés patrimoniales, des sociétés de management ou des sociétés familiales appartenant à une personne politiquement exposée.

Il convient également de souligner que, même dans les cas où l'article 12, § 3, de la loi ne trouve pas à s'appliquer, les organismes financiers demeurent tenus par ailleurs d'exercer une vigilance constante proportionnée au profil de risque de chaque client (cf. article 12, § 1er de la loi, et sections 6.1.4 et 6.1.5., infra).

39 L'article 43, § 3, de la loi du 11 janvier 1993 prévoit une période transitoire d'un an à dater de l'entrée en vigueur de la loi du 18 janvier 2009 pour identifier les clients qui sont des personnes politiquement exposées et mettre en œuvre à leur égard les mesures de vigilance renforcée requises par la loi.

Ainsi, notamment, bien que l'encadrement spécifique prévu à l'article 12, § 3, de la loi ne trouve pas à s'appliquer aux clients qui exercent ou ont exercé des fonctions publiques à un niveau inférieur au niveau national, la CBFA recommande aux organismes financiers, dans la ligne du 3ème Considérant de la Directive 2006/70/CE, d'évaluer s'il s'indique de mettre en œuvre, en fonction du risque, des mesures de vigilance analogues à l'égard de clients qui exercent des fonctions publiques importantes à ces autres niveaux de pouvoir, lorsque le degré d'exposition politique qui y est lié est comparable à celui de personnes occupant des positions analogues au niveau national.

De même, bien que l'article 12, § 3, alinéa 1er, de la loi ne soit pas d'application aux personnes qui exercent des fonctions publiques importantes à l'étranger mais qui résident en Belgique, la CBFA recommande aux organismes financiers d'évaluer, en fonction du risque, si des mesures de vigilance renforcée analogues à celles prévues par l'article 12, § 3, de la loi devraient être mises en œuvre. Il en va de même lorsque le client est un membre de la proche famille d'une Personne Politiquement Exposée non visée à l'article 12, § 3, alinéa 4 de la loi ou une personne ayant cessé d'exercer depuis un an ou plus une fonction politique importante visée à l'alinéa 2 du même article.

5.2.2.2.2. Mesures spécifiques requises

Article 12, § 3, alinéa 6, de la loi

Les mesures spécifiques requises incluent:

1° de mettre en œuvre des procédures adéquates et adaptées, en fonction du risque, de manière à pouvoir déterminer si le client ou un bénéficiaire effectif du client est une personne politiquement exposée;

2° d'obtenir l'autorisation d'un niveau adéquat de la hiérarchie avant de nouer une relation d'affaires avec de tels clients;

3° de prendre toute mesure appropriée, en fonction du risque, pour établir l'origine du patrimoine et l'origine des fonds impliqués dans la relation d'affaires ou la transaction;

4° d'assurer une surveillance continue renforcée de la relation d'affaires.

La première obligation des organismes consiste à déterminer la méthodologie permettant de déterminer si le client rencontre les critères qui le qualifient de « personne politiquement exposée ».Compte tenu du commentaire fourni par le Considérant n° 2 de la directive 2006/70/CE, il est à noter que l'obligation de déterminer si un client relève de l'une des catégories énumérées à l'article 12, § 3, alinéa 1er, de la loi est une obligation de moyens et non de résultats. Il importe néanmoins que les méthodes définies par les procédures internes et effectivement mises en application apparaissent suffisantes pour raisonnablement permettre l'identification de ces clients.

A cet effet, la politique d'acceptation des clients peut prescrire, par exemple, de consulter des sources d'informations fiables qu'elle désigne, ou de s'appuyer sur les déclarations recueillies auprès du client, par exemple, par la voie de l'inclusion de questions appropriées dans les documents de demande d'ouverture de relations ou, en matière d'assurances-vie, dans les documents précontractuels. Une combinaison des deux méthodes pourrait également utilement être retenue. Ainsi, lorsque des informations publiquement disponibles, telles que des articles de presse, semblent indiquer qu'un client pourrait relever de l'une des catégories définies à l'article 12, § 3, alinéa 1er, de la loi, les procédures d'acceptation des clients des organismes financiers pourraient prévoir que des questions spécifiques soient posées au client afin de clarifier son statut au regard de cette disposition légale. En toute hypothèse, il est également rappelé que les informations à caractère personnel collectées à propos du client doivent être proportionnées aux finalités poursuivies par la loi, afin d'éviter que cette collecte d'informations constitue une intrusion excessive dans la vie privé des clients.

Lorsqu'un client est identifié comme relevant de l'une des catégories visées à l'article 12, § 3, alinéa 1er, de la loi, les procédures internes devraient définir des critères permettant de déterminer le niveau hiérarchique de la ou des personnes appelées à autoriser, pour l'organisme financier, sous le contrôle et la responsabilité de la haute direction, la relation d'affaires ou l'exécution de l'opération avec ce client. Ces critères peuvent tenir compte d'une combinaison du risque associé au profil du client et de celui qui est inhérent à la nature de la relation d'affaires ou de l'opération à conclure.

De même, les procédures d'acceptation des clients devraient spécifier les mesures requises en vue de déterminer l'origine des fonds impliqués dans la relation d'affaires. Ces mesures devraient également tenir adéquatement compte de la combinaison du risque associé au profil du client et de celui qui est inhérent à la nature de la relation d'affaires ou de l'opération à conclure. Des critères liés à l'importance des sommes impliquées pourraient également être pris en considération.

Quant aux mesures spécifiques de surveillance des opérations du client qui sont requises en vertu de l'article 12, § 3, alinéa 6, 4°, de la loi, il est renvoyé à la section 6.1.4 ci-dessous.

5.2.2.3. Correspondants bancaires

Article 12, § 4 de la loi

Sans préjudice des obligations visées aux articles 7 et 8 et des dérogations prévues à l'article 11, § 1er, 1°, les organismes et personnes visés à l'article 2, § 1er qui nouent des relations transfrontalières de correspondants bancaires avec des établissements correspondants de pays tiers sont tenus :

1° de recueillir sur l'établissement correspondant 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;

2° d'évaluer les contrôles anti-blanchiment et en matière de lutte contre le financement du terrorisme mis en place par l'établissement correspondant;

3° d'obtenir l'autorisation d'un niveau adéquat de leur hiérarchie avant de nouer de nouvelles relation;

4° d'établir, par convention écrite, les responsabilités respectives de chaque établissement;

5° de s'assurer, en ce qui concerne les « comptes de passage» («payable through accounts»), que l'établissement 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.

Ils ne peuvent ni nouer ni maintenir une relation de correspondant bancaire avec une société bancaire écran, et sont tenus de prendre des mesures appropriées pour garantir qu'ils ne nouent pas ou ne maintiennent pas une relation de correspondant bancaire avec un établissement connu pour permettre à une société bancaire écran d'utiliser ses comptes.

Article 28, § 1er, du règlement

Lorsque le client est un établissement de crédit ou une institution financière de droit étranger visés à l'article 12, § 4, de la loi, la décision de nouer la relation d'affaires ou l'opération occasionnelle envisagée doit être fondée sur un dossier contenant les éléments permettant de démontrer que les obligations définies à l'article 12, § 4, de la loi sont remplies. L'organisme doit tenir ce dossier à jour.

Pour rappel, et sous les réserves énoncées aux sections 4.5.1 et 4.5.2.1 supra, l'article 11, § 1er, 1°, de la loi autorise la mise en œuvre d'une vigilance simplifiée lors de l'identification des clients et des bénéficiaires effectifs qui sont des établissements de crédit ou des établissements financiers visés à l'article 2 de la directive 2005/60/CE établis en Belgique ou dans un autre pays de l'Espace économique européen ou un établissement équivalent établi dans un pays tiers imposant des obligations et un contrôle équivalents à ceux prévus par la directive 2005/60/CE. Dans ces cas, les organismes sont dès lors également dispensés de l'obligation de soumettre la conclusion de relations de correspondance bancaire [40] avec ces clients à des règles renforcées d'acceptation des clients.

En revanche, lorsque l'établissement de crédit ou l'établissement financier client est établi dans un autre pays que ceux visés à l'article 11, § 1er, 1°, de la loi, et que des relations de banques correspondantes sont envisagées, l'article 12, § 3, de la loi, complété par l'article 28, § 1er, du règlement, précise les conditions dans lesquelles des relations ou opérations peuvent être nouées avec lui.

Ces règles comprennent notamment l'obligation de vérifier qu'il ne s'agit pas d'un établissement fictif ("*une société bancaire écran")* ou qui accepte de nouer des relations ou des opérations avec de tels établissements fictifs.

Elles imposent que la décision de nouer la relation d'affaires s'appuie sur une identification complète de l'établissement client, et sur une analyse critique du régime légal et réglementaire de prévention du blanchiment de capitaux et du financement du terrorisme du pays d'établissement, d'une part, et de la réputation de l'établissement client, d'autre part.

Les procédures internes devraient en outre préciser le niveau hiérarchique de la ou des personnes ayant le pouvoir d'autoriser, sous le contrôle et la responsabilité de la haute direction, la conclusion de relations d'affaires avec des banques correspondantes.

40 Peuvent être qualifiés de correspondants bancaires les établissements bancaires avec lesquels sont nouées des relations contractuelles aux termes desquelles sont offerts ou reçus des services de paiement ou diverses autres prestations de services interbancaires.

De plus, des mesures complémentaires et renforcées sont à mettre en œuvre lorsque des comptes de passage sont à ouvrir à l'établissement étranger, afin d'empêcher que les clients de cet établissement utilisent l'organisme pour réaliser des opérations liées au blanchiment de capitaux ou au financement du terrorisme au moyen du compte de passage.

L'article 28, § 1er, du règlement impose l'établissement d'un dossier permettant de démontrer que la décision de nouer la relation d'affaires a effectivement été prise en conformité avec les exigences de la loi.

5.2.2.4. Cas particuliers visés à l'article 27 du règlement

Article 27 du règlement

La politique d'acceptation des clients des organismes soumet à un examen particulier et à un pouvoir de décision à un niveau hiérarchique adéquat l'acceptation des clients susceptibles de présenter des niveaux particuliers de risque, notamment ceux:

- *qui sollicitent l'ouverture de comptes numérotés visés à l'article 5, alinéa 2;*
- *qui sollicitent la fourniture de services de gestion de fortune;*
- *qui résident ou ont leur domicile dans un pays ou un territoire qualifié de pays ou territoire non coopératif par le Groupe d'Action Financière ou à l'égard duquel celui-ci recommande des contre-mesures ou l'exercice d'une vigilance renforcée;*
- *qui sont des personnes physiques dont l'identification a été opérée à distance sur la base d'une copie de document probant; ou*
- *dont les bénéficiaires effectifs sont des personnes dont l'identité n'a pas pu être vérifiée, et/ou pour lesquelles il n'a pas été possible d'identifier le lieu et la date de naissance, et/ou dont il n'a pas été possible de recueillir des informations pertinentes concernant l'adresse.*

Afin de tenir à jour la liste des pays et territoires considérés comme non coopératifs par le GAFI, ou à l'encontre desquels le GAFI recommande des contre-mesures ou l'exercice d'une vigilance renforcée, il appartient aux organismes de consulter régulièrement le site internet de cette organisation (*http://www.fatf-gafi.org*), en particulier après chacune de ses Réunions Plénières qui se tiennent régulièrement dans le courant des mois d'octobre, février et juin de chaque année.

5.2.3. Critères de risque spécifiques

Afin que l'échelle des risques sur laquelle s'appuie la politique d'acceptation des clients de chaque organisme soit aussi adéquate que possible pour atteindre les objectifs poursuivis, il appartient à chacun d'entre eux de définir pour ce qui le concerne, en fonction des caractéristiques des produits et services qu'il offre et de la clientèle à laquelle il s'adresse, des critères conduisant à la mise en œuvre de procédures différenciées d'acceptation pour tenir compte du niveau de risque.

Ainsi, par exemple, peuvent notamment constituer des critères appropriés pour définir des niveaux particuliers de risque des critères tels que:

- l'éloignement géographique entre le lieu de résidence du client et le point de contact avec l'organisme qu'il a choisi,
- le fait qu'il soit non résident,
- le fait qu'il exerce des activités dans un secteur économique sensible au risque de blanchiment de capitaux ou au financement du terrorisme,
- le fait que le client est une société dont une part importante du capital est représentée par des actions au porteur susceptibles de changer aisément de propriétaire à l'insu de l'organisme,
- le fait qu'il s'agisse d'un trust, d'une association de fait ou d'une autre structure juridique dont une bonne connaissance requiert une analyse plus approfondie,
- le fait qu'il s'agisse d'un client présentant des caractéristiques inhabituelles pour l'organisme concerné,
- le fait qu'il sollicite l'organisme pour des produits ou services considérés comme exposés au risque d'être utilisés pour des tentatives de blanchiment de capitaux ou de financement du terrorisme,
- le fait que la relation d'affaires envisagée impliquerait d'importants mouvements en espèces dont l'origine ou la destination sont difficilement vérifiables,
- l'importance des valeurs patrimoniales remises,
- etc.

Pour définir leurs critères de risques particulier, les organismes pourront utilement s'inspirer des publications du GAFI en la matière et consultables sur son site internet [41] «*www.fatf-gafi.org*», en particulier du document intitulé *«Directives à l'attention des institutions financières pour la détection des activités de financement du terrorisme»* publié le 24 avril 2002, les "*Guidance on the risk-based approach to combating money laundering and terrorist financing*" publiées en juin 2007 et le document intitulé "*Risk-Based Approach - Guidance for the Life Insurance Sector"* publié en octobre 2009.

Complémentairement aux risques particuliers liés aux pays et territoires désignés par le GAFI comme non coopératifs ou vis-à-vis desquels le GAFI recommande une vigilance accrue ou la mise en œuvre de "contre-mesures" (cf. art. 27 du règlement - section 5.2.2.4. supra), la CBFA recommande de tenir compte également des avertissements relatifs aux risques particuliers liés à certains pays ou territoires qui n'appliquent pas ou insuffisamment les Recommandation du GAFI et qui font l'objet d'avertissements publiés par le GAFI lui-même ou par les "*organisations régionales de type GAFI*" ("FSRB") qui bénéficient du statut d'organisation associées au GAFI, et en particulier par Moneyval, la FSRB créée par le Conseil de l'Europe [42].

La politique d'acceptation des clients des organismes devrait aussi tenir compte, grâce à des critères de risques appropriés, de la vulnérabilité des organismes à but non lucratif à une utilisation abusive à des fins de financement du terrorisme.

De plus, les organismes sont encouragés à inclure dans la liste des critères de risques fondant leur politique d'acceptation des clients des critères aptes à appréhender d'autres aspects du risque de réputation que celui lié au blanchiment de capitaux et au financement du terrorisme.

Il importe par ailleurs que, tant dans le choix de leurs critères spécifiques de risque que dans l'agencement de ces critères pour former l'échelle des risques sur laquelle ils fondent leur politique d'acceptation des clients, les organismes veillent à une bonne application du principe de proportionnalité. A ce titre, il convient qu'ils évitent avec soin de recourir à des critères ou à des agencements de critères qui ne puissent pas être justifiés, ou qui puissent apparaître excessifs au regard des risques que leur politique d'acceptation des clients est censée leur permettre de gérer. Leur attention est en outre attirée sur leur obligation de respecter, dans ce contexte particulier, les législations "anti-discrimination" en vigueur. La définition d'une échelle des risques qui ne répondrait pas à ces conditions de proportionnalité et de légalité au regard des législations "anti-discrimination" ne permettrait en effet pas d'appréhender de manière efficace les risques encourus, et pourrait de plus engager la responsabilité civile, voire pénale, de l'organisme financier et/ou de ses dirigeants.

Les informations à recueillir en vertu de l'article 12 du règlement doivent permettre, tant de sélectionner ceux des clients qui présentent des niveaux particuliers de risque, que de documenter de manière adéquate l'examen et la décision de leur acceptation par l'organisme.

6. Devoirs de vigilance

6.1. Règle générale - Vigilance constante

6.1.1. Prévention du blanchiment de capitaux et du financement du terrorisme

Article 14, §§ 1er et 2, de la loi

§ 1er. Les organismes et les personnes visés aux articles 2, § 1er, 3 et 4 doivent exercer une vigilance constante à l'égard de la relation d'affaires et procéder à un examen attentif des opérations effectuées et, lorsque cela est nécessaire, de l'origine des fonds, et ce, afin de s'assurer que celles-ci sont cohérentes avec la connaissance qu'ils ont de leur client, de ses activités commerciales, de son profil de risque.

Les organismes et les personnes visés aux articles 2, § 1er, 3 et 4 examinent avec une attention particulière, toute opération ou tout fait qu'ils considèrent particulièrement susceptible d'être lié au blanchiment de capitaux ou au financement du terrorisme et ce, en raison de sa nature ou de son caractère inhabituel par rapport aux activités du client ou en raison des circonstances qui l'entourent ou de par la qualité des personnes impliquées.

§ 2. Les organismes et les personnes visés aux articles 2, § 1er, 3 et 4 établissent un rapport écrit de l'examen réalisé en application du § 1er. Ce rapport est transmis aux personnes

41 *http://www.fatf-gafi.org*.
42 *http://www.coe.int/t/dghl/monitoring/moneyval/*.

visées à l'article 18 et ce, aux fins qu'il y soit réservé, si nécessaire, les suites requises, conformément aux articles 23 à 28.

La prévention effective du blanchiment des capitaux et du financement du terrorisme suppose que toute opération "atypique" ou tout fait intriguant soit détecté et soumis à un examen approfondi visant à déterminer s'ils suscitent des soupçons en raison desquels l'organisme financier est légalement tenu de procéder à la déclaration de ces opérations ou de ces faits suspects à la CTIF.

Cette détection des opérations atypiques et des faits intrigants repose essentiellement sur la vigilance que les organismes financiers sont tenus d'exercer à l'égard des opérations de leurs clients, cette vigilance supposant la mise en œuvre des moyens appropriés. Le degré de vigilance à exercer doit en outre être proportionné au niveau de risque associé au client ou à la relation d'affaires. L'article 14 de la loi définit les modalités essentielles et la finalité de cette obligation de vigilance.

Afin que cette vigilance constante puisse effectivement atteindre ses objectifs, il est nécessaire qu'elle repose sur une organisation systématique et adéquate, et qu'elle soit exercée de manière différenciée en fonction du profil de risque du client et de la relation d'affaires.

Ce système de surveillance doit également permettre à chaque organisme de se conformer à ses obligations en matière d'embargo financier et de gel des avoirs de certaines personnes, déjà évoquées à la section 5.1 ci-dessus.

6.1.2. Prévention de la prolifération des armes de destruction massive

6.1.2.1. Contexte général

Face aux dangers pour la paix mondiale que représente la prolifération des armes nucléaires, chimiques et biologiques (dites « *armes de destruction massive* »), le Conseil de Sécurité des Nations Unies a adopté depuis 2006 diverses Résolutions visant à la contrecarrer. Ces résolutions, qui visent en particulier la Corée du Nord et l'Iran, ne comprennent pas seulement des mesures imposant des interdictions ou restrictions applicables à la fourniture de composants des armes de destruction massive à ces pays ou d'une assistance technique pouvant servir au développement des programmes de fabrication de ces armes. Elles comprennent aussi des mesures de gel des avoirs de personnes et entités reconnues par le Conseil de Sécurité comme prenant part à la prolifération des armes de destruction massive, et demandent à tous les pays de prendre les mesures nécessaires en vue d'empêcher la fourniture d'assistance financière, d'investissements ou de financements qui puissent concourir aux programmes de prolifération des armes de destruction massive de ces pays.

En ce qui concerne les mesures à l'encontre de la Corée du Nord, l'on citera notamment la Résolution 1695 (2006) du 15 juillet 2006 [43] (notamment son §4), et la Résolution 1718 (2006) du 14 octobre 2006 (notamment son § 8, d).

Vis-à-vis de l'Iran, l'on se réfèrera aux Résolutions n° 1696 (2006) du 31 juillet 2006, n° 1737 (2006) du 23 décembre 2006 (en particulier, ses §§ 6 et 12 à 15), n° 1803 (2008) du 3 mars 2008 (en particulier son § 7) et n° 1929 (2010) du 9 juin 2010 (en particulier ses §§ 8 et 21 à 24).

Dans le prolongement de ces Résolutions, le GAFI a élaboré et publié en juin 2007 des lignes de conduite (« guidance ») en vue de l'application des dispositions financières des Résolutions du Conseil de Sécurité des Nations Unies. Le GAFI les a complétées par la publication de lignes de conduite spécifiquement relatives à la mise en œuvre des interdictions financières fondées sur les activités qui sont énoncées par la Résolution 1737 (2006) précitée relative à l'Iran (octobre 2007), et à la mise en œuvre de la Résolution 1803 (2008) relative à l'Iran (octobre 2008).

6.1.2.2. Mesures restrictives à l'encontre de la République Populaire Démocratique de Corée et de l'Iran

En Europe, le Conseil Européen a adopté en la matière les règlements (CE) 329/2007 du 27 mars 2007 [44] (modifié à plusieurs reprises depuis, notamment par le règlement (UE) 1283/2009 du Conseil du 22 décembre 2009 [45]) et le règlement (UE) n° 961/2010 du 25 octobre 2010 [46], concernant l'adoption de mesures restrictives à l'encontre, respectivement, de la République populaire démocratique de Corée

43 Les résolutions du Conseil de Sécurité peuvent être consultées sur le site internet de l'ONU, à l'adresse : *http://www.un.org/documents/scres.htm*

44 JO L 88 du 29 mars 2007, p. 1

45 JO L 346 du 23 décembre 2009, p. 1

46 JO n° L 281 du 27 octobre 2010, p. 1.

et de l'Iran. Ces règlements européens sont directement applicables dans les droits nationaux des Etats Membres.

La CBFA attire particulièrement l'attention sur le fait qu'outre les obligations de gel des avoirs de personnes liées aux activités coréennes ou iraniennes en relation avec la prolifération prévues dans les conditions et selon les modalités définies par ces règlements (cf. supra, section 5.1 de la présente circulaire), ces mêmes règlements européens énoncent également :

- l'interdiction ou la restriction de l'autorisation de fournir, directement ou indirectement, des investissements ou des financements en rapport avec des biens ou technologies énumérés en annexe à ces règlements (cf. article 3 du Règlement (CE) 329/2007 du 27 mars 2007 modifié, et article 5 du Règlement (UE) n° 961/2010 du 25 octobre 2010);
- et des obligations de vigilance en vue de prévenir le financement de la prolifération (cf. article 11 bis du Règlement (CE) 329/2007 du 27 mars 2007 modifié, et article 23 du Règlement (UE) n° 961/2010 du 25 octobre 2010).

De plus, concernant l'Iran, l'attention est attirée sur le fait que le Règlement (UE) n° 961/2010 a significativement élargi les restrictions applicables aux relations et opérations des institutions financières européennes avec des contreparties iraniennes. Ainsi, les restrictions au financement de certaines entreprises qui sont définies au chapitre III de ce règlement s'étendent actuellement aux personnes, entités et organismes iraniens qui se livrent, non seulement, à la fabrication de biens ou de technologies relatifs à des équipements militaires ou susceptibles d'être utilisés à des fins de répression interne, mais aussi à l'exploration ou à la production de pétrole brut ou de gaz naturel, au raffinage de combustibles ou à la liquéfaction du gaz naturel. En outre, il y a lieu d'être particulièrement attentif au respect des restrictions et interdictions suivantes instaurées par ce règlement :

- l'exécution et la réception des transferts de fonds à destination ou en provenance d'une personne, d'une entité ou d'un organisme iraniens requièrent, lorsque leurs montants excèdent les seuils définis à l'article 21 du Règlement (UE) n° 961/2010, que l'établissement financier belge intervenant dans l'opération obtienne l'autorisation préalable du SPF des Finances, Administration de la Trésorerie [47];
- lesdits transferts.de fonds doivent mentionner, non seulement les données relatives au donneur d'ordre, mais également celles relatives au bénéficiaire et, en l'absence de tout ou partie des informations requises, l'établissement financier belge est tenu de refuser l'opération [48];
- Il est interdit d'ouvrir de nouveaux comptes bancaires auprès d'établissements financiers ou de crédit domiciliés en Iran, de nouer de nouvelles relations de correspondance bancaire avec ces établissements, d'établir un nouveau bureau de représentation, une nouvelle succursale ou une nouvelle filiale en Iran; Sont réciproquement interdits l'établissement dans l'Union européenne d'un bureau de représentation, d'une succursale ou d'une filiale par un établissement financier ou de crédit domicilié en Iran, de même que l'acquisition ou l'accroissement d'une participation par un établissement iranien dans un établissement financier ou de crédit européen [49];
- Il est interdit de vendre ou d'acheter, directement ou par personne interposée, à l'Etat iranien ou à des établissements financiers ou de crédit domiciliés en Iran des obligations de l'Etat ou garanties par l'Etat émises après le 26 juillet 2010, d'offrir à ces mêmes entités et personnes iraniennes des services de courtage relatifs à ces mêmes obligations, ou de fournir de l'assistance en vue de l'émission d'obligations de l'Etat ou garanties par lui [50];
- Il est interdit de fournir des produits d'assurance ou de réassurance à l'Iran, son gouvernement, ses organismes, entreprises et agences publics, aux personnes morales, entités ou organismes iraniens et aux personnes agissant pour le compte ou selon les instructions des personnes ou entités précitées qui sont visées par cette interdiction [51];

Afin de remplir les obligations énoncées par ces règlements européens, il appartient dès lors aux organismes financiers de mettre en œuvre les mesures appropriées en vue du strict respect des restrictions précitées à l'encontre de l'Iran et de la Corée du Nord, et, notamment, de mettre en œuvre leurs systèmes de vigilance de première et de deuxième ligne décrits à la section 6.1.4 de la présente circulaire, non seulement dans le but de prévenir le blanchiment des capitaux et le financement du

47 30 Avenue des Arts, 1040 Bruxelles – *quesfinvragen.tf@minfin.fed.be*
48 Article 23.1, b) du Règlement(UE) n° 961/2010 du 25 octobre 2010.
49 Article 24 du Règlement(UE) n° 961/2010 du 25 octobre 2010.
50 Article 25 du Règlement(UE) n° 961/2010 du 25 octobre 2010.
51 Article 26 du Règlement(UE) n° 961/2010 du 25 octobre 2010.

terrorisme, mais également le financement de la prolifération des armes de destruction massive imputable à l'Iran conformément aux dispositions rappelées ci-dessus.

6.1.3. Mise à jour des données d'identification et du profil du client

Article 7, § 3, de la loi

Les organismes et les personnes visés aux articles 2, § 1er et 3 doivent mettre à jour, en fonction du risque, les données d'identification de leurs clients habituels et des mandataires de ceux-ci lorsqu'il apparaît que les informations qu'ils détiennent les concernant ne sont plus actuelles. Dans ce cas, ils procèdent à une nouvelle vérification de l'identité de ces clients ou de leurs mandataires conformément aux §§ 1er et 2.

Article 8, § 2, de la loi

« Les organismes et les personnes visés aux articles 2, § 1er et 3 doivent mettre à jour, en fonction du risque, les données d'identification des bénéficiaires effectifs d'un client avec lequel ils entretiennent une relation d'affaires lorsqu'il apparaît que les informations qu'ils détiennent les concernant ne sont plus actuelles.

Article 30 du règlement

Le devoir de vigilance constante des organismes prévu par l'article 14, § 1er, de la loi inclut celui de vérifier et, le cas échéant, de mettre à jour dans un délai déterminé en fonction du risque les informations visées à l'article 12 du présent règlement qu'ils détiennent concernant les clients avec lesquels ils entretiennent une relation d'affaires lorsque des indications leur sont fournies que ces données ne sont plus actuelles.

Les dispositions légales et règlementaires rappelées ci-dessus imposent aux organismes de vérifier la pertinence des informations d'identification et des autres informations qu'ils détiennent et qui déterminent le "profil" des clients avec lesquels ils entretiennent des relations d'affaires, dès lors qu'ils disposent d'indications que ces données ou ces informations ne sont plus à jour. Il peut en être ainsi dans le cas d'indications concernant un changement d'adresse ou le décès d'un client personne physique. Une mise à jour des informations recueillies par application de l'article 12 du règlement peut aussi s'avérer nécessaire lorsque la nature des opérations du client n'apparait plus cohérente avec les activités professionnelles qu'il a antérieurement déclaré exercer. Les clients qui sont des personnes morales peuvent requérir de ce point de vue une attention particulière pour tenir compte du nombre de changements potentiels plus élevé des données d'identification les concernant (modification de la dénomination sociale ou du siège social, changement des actionnaires significatifs ou de contrôle ou des administrateurs, fusion, liquidation, etc.).

Le délai de mise à jour des informations peut être fixé en fonction du risque. Il appartient à chaque organisme de définir des critères adéquats à cet effet, en cohérence avec ceux qui sont mis en œuvre dans le cadre de la politique d'acceptation des clients (cf. section 5.2., supra). Les nouvelles données d'identification doivent également être vérifiées au moyen d'un document probant approprié, comme dans l'hypothèse d'une identification initiale.

Il est également à souligner que l'accès indirect au Registre national prévu par l'article 16, § 3, de la loi du 11 janvier 1993 est autorisé dans le but de procéder, par application de ses articles 7, § 3, et 8, § 2, à la mise à jour des données d'identification des personnes qu'elle vise; à savoir les clients, leurs mandataires et leurs bénéficiaires effectifs sans que ces personnes ne soient physiquement présentes pour y procéder. S'agissant de procéder à l'actualisation des données d'identification des clients et des mandataires, la consultation du Registre national peut être opérée sur la base de la copie du document probant obtenue lors de l'identification initiale. S'agissant de l'actualisation des données d'identification des bénéficiaires effectifs, il est également rappelé que les procédures internes des organismes financiers peuvent autoriser la consultation du Registre national sans disposer d'une copie de la carte d'identité de ces personnes (cf. section 4.4.4.1, supra).

La Commission recommande en outre aux organismes d'exercer une vigilance appropriée en fonction du risque quant à la validité dans le temps des informations dont ils disposent à propos des clients avec lesquels ils sont en relation d'affaires. Lorsque cela apparaît nécessaire en vue d'une prévention efficace du blanchiment de capitaux et du financement du terrorisme, il est notamment souhaitable de vérifier la pertinence des informations détenues concernant les clients.

6.1.4. Surveillance de 1ère et de 2ème ligne

Les articles 31 et 32 du règlement imposent que la vigilance à l'égard des relations d'affaires et des opérations, repose sur une surveillance à deux niveaux des opérations des clients.

6.1.4.1. Surveillance de 1ère ligne

Article 31 du règlement

Les organismes précisent par écrit à l'intention de leur préposés chargés de la surveillance de première ligne les critères appropriés leur permettant de déterminer les opérations atypiques, auxquelles il est requis qu'ils attachent une attention particulière, et qui doivent faire l'objet d'un rapport écrit visé à l'article 14, § 2, de la loi.

L'examen des opérations et faits visés à l'article 14, § 1er, alinéa 2, de la loi, inclut, notamment, celui de leur justification économique et de leur légitimité apparentes.

Les organismes précisent également par écrit à l'intention de leurs préposés chargés de la surveillance de première ligne la procédure requise en vue de la transmission des rapports écrits au responsable de la prévention du blanchiment de capitaux et du financement du terrorisme visé à l'article 18 de la loi, incluant les délais requis de transmission.

La « surveillance de première ligne » est celle qui est exercée par les préposés de l'organisme qui sont en contact direct avec les clients. Elle consiste à recourir à leur expérience, à leur esprit critique et à leur capacité d'appréciation des situations auxquelles ils sont confrontés, en contact direct avec les clients pour, détecter les opérations « atypiques » au sens de l'article 1er, 8° du règlement. Sont visées les opérations qui apparaissent particulièrement susceptibles d'être liées au blanchiment de capitaux ou au financement du terrorisme, notamment parce qu'elles n'apparaissent pas cohérentes avec ce que l'organisme connaît de son client, de ses activités professionnelles, de son profil de risque et, lorsque cela s'avère nécessaire, de l'origine des fonds.

C'est en outre essentiellement en s'appuyant sur ses mécanismes de surveillance de 1ère ligne que l'organisme peut être à même de détecter des faits susceptibles de constituer un indice de blanchiment de capitaux ou de financement du terrorisme et de remplir son obligation légale d'informer la CTIF de ces faits.

Afin que les préposés concernés puissent adéquatement assumer leurs responsabilités en la matière, il s'impose, d'une part, que les efforts nécessaires de formation et de sensibilisation soient fournis (cf. chapitre 13 du règlement et chapitre 11 de la présente circulaire). Mais il s'impose également que des procédures écrites adéquates soient établies pour préciser à leur intention une liste non limitative de critères à prendre en considération dans la détection des opérations atypiques, ainsi que la façon d'établir les rapports écrits requis et de les transmettre au responsable de la prévention du blanchiment de capitaux et du financement du terrorisme.

Il est recommandé que les critères évoqués soient cohérents avec ceux qui sont appliquée dans le cadre de la politique d'acceptation des clients (cf. supra, chapitre 5) pour classifier les clients en fonction du risque. Toutefois, il s'indique que la surveillance de première ligne s'appuie également sur des critères relatifs aux opérations elles-mêmes. Une attention particulière doit notamment être attachée à cet égard à la justification économique et à la légitimité apparente des opérations. De ce point de vue, une vigilance accrue peut s'imposer à l'égard de dépôts de sommes importantes en espèces qui seraient effectués par des « marchands de biens de grande valeur » assujettis aux dispositions de l'article 21 de la loi, qui interdit de recevoir en espèces le paiement du prix de vente d'un ou plusieurs biens pour un montant de 15.000 € ou plus.

En outre, des critères appropriés doivent conduire les préposés à être attentifs aux circonstances en raison desquelles une opération peut être particulièrement susceptible d'être liée au blanchiment de capitaux ou au financement du terrorisme, ainsi qu'aux faits susceptibles d'en constituer des indices (comme, par exemple, une absence suspecte d'intérêt du client pour certaines conditions pourtant importantes des services proposés, telle que leur tarification).

Pour définir ces critères, les organismes pourront utilement s'inspirer du document intitulé *«Directives à l'attention des institutions financières pour la détection des activités de financement du terrorisme»* publié le 24 avril 2002 par le GAFI et consultable sur son site internet «*www.fatf-gafi.org*».

6.1.4.2. Surveillance de 2ème ligne

Article 32, alinéas 1er et 2, du règlement

Les organismes complètent la surveillance de première ligne par une surveillance de seconde ligne exercée par un système de surveillance permettant de détecter les opérations atypiques, qui doivent faire l'objet d'un rapport écrit visé à l'article 14, § 2, de la loi.

Le système de surveillance doit :

- *couvrir l'intégralité des comptes des clients et de leurs opérations;*

- *être basé sur des critères précis et pertinents, fixés par chaque organisme en tenant compte, notamment, des caractéristiques des services et produits qu'il offre et de celles de la clientèle à laquelle il s'adresse, et suffisamment discriminants pour permettre de détecter effectivement les opérations atypiques;*
- *permettre une détection rapide de ces opérations;*
- *produire des rapports écrits décrivant les opérations atypiques détectées et ceux des critères visés au deuxième tiret du présent alinéa sur la base desquels elles sont considérées atypiques, ces rapports étant transmis au responsable de la prévention du blanchiment de capitaux et du financement du terrorisme visé à l'article 18 de la loi;*
- *être automatisé, sauf si l'organisme peut démontrer que la nature et le volume des opérations à surveiller ne requièrent pas l'automatisation du système de surveillance;*
- *faire l'objet d'une procédure de validation initiale et d'un réexamen périodique de sa pertinence en vue de l'adapter, au besoin, en fonction de l'évolution des activités, de la clientèle ou de l'environnement.*

La surveillance de première ligne doit être complétée par une «surveillance de seconde ligne» exercée par un «système de surveillance» répondant aux conditions définies à l'article 32, alinéa 2, du règlement. L'objectif de cette surveillance de seconde ligne consiste à détecter de manière systématique les opérations qui, bien qu'atypiques, ne pouvaient pas être détectées en tant que telles par la surveillance de première ligne ou qui ont échappé à sa vigilance.

Le système de surveillance doit permettre de même aux organismes de s'assurer qu'ils satisfont à leurs obligations de déclaration étendues, conformément à l'article 27 de la loi (cf. infra, section 7.1.1.). Sont visées les opérations dans lesquelles interviennent des personnes domiciliées dans des pays ou territoires non coopératifs ("PTNC") à l'encontre desquels le GAFI recommande à ses membres d'adopter des contre-mesures telles que prévues par la Recommandation 21.

Compte tenu des rôles respectifs et complémentaires des entreprises d'assurance-vie et des intermédiaires non exclusifs en assurance-vie, la Commission recommande à ces organismes de répartir entre eux, sans préjudice de leur responsabilité respective au regard de la loi, non seulement les tâches d'identification des clients et des bénéficiaires effectifs, le cas échéant, en se fondant sur l'article 10 de la loi (cf. section 4.7 supra), mais aussi celles relatives de détection des opérations atypiques. A cet égard, l'attention est attirée sur les dispositions de l'article 30, § 3, 2°, de la loi, commenté de façon détaillée à la section 7.1.3.2.2 ci-après, qui prévoit une exception à l'interdiction prévue au § 1er du même article d'informer des tiers du fait qu'une déclaration d'opération suspecte a été transmise à la CTIF, lorsque information est communiquée à un autre organisme financier qui intervient en relation avec le même client ou dans le cadre de la même transaction.

Les mêmes recommandations s'appliquent également aux relations entre les établissements de crédit ou les entreprises d'investissement, d'une part, et les courtiers en produits bancaires et d'investissement, d'autre part.

En règle générale, les exigences d'efficacité et de rapidité de réaction du système de surveillance de seconde ligne imposeront qu'il soit automatisé. Toutefois, un système non automatisé peut être admis lorsque l'organisme peut démontrer que la nature et le volume des opérations permettent d'exercer cette surveillance sans recours à l'automatisation.

Cette démonstration suppose néanmoins également que les moyens humains nécessaires à l'efficacité et à la rapidité de réaction du système non automatisé soient mis en œuvre.

Compte tenu de ce que la prévention du blanchiment de capitaux et du financement du terrorisme constitue un élément important de la gestion adéquate du risque de réputation, et complémentairement aux commentaires formulés à la section 10.3 de la présente circulaire, la Commission recommande aux organismes qui ont établi des filiales ou des succursales à l'étranger qu'ils s'assurent, au besoin par des contrôles sur place effectués par leur département d'audit interne, que ces filiales et succursales disposent également d'un système de surveillance approprié des opérations permettant effectivement de détecter les opérations suspectes et de se conformer à la législation locale.

6.1.5. Exercice de la vigilance constante en fonction du risque

6.1.5.1. Principe général - cohérence avec la politique d'acceptation des clients

Article 12, § 1er, de la loi

Sans préjudice des obligations prévues aux articles 7 à 9, les organismes et les personnes visés aux articles 2, § 1er, 3 et 4 appliquent, en fonction de leur appréciation du risque, des

mesures de vigilance renforcées à l'égard de la clientèle, dans les situations qui, de par leur nature, peuvent présenter un risque élevé de blanchiment de capitaux et de financement du terrorisme et, à tout le moins, dans les cas visés ci-dessous.

Article 32, alinéa 3 du règlement

Les critères visés à l'alinéa précédent, 2ème tiret, tiennent compte notamment du risque particulier au regard du blanchiment de capitaux ou du financement du terrorisme qui est lié aux opérations réalisées par les clients dont l'acceptation a été soumise à des règles renforcées en vertu de la politique d'acceptation des clients visée au chapitre 8.

Article 28, § 2, du règlement

Les organismes qui entretiennent des relations d'affaires avec des établissements de crédit ou des institutions financières de droit étranger visés au paragraphe précédent procèdent :

- *à un examen périodique, en fonction du risque, et, le cas échéant, à la mise à jour des informations sur la base desquelles la décision a été prise de nouer lesdites relations ;*
- *à un nouvel examen desdites relations lorsque des informations sont obtenues qui sont de nature à ébranler la confiance dans les dispositifs légaux et réglementaires de lutte contre le blanchiment de capitaux et le financement du terrorisme du pays d'établissement de l'établissement financier client, ou dans l'efficacité des contrôles mis en place par ce dernier sur le plan de la lutte contre le blanchiment de capitaux et le financement du terrorisme ;*
- *à des vérifications et des tests périodiques, en fonction du risque, pour s'assurer du respect en tout temps par l'établissement financier client des engagements auxquels il a souscrit, notamment, en ce qui concerne la communication sans retard sur demande des données pertinentes d'identification de ses clients ayant un accès directs aux comptes de passage qui lui ont été ouverts.*

Les devoirs de vigilance constante à l'égard de la relation d'affaires ou des opérations constituent le prolongement logique de la politique d'acceptation des clients. Dès lors, les critères sur lesquels se fonde le système de vigilance, tant de première que de seconde ligne, doivent être définis de manière telle que le niveau de la vigilance exercée soit proportionné au niveau de risque et varie en fonction de lui.

Les critères de risque qui déterminent l'exercice d'une vigilance accrue doivent en outre être cohérents avec les critères de risque pris en considération dans le cadre de la politique d'acceptation des clients. Doivent ainsi faire l'objet d'une vigilance accrue les relations d'affaires visées à l'article 12, §§ 2 à 4, de la loi, ou à l'article 27 du règlement, ainsi que celles réputées risquées par application des critères spécifiques de risque sur lesquels l'organisme fonde sa politique d'acceptation des clients.

6.1.5.2. Critères complémentaires de risque

Article 32, alinéas 4 et 5, du règlement

Ces critères tiennent également compte du risque particulier de blanchiment de capitaux et de financement du terrorisme qui est associé aux opérations qui portent sur des montants inhabituels en termes absolus ou au regard des habitudes du client considéré dans ses relations avec l'organisme.

Constitue une opération atypique au sens du présent article, un virement de fonds reçu au profit d'un client sans être accompagné des renseignements relatifs au donneur d'ordre qui sont requis par le 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.

Article 33 du règlement

Lorsqu'un organisme communique à la Cellule de traitement des informations financières une information relative à une opération suspecte conformément aux articles 23, 24, 27 ou 28 de la loi, ou relative à un fait susceptible d'être l'indice d'un blanchiment de capitaux ou d'un financement du terrorisme conformément à l'article 25 de la loi, l'organisme soumet à une vigilance accrue ses relations d'affaires avec les personnes concernées par les informations ainsi communiquées.

Dans ce cas, les organismes soumettent notamment à un examen particulier, conformément à l'article 14 de la loi, toute opération souhaitée par le client consistant dans un *retrait, un transfert, un rachat, ou toute autre opération qui serait susceptible de contribuer à la dissimulation de l'emplacement de fonds soupçonnés d'être d'origine illicite. Le cas échéant, les organismes procèdent dans ces circonstances à une nouvelle communication*

d'information à la Cellule de traitement des informations financière conformément aux articles 23, 24, 25, 27 ou 28 de la loi.

Outre le recours aux critères de risque qui fondent la politique d'acceptation des clients, il apparaît indispensable que des critères spécifiques, prenant également en considération l'évolution constatée de la relation d'affaires et des opérations effectuées par le client, complètent l'arsenal de critères sur la base desquels le niveau de vigilance à exercer est déterminé.

Ainsi en est-il des situations visées aux articles 32, alinéas 4 et 5, et 33 du règlement. L'exercice d'une vigilance accrue s'impose notamment à l'égard des opérations portant sur des montants inhabituellement élevés pour le client, ou à l'égard des virements de fonds reçus au profit du client et qui ne sont pas accompagnés des informations requises sur le donneur d'ordre (cf. infra, section 8.1).

Une vigilance accrue doit également être exercée à l'égard des clients qui ont effectué des opérations que l'organisme a estimées suspectes et qu'il a transmises à ce titre à la CTIF. Outre que ce renforcement de la vigilance doit permettre à l'organisme financier d'apprécier si l'opération suspecte peut ou non être considérée comme isolée, elle doit également lui permettre de relever et de soumettre à une analyse particulière toute opération souhaitée par le client par laquelle il pourrait s'efforcer de soustraire ses fonds aux éventuelles mesures de saisie susceptibles d'être décidées par les autorités judiciaires. Ainsi en serait-il, par exemple, s'il souhaitait clôturer son compte ou opérer un retrait de montants importants en espèces. Dans ces mêmes circonstances, si l'organisme envisage de mettre fin de sa propre initiative à la relation avec le client, notamment en raison de la rupture de la confiance à l'égard de celui-ci, il est recommandé à l'organisme financier d'en informer au préalable la CTIF.

Compte tenu de la finalité de la vigilance accrue, la CBFA recommande de la maintenir en vigueur à l'égard des clients ci-dessus visés aussi longtemps que cela apparaît nécessaire en fonction des circonstances, pour conclure au caractère isolé de l'opération ayant éveillé les soupçons de l'organisme financier ou pour identifier sans retard de nouvelles opérations suspectes éventuelles effectuées par le client. La décision de lever cette mesure de vigilance accrue devrait être prise sous la responsabilité du responsable de la prévention du blanchiment de capitaux et du financement du terrorisme.

Il est également recommandé aux organismes de soumettre leurs relations d'affaires avec les clients à une vigilance accrue chaque fois que cela apparaît nécessaire en fonction des circonstances, afin de remplir pleinement leur obligation générale de prévention du blanchiment de capitaux et du financement du terrorisme définie à l'article 6 de la loi. Une telle nécessité peut par exemple se faire jour à l'égard de clients dont une ou, a fortiori, plusieurs opérations ont fait l'objet de rapports écrits adressés au responsable de la prévention du blanchiment en vertu de l'article 14, § 2, de la loi, sans que ces rapports écrits n'aient suscité de soupçons suffisants pour justifier la transmission d'informations à la CTIF en vertu des articles 23 à 25, 27 ou 28 de la loi, mais sans pour autant que la légitimité des opérations concernées ait pu être établie de manière indubitable.

7. Déclaration des opérations suspectes

7.1. Soupçons de blanchiment de capitaux ou de financement du terrorisme

7.1.1. Déclarations de soupçons

Article 23, § 1er, alinéa 1er, de la loi

Lorsque les organismes ou les personnes visés à l'article 2, § 1er savent ou soupçonnent qu'une opération à exécuter est liée au blanchiment de capitaux ou au financement du terrorisme, ils en informent par écrit la Cellule de traitement des informations financières, avant d'exécuter l'opération, en indiquant, le cas échéant, le délai dans lequel celle-ci doit être exécutée.

Article 24 de la loi

Dans l'hypothèse où les organismes ou les personnes visés à l'article 2, § 1er, qui savent ou soupçonnent qu'une opération à exécuter est liée au blanchiment de capitaux ou au financement du terrorisme, ne peuvent en informer la Cellule de traitement des informations financières avant d'exécuter l'opération, soit parce que le report de l'exécution de l'opération n'est pas possible en raison de la nature de celle-ci, soit parce qu'il serait susceptible d'empêcher la poursuite des bénéficiaires du blanchiment présumé de capitaux et du financement présumé du terrorisme, les organismes ou les personnes procèdent à l'information par écrit de la Cellule immédiatement après avoir exécuté l'opération. Dans ce

cas, la raison pour laquelle il n'a pu être procédé à l'information préalablement à l'exécution de l'opération doit être indiquée.

Article 25 de la loi

Hors les cas visés aux articles 23 et 24, lorsque les organismes ou les personnes visés à l'article 2, § 1er ont connaissance d'un fait qui pourrait être l'indice d'un blanchiment de capitaux ou d'un financement du terrorisme, ils en informent immédiatement par écrit la Cellule de traitement des informations financières.

Article 27 de la loi

Sur avis de la Cellule de traitement des informations financières, le Roi peut étendre l'obligation d'information visée aux articles 23 à 26 aux opérations et aux faits concernant des personnes physiques ou morales domiciliées, enregistrées ou établies dans un Etat ou un territoire dont la législation est reconnue insuffisante ou dont les pratiques sont considérées comme faisant obstacle à la lutte contre le blanchiment des capitaux par une instance internationale de concertation et de coordination compétente. Le Roi peut déterminer le type de faits et d'opérations visés ainsi que le montant minimal.

Article 28, alinéa 1er, de la loi

Lorsque les organismes et les personnes visés aux articles 2, § 1er, 3 et 4 soupçonnent qu'un fait ou une opération est susceptible d'être lié au blanchiment de capitaux provenant de la fraude fiscale grave et organisée qui met en œuvre des mécanismes complexes ou qui use de procédés à dimension internationale, ils en informent immédiatement par écrit la Cellule de Traitement des Informations Financières, y compris dès qu'ils détectent au moins un des indicateurs que le Roi déterminera, par arrêté royal délibéré en Conseil des Ministres.

Pour rappel, conformément à ces articles de la loi, les organismes sont tenus de transmettre une information à la Cellule de traitement des informations financières dans les cas ci-dessous.

Lorsqu'ils savent ou soupçonnent qu'une opération à exécuter est liée au blanchiment de capitaux ou au financement du terrorisme.

En principe, la transmission de l'information doit être préalable à l'exécution de l'opération (cf. article 23 de la loi). Dans ce cas, la déclaration doit indiquer le délai dans lequel l'opération sera exécutée, afin de permettre à la Cellule, si elle l'estime nécessaire en raison de la gravité ou de l'urgence de l'affaire, de faire opposition avant l'expiration de ce délai à l'exécution de l'opération (cf. infra).

Par dérogation à la règle générale, l'information peut être communiquée à la Cellule postérieurement à l'exécution de l'opération, soit si son report est impossible en raison de la nature même de l'opération, soit si ce report est susceptible d'empêcher la poursuite des bénéficiaires du blanchiment de capitaux ou du financement du terrorisme (cf. article 24 de la loi). Dans ces hypothèses, la Cellule doit être informée immédiatement après l'exécution de l'opération, en lui indiquant la raison pour laquelle l'information n'a pas été transmise préalablement à l'exécution de l'opération.

Lorsque les soupçons concernent la commission d'une fraude fiscale grave et organisée qui met en œuvre des mécanismes complexes ou qui use de procédés à dimension internationale, les organismes se réfèrent en outre à la liste des indicateurs établie par arrêté royal en vertu de l'article 28 de la loi. Cet arrêté royal peut notamment être consulté sur le site internet de la CTIF (*http://www.ctif-cfi.be*).

Lorsqu'ils ont connaissance, dans le cadre de leurs activités professionnelles, d'un fait qui pourrait être l'indice d'un blanchiment de capitaux ou d'un financement du terrorisme. (cf. article 25 de la loi)

Contrairement au premier cas, celui-ci ne vise pas l'exécution d'une opération en particulier, mais est plus général. Il peut par exemple s'agir d'un ensemble d'opérations qui, prises séparément, n'avaient pas éveillé de soupçons, mais qui apparaissent a posteriori susceptibles d'être liées au blanchiment de capitaux ou au financement du terrorisme.

Pourraient également devoir faire l'objet d'une telle communication des faits qui témoignent de l'intention d'un client de réaliser une opération à laquelle il renonce ensuite de son propre chef avant qu'elle ne soit exécutée, mais qui aurait été une opération suspecte si elle avait été réalisée.

Le cas échéant, il peut également y avoir lieu de se référer à la liste d'indices de fraude fiscale grave et organisée qui met en œuvre des mécanismes complexes ou qui use de procédés à dimension internationale établie par arrêté royal en vertu de l'article 28 de la loi.

Lorsque des personnes résidant dans des pays ou territoires qualifiés de non coopératifs sont impliquées dans les opérations.

Dans ces cas, le seul fait qu'une personne (physique ou morale) intervenant dans l'opération est domiciliée, enregistrée ou établie dans un pays désigné par arrêté royal comme non coopératif suffit pour qu'une déclaration à la CTIF soit obligatoire. Actuellement, aucun pays ou territoire n'est désigné par le Roi en application de l'article 27 de la loi.

7.1.2. Demandes d'informations émanant de la CTIF

Article 33, alinéa 1er, 1°, de la loi

Lorsque la Cellule de traitement des informations financières reçoit une information visée à l'article 22, § 2, la Cellule ou l'un de ses membres ou l'un des membres de son personnel désigné à cette fin par le magistrat qui la dirige ou son suppléant peuvent se faire communiquer, dans le délai qu'ils déterminent, tous les renseignements complémentaires qu'ils jugent utiles à l'accomplissement de la mission de la Cellule, de la part:

1° de tous les organismes et les personnes visés aux articles 2, § 1er, 3 et 4 ainsi que de la part du bâtonnier visé à l'article 26, § 3;

(...)

Indépendamment des obligations de communication des opérations et faits suspects à la CTIF, la Commission rappelle également les obligations des organismes face aux demandes d'informations que peut leur adresser la Cellule en vertu de l'article 32, § 1er, 1° de la loi, et la nécessité de pouvoir y donner suite dans les délais impartis.

Les informations ainsi demandées par la CTIF lui sont normalement fournies par le responsable de la prévention du blanchiment de capitaux. Les règles ci-dessous commentées concernant l'interdiction d'informer le client ou les tiers et l'exonération de responsabilité du fait d'informations communiquées de bonne foi sont d'application.

7.1.3. Modalités de déclaration des opérations ou faits suspects

7.1.3.1. Personnes autorisées à procéder à des déclarations d'opérations ou de faits suspects

Article 29 de la loi

La transmission d'informations visée aux articles 20, 23 à 28, est effectuée normalement par la personne désignée au sein des organismes et personnes visés aux articles 2, § 1er, 3 et 4, conformément à l'article 18 de la présente loi (...).

Tout employé et tout représentant des organismes ou des personnes visés aux articles 2, § 1er et 4 procèdent toutefois personnellement à la transmission d'informations à la Cellule chaque fois que la procédure visée à l'alinéa 1er ne peut être suivie.

Les déclarations d'opérations ou de faits suspects doivent normalement être effectuées par le responsable de la prévention du blanchiment de capitaux et du financement du terrorisme sur la base de son analyse des rapports internes qui lui sont adressés concernant des opérations "atypiques" ou des faits susceptibles de constituer des indice de blanchiment de capitaux ou de financement du terrorisme.

Toutefois, l'absolue nécessité de lutter contre l'utilisation du système financier aux fins du blanchiment de capitaux et le financement du terrorisme et l'urgence des réactions requises lorsqu'une telle opération est détectée justifient que tout employé ou tout représentant (notamment les agents délégués) est autorisé à procéder à cette déclaration lorsqu'il n'est pas possible en raison des circonstances de suivre la procédure normale.

Il convient de respecter, dans toute la mesure du possible, les modalités et procédures de communication recommandées par la Cellule. Il y a notamment lieu de se référer à cet égard à la Note d'Information diffusée le 12 janvier 2011 par la CTIF concernant la transmission d'informations à la Cellule de Traitement des Informations Financières [52].

Comme le soulignent les travaux préparatoires de la loi du 11 janvier 1993, les organismes ne sont pas dispensés de leur obligation légale de procéder aux déclarations requises auprès de la Cellule lorsqu'ils savent, directement ou indirectement, que les autorités judiciaires sont déjà informées ou saisies des opérations financières ou des faits concernés. En effet, les compétences de la CTIF de recevoir et

52 http://www.ctif-cfi.be/website/images/FR/t1000_inst_fin-immobilier-diamants-fr.pdf

d'analyser les déclarations d'opérations ou de faits suspects sont définies à article 22, § 2, de la loi *« sans préjudice des compétences des autorités judiciaires »*.

De plus, la déclaration d'une opération suspecte à la CTIF est une obligation individuelle de chaque organisme financier. Dès lors que la loi ne prévoit aucune dispense de procéder à une déclaration d'opération suspecte par un organisme financier qui sait que cette même opération a déjà fait l'objet d'une déclaration à la CTIF par un autre organisme financier, fût-il du même groupe, la décision de ne pas procéder à une telle déclaration ne peut se fonder sur le fait que la CTIF a déjà été informée de l'opération par cet autre organisme financier.

7.1.3.2. Interdiction d'informer le client ou les tiers

7.1.3.2.1. Principe

Article 30, § 1er, alinéa 1er, de la loi

Les organismes et les personnes visés aux articles 2, § 1er, 3 et 4 et leurs dirigeants et employés (…) ne peuvent en aucun cas porter à la connaissance du client concerné ou de personnes tierces que des informations ont été transmises à la Cellule de traitement des informations financières en application des articles 20 ou 23 à 28 ou qu'une information du chef de blanchiment de capitaux ou de financement du terrorisme est en cours ou pourrait être ouverte.

Un respect scrupuleux de cette interdiction de divulgation apparaît capital au regard des objectifs qu'elle poursuit. D'une part, le secret des déclarations d'opérations suspectes constitue une condition indispensable pour que les auteurs d'opérations de blanchiment de capitaux ou de financement du terrorisme puissent être appréhendés et leurs avoirs saisis par les autorités judiciaires. D'autre part, l'interdiction d'informer les tiers vise également à préserver la réputation des personnes concernées aussi longtemps que ces déclarations de soupçon n'ont pas conduit au prononcé d'une sanction pénale par les autorités judiciaires.

Il importe aussi de souligner qu'une rupture de cette obligation de secret dans le but de permettre à l'auteur de l'opération de blanchiment de capitaux ou de financement du terrorisme de se soustraire aux conséquences de la déclaration effectuée ou à effectuer pourrait, en fonction des circonstances, constituer en outre un acte de complicité de blanchiment de capitaux ou de financement du terrorisme.

Il convient dès lors de considérer que cette interdiction d'informer le client couvre, non seulement la déclaration d'opération suspecte elle-même, mais également l'établissement du rapport écrit visé à l'article 14 de la loi et le résultat de l'analyse de ce rapport par le responsable du blanchiment de capitaux et du financement du terrorisme.

7.1.3.2.2. Exceptions

Article 30, § 2 et § 3, 1° et 2° de la loi

§ 2. *L'interdiction énoncée au § 1er ne s'applique ni à la divulgation aux autorités compétentes visées à l'article 38 ni à la divulgation à des fins répressives.*

§ 3. *L'interdiction énoncée au § 1er ne s'applique pas à la divulgation d'informations:*

1° entre les établissements de crédit ou établissements financiers visés à l'article 2, § 1er, 1) et 2) de la directive 2005/60/CE établis dans l'Espace économique européen ou entre de tels établissements et des établissements équivalents établis dans des pays tiers désignés par le Roi en vertu de l'article 37, § 2, alinéa 1er, 2°, dont la législation impose des obligations et un contrôle équivalents à ceux prévus par la directive, lorsque ces établissements appartiennent à un même groupe au sens de l'article 2, point 12 de la directive 2002/87/CE du 16 décembre 2002 relative à la surveillance complémentaire des établissements de crédit, des entreprises d'assurance et des entreprises d'investissement appartenant à un conglomérat financier;

2° entre les établissements de crédit ou établissements financiers visés à l'article 2, § 1er, 1) et 2) de la directive 2005/60/CE établis dans l'Espace économique européen ou entre de tels établissements et des établissements équivalents établis dans des pays tiers désignés par le Roi en vertu de l'article 37, § 2, alinéa 1er, 2°, dont la législation impose des obligations et un contrôle équivalents à ceux prévus par la directive, lorsque ces établissements interviennent en relation avec un même client et dans le cadre d'une même transaction, à condition que les informations échangées concernent ce client ou cette transaction, qu'elles soient utilisées exclusivement à des fins de prévention du blanchiment de capitaux ou du financement du terrorisme et que l'établissement

destinataire des informations soit soumis à des obligations équivalentes en matière de secret professionnel et de protection des données à caractère personnel ;

L'article 30, § 3, 1° et 2°, de la loi transpose en droit belge l'article 28, §§ 3 et 5, de la Directive 2005/60/CE. Ces dispositions prévoient, par exception à l'interdiction énoncée à l'article 30, § 1er, alinéa 1er, de la loi, une autorisation d'informer un autre organisme financier qu'une opération effectuée par un client a fait l'objet d'une déclaration de soupçon à la CTIF, lorsque le destinataire de cette information est un organisme qui intervient dans le cadre de la même opération en relation avec le même client, ou lorsqu'il appartient au même groupe que l'organisme qui la transmet.

L'objectif essentiel de ces dispositions consiste à favoriser l'efficacité de la prévention du blanchiment de capitaux et du financement du terrorisme, et donc, celle de la gestion du risque de réputation des organismes concernés. Elles ne doivent pas être comprises comme instituant une obligation de divulgation, mais permettent à l'organisme financier qui a procédé à une déclaration d'opération suspecte de décider, au cas par cas, s'il apparaît utile, au regard des objectifs poursuivis, d'informer d'autres organismes financiers concernés. Cette décision relève de la compétence du responsable de la prévention du blanchiment des capitaux et du financement du terrorisme désigné en vertu de l'article 18, alinéa 1er de la loi, et devrait s'inscrire dans le cadre de la politique définie par le groupe en matière d'échange d'informations (cf. section 10.3.2.2.4. infra).

Il est à relever par ailleurs que les paragraphes 3 et 5 de l'article 28 de la directive présentent des différences, également reflétées aux 1° et 2° de l'article 30, § 3, de la loi, quant aux conditions auxquelles sont soumis ces échanges d'informations. Ainsi, lorsque l'information est à transmettre à un organisme financier, extérieur au groupe, qui est intervenu dans le cadre de la même opération en relation avec le même client, la directive et la loi requièrent, non seulement que le destinataire soit soumis à une législation équivalente en matière de prévention du blanchiment de capitaux et du financement du terrorisme, mais aussi que les informations ne puissent être utilisées par lui qu'à cette seule fin, d'une part, et que ce destinataire soit soumis à des obligations équivalentes en matière de secret professionnel et de protection des données à caractère personnel, d'autre part. Ces conditions complémentaires ne sont pas expressément prévues lorsque l'information est transmise au sein d'un groupe. Néanmoins, ces échanges d'informations demeurent en outre régis par la loi du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. On relèvera cependant qu'en vertu de l'article 21 de celle-ci, le transfert de données pourra notamment s'effectuer vers un pays dont la Commission européenne a déjà reconnu le caractère adéquat du niveau de protection.

7.1.3.3. Exonération de responsabilité

Article 32 de la loi

Aucune action civile, pénale ou disciplinaire ne peut être intentée ni aucune sanction professionnelle prononcée contre les organismes ou les personnes visés aux articles 2, § 1er, 3 et 4, leurs dirigeants, leurs employés ou leurs représentants, (...), du chef d'une déclaration de soupçon effectuée de bonne foi, conformément aux articles 20, 23 à 28 ou 31.

7.1.4. Suivi des déclarations d'opérations ou de faits suspects

Article 23, § 1er, alinéa 2, § 2 et § 3, de la loi

§ 1er (...)

Dès réception de l'information, la Cellule en accuse réception.

§ 2. Si, en raison de la gravité ou de l'urgence de l'affaire dont elle est saisie par une déclaration de soupçons visée au § 1er, la Cellule l'estime nécessaire, elle peut faire opposition à l'exécution de toute opération afférente à cette affaire. La Cellule détermine les opérations ainsi que les comptes bancaires concernés par l'opposition.

La Cellule notifie immédiatement sa décision par télécopie ou à défaut, par tout autre moyen écrit, aux organismes et aux personnes visés à l'article 2, § 1er qui sont concernés par cette opposition.

Cette opposition fait obstacle à l'exécution des opérations, visées à l'alinéa 1er, pendant une durée maximale de deux jours ouvrables à compter de la notification.

§ 3. Si la Cellule estime que la mesure visée au § 2 doit être prolongée, elle en réfère sans délai au procureur du Roi ou au procureur fédéral, qui prend les décisions nécessaires. A défaut de décision notifiée aux organismes ou aux personnes visés à l'article 2, § 1er dans le délai visé au § 2, les organismes ou les personnes sont libres d'exécuter les opérations.

Dès l'instant où la déclaration d'une opération suspecte a été adressée à la CTIF préalablement à son exécution conformément à l'article 23, § 1er, alinéa 1er, il est recommandé à l'établissement financier déclarant de suspendre l'exécution de cette opération pendant le temps qui est nécessaire pour permettre à la CTIF de décider si les circonstances justifient qu'elle ait recourt au pouvoir d'opposition que lui confère l'article 23, § 2, de la loi.

L'attention des organismes financiers est attirée sur le fait que la CTIF peut adresser une telle décision d'opposition, non seulement à l'organisme qui lui a adressé la déclaration d'opération suspecte, mais également à tout autre organisme ou toute autre personnes visée à l'article 2, § 1er, de la loi qui serait concernée.

7.2. Déclarations de soupçons de financement de la prolifération des armes de destruction massive

L'article 11 bis du règlement (CE) n° 329/2007 du Conseil du 27 mars 2007 concernant l'adoption de mesures restrictives à l'encontre de la République populaire démocratique de Corée et l'article 23.1, d), du règlement (UE) n° 961/2010 du Conseil du 25 octobre 2010 concernant l'adoption de mesures restrictives à l'encontre de l'Iran déjà évoqués aux sections 5.1 et 6.1.2.2 supra, prévoient également une obligation de déclaration des soupçons de financement des programmes coréens et iraniens de prolifération des armes de destruction massive.

8. Règles particulières

8.1. Virements électroniques de fonds

8.1.1. Réglementation européenne

La Recommandation Spéciale VII du GAFI vise à prévenir que les systèmes de payements puissent être utilisés pour blanchir des capitaux ou assurer le financement du terrorisme. Une mise en œuvre de cette Recommandation par chaque Etat membre de l'Union européenne indépendamment les uns des autres aurait pu faire surgir un risque de discriminations entre les paiements nationaux dans un État membre et les paiements transfrontaliers entre États membres, ce qui aurait pu 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. Dans le but d'empêcher les terroristes et autres criminels d'avoir accès aux systèmes de paiement et de les utiliser pour déplacer des fonds au sein, en direction ou au départ des Etats membres de l'Espace Economique Européen, il a dès lors été jugé préférable de procéder à la mise en œuvre au niveau européen, et de manière identique dans tous les Etats membres, de la Recommandation Spéciale VII du GAFI.

Tel est l'objet du 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 [53]. Il importe de rappeler que ce règlement, dont les dispositions sont reproduites et commentées ci-après, est, de par sa nature, directement applicable dans les ordres juridiques des différents Etats membres.

La mise en application de ce règlement doit aussi être combinée avec celle des dispositions légales belges et des règlements européens imposant le gel des avoirs de certaines personnes lorsqu'il apparaît que l'examen des informations relatives au donneur d'ordre d'un transfert de fonds reçu est une personne visée par ces mesures. A cet égard, il est également renvoyé 5.1 supra.

De plus, afin de veiller à une mise en œuvre uniforme de ce règlement sous le contrôle des autorités prudentielles des Etats membres, les trois comités de contrôleurs prudentiels institués par la Commission européenne [le « comité européen des contrôleurs bancaires » (CEBS), le « comité européen des contrôleurs des assurances et des pensions professionnelles » (CEIOPS) et le « comité européen des régulateurs des marchés de valeurs mobilières » (CESR)] ont élaboré et publié le 16 octobre 2008 un document commun intitulé « *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* » [54] (ci-après « *le Common Understanding* »). Ce document vise principalement à clarifier les attentes des autorités de contrôle quant au comportement adéquat des organismes financiers lorsqu'ils reçoivent des paiements électroniques au profit de leurs clients sans que

53 JO L345 du 2 décembre 2006.

54 Cf. *http://www.c-ebs.org/getdoc/64c0be05-9e6e-44b5-a8de-da6a2ba6813e/2008-16-10-AMLTF-Common-understanding-on-payment-f.aspx*.

les informations requises par le règlement (CE) n° 1781/2006 concernant le donneur d'ordre ne soient simultanément fournies.

La CBFA s'attend à ce que les organismes financiers belges tiennent pleinement compte de ce « *Common understanding* » dans le cadre de leurs procédures et leur contrôle interne.

Sur le plan de la mise en œuvre pratique du règlement européen, l'attention est également attirée sur la « *Guidance Note* » publiée le 3 octobre 2008 par le « European Payments Council » [55], par lesquelles les entreprises européennes qui en sont membres se sont efforcées de définir des solutions opérationnelles communes pour se conformer aux obligations découlant du règlement.

8.1.2. Objet, définitions et champ d'application du règlement (CE) n° 1781/2006

Article 1er du règlement (CE) n° 1781/2006 - 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 du règlement (CE) n° 1781/2006 - 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 1er, 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 1er, paragraphes 2 ou 3, de la directive 2005/60/CE;*
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.*

Article 3 du règlement (CE) n° 1781/2006 - 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

[55] « *Guidance Notes on the implementation of Regulation (EC) No 1781/2006 on information on the payer transposing SR VII of the FATF related to anti money laundering and fight against terrorism into EC law* » Doc EPC209-08 du 3 Octobre 2008 : *http://www.europeanpaymentscouncil.eu/documents/EPC209-08_Guidance%20Notes_FATF_v2_September%202008%20Plenary.pdf*.

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 post-payés 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.

En ce qui concerne la Belgique, l'on rappellera que le Législateur a fait usage de l'article 11.5, d), de la directive 2005/60/CE (cf. article 11, § 2, 4°, de la loi du 11 janvier 1993 - cf. supra, section 4.5.3) en ce qui concerne la monnaie électronique. La dérogation prévue à l'article 3.3 du règlement (CE) n° 1781/2006 est dès lors applicable pour autant que le virement de fonds effectué par le client au moyen de la monnaie électronique qu'il possède n'excède pas 1.000 €. En revanche, outre le cas déjà évoqué plus haut où le client demande le remboursement de la monnaie électronique émise pour un montant de 1.000 € ou plus au cours d'une même année civile (cf. article 11, § 2, 4°, de la loi du 11 janvier 1993), ce client doit être identifié, et son identité doit être vérifiée conformément au règlement (CE) n° 1781/2006 pour permettre la correcte application de celui-ci lorsqu'il souhaite effectuer un virement électronique de fonds de 1.000 € ou plus au moyen de la monnaie électronique qu'il possède.

L'on relèvera également que le Législateur belge a décidé de faire usage de la faculté laissée par l'article 3.6 du règlement (CE) n° 1781/2006. L'article 7, § 1er, alinéa 2, de la loi du 11 janvier 1993 précise en effet que ces opérations ne sont pas des virements de fonds au sens du règlement (CE) n° 1781/2006 (cf. section 4.2.2.2.2 supra).

8.1.3. Obligations du prestataire de services de paiement du donneur d'ordre

Article 4 du règlement (CE) n° 1781/2006 - 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 du règlement (CE) n° 1781/2006 - 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.*

Les règles d'identification et de vérification de l'identité du donneur d'ordre définies aux articles 4 et 5 du règlement (CE)n° 1781/2006 sont pour l'essentiel cohérentes avec celles définies par la loi du 11 janvier 1993.

Dès lors qu'en vertu de l'article 7, § 1er, alinéa 3, de la loi, l'identification et la vérification portent sur le nom, le prénom et le lieu et la date de naissance du client (cf. section 4.2.3.1 supra), l'on peut s'attendre à ce que les organismes financiers assujettis au droit belge fassent généralement usage de la faculté laissée par l'article 4.2 du règlement (CE) n° 1781/2006 de remplacer l'adresse du donneur d'ordre par son lieu et sa date de naissance. S'ils choisissent néanmoins de communiquer l'adresse du donneur d'ordre, il leur appartient de vérifier préalablement cette information conformément à l'article 5.2 du règlement (CE) n° 1781/2006 sur la base de documents, de données ou de renseignements obtenus auprès d'une source fiable et indépendante. A cet effet, une simple déclaration du client concernant son adresse telle qu'évoquée à la section 4.2.6.1 ci-dessus ne peut suffire.

Article 6 du règlement (CE) n° 1781/2006 - 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 du règlement (CE) n° 1781/2006 - 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.*

L'article 6 du règlement (CE) n° 1781/2006 soumet les virements de fonds intra-communautaires à des règles allégées identiques lorsque le prestataire de services du donneur d'ordre et celui du bénéficiaire sont tous deux établis dans le même Etat membre de l'Espace Economique Européen ou lorsqu'ils sont établis dans des Etats membres différents.

Par ailleurs, la CBFA estime que les organismes financiers qui entendent recourir aux dispositions de l'article 6.1 du règlement (CE) n° 1781/2006 devraient préciser dans leurs procédures internes relatives aux virements de fonds les modalités d'organisation leur permettant de fournir à la demande et dans le délai prescrit de trois jours ouvrables les informations complètes à propos de leurs clients qui ont donné ordre d'effectuer un virement électronique de fonds national ou intra-communautaire.

8.1.4. Obligations du prestataire de services de paiement du bénéficiaire

Article 8 du règlement (CE) n° 1781/2006 - 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.

Dans leur « Common Understanding » précité, CEBS, CEIOPS et CESR ont consacré le commentaire suivant [56] à cet article du règlement (CE) n° 1781/2006 :

2. Interprétation commune de l'article 8 du règlement.

4. Les prestataires devront disposer de procédures efficaces afin de détecter si, dans le système de messagerie, ou de paiement et de règlement utilisé pour effectuer un virement de fonds, les champs relatifs aux informations concernant le donneur d'ordre sont complétés conformément aux articles 4 et 6. Ils doivent remplir cette obligation en appliquant les deux éléments suivants.

5. En premier lieu, comme le stipule le règlement, le prestataire du bénéficiaire doit détecter si, dans le système de messagerie, ou de paiement et de règlement utilisé pour effectuer un virement de fonds, les champs relatifs aux informations concernant le donneur d'ordre ont été complétés à l'aide de caractères ou d'éléments compatibles avec les conventions de ce système.

56 Pour la facilité de lecture, la présente circulaire fournit une traduction non officielle du '*common understanding*'. Néanmoins, seule la version anglaise en est la version officielle.

6. Ce premier élément découlera en général de la simple application des règles de validation de ce système, si celles-ci empêchent l'envoi ou la réception des paiements lorsque les informations obligatoires concernant le donneur d'ordre ne sont pas fournies.

7. Toutefois, il est avéré qu'il est très difficile d'évaluer l'exhaustivité de tous les messages en utilisant un filtre standard : il arrivera donc que le paiement soit effectué, même si les champs relatifs aux informations concernant le donneur d'ordre sont complétés avec des informations incorrectes ou non pertinentes.

8. Les prestataires sont en outre incités, en se fondant sur leur expérience, à utiliser des filtres permettant de détecter les informations à l'évidence non pertinentes, parfois clairement destinées à contourner les intentions de la recommandation spéciale VII du GAFI et de ce règlement : cela les aiderait à évaluer si les informations fournies sont utiles et, dans le cas contraire, ils seraient alors obligés de rejeter le virement ou de demander des informations complémentaires. Les prestataires doivent s'efforcer d'appliquer ce premier élément au moment du traitement.

9. En deuxième lieu, à moins que le prestataire n'ait détecté le caractère incomplet de tous les virements au moment du traitement, il doit, en plus du respect de l'article 8.1, soumettre les flux de paiement entrants à une surveillance appropriée afin de détecter les virements incomplets ou fournissant des informations non pertinentes, en procédant à un échantillonnage aléatoire a posteriori. Celui-ci peut se concentrer davantage sur les virements provenant de prestataires présentant un risque plus élevé, notamment ceux qui ont déjà été identifiés par cette méthode comme n'ayant pas respecté les exigences en matière d'informations. Il convient d'accorder une attention particulière, lors de l'application de cette méthode d'échantillonnage, aux prestataires identifiés comme omettant régulièrement de fournir les informations requises.

Article 9 du règlement (CE) n° 1781/2006 - 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 du règlement (CE) n° 1781/2006 - 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 du règlement (CE) n° 1781/2006 - 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.

Dans leur « Common Understanding » précité, CEBS, CEIOPS et CESR ont consacré le commentaire suivant à cet article du règlement (CE) n° 1781/2006 :

3. Interprétation commune des articles 9 §1 et 10 du règlement

10. En application de l'article 8 conformément à ce qui figure supra, les prestataires de services de paiement bénéficiaires pourraient constater la nature incomplète ou non pertinente des informations

accompagnant un virement soit au moment du traitement (voire auparavant), soit ultérieurement s'il est procédé à un contrôle a posteriori.

11. La présente section tient compte de l'article 9 §1 et de l'article 10. Ce dernier concerne en particulier les obligations de déclaration définies au chapitre III de la troisième directive. Ce chapitre comprend notamment les articles 22 et 24 qui sont particulièrement importants pour l'application de l'article 9 §1. Ces articles sont pris en compte par les présentes lignes directrices. Il convient également de noter que l'article 9 §1 du règlement fait référence aux règlements 2580/2001 et 881/2002.

3.1 Le prestataire de services de paiement constate, à la réception du virement, qu'il est incomplet

12. Si le prestataire de services de paiement constate, à la réception du virement, qu'il est incomplet, il doit soit rejeter cette opération, soit demander la totalité des informations. Pendant qu'il demande les informations complètes, il peut soit exécuter le virement, soit bloquer les fonds en suspendant temporairement l'opération (si le blocage des fonds est autorisé par la législation nationale, en tenant compte de toute obligation juridique ou relative à la protection des consommateurs).

3.1.1. Politique, processus et procédures internes

13. Les prestataires de services de paiement doivent adopter une politique définissant leur réaction lorsqu'ils constatent qu'un virement est incomplet ou assorti d'informations non pertinentes.

14. À l'exception de ceux qui ont choisi de rejeter systématiquement tous les virements de cette nature, les prestataires de services de paiement doivent s'attacher à appliquer une combinaison du point 3.1.3 avec le 3.1.4 ou le 3.1.2. Sans préjudice de toute autre législation ou de tout autre règlement éventuellement applicable, le prestataire de services de paiement ne doit normalement pas exécuter systématiquement tous les virements incomplets ou assortis d'informations non pertinentes.

15. Les prestataires de services de paiement doivent définir les critères sur lesquels les processus et les procédures internes s'appuieront afin de distinguer les virements qu'ils exécuteront directement de ceux qui feront l'objet d'un blocage ou d'un rejet. Les prestataires de services de paiement définiront ces processus et procédures internes en tenant compte de toutes les obligations applicables. Ils devront en particulier limiter le risque de conformité en cas de blocage des fonds ou de rejet du virement. En outre, les prestataires de services de paiement respecteront notamment les règlements 2580/2001 et 881/2002 ainsi que toute autre liste qu'il leur est fait obligation d'appliquer conformément à leur juridiction.

16. La politique, les processus et les procédures doivent être approuvés au niveau hiérarchique approprié et faire l'objet d'un réexamen régulier.

3.1.2 Le prestataire de services de paiement choisit de rejeter le virement (si la législation nationale l'y autorise)

17. Dans ce cas, le prestataire de services de paiement n'est pas obligé de demander les informations complètes. À l'occasion du rejet d'un virement, le prestataire de services de paiement est invité à en communiquer la raison au prestataire du donneur d'ordre.

18. Toutefois, le prestataire de services de paiement considérera la nature incomplète du virement ou la non pertinence des informations comme un facteur à prendre en compte dans l'appréciation du caractère éventuellement suspect du virement rejeté et de toutes les opérations qui y sont liées et, le cas échéant, de la nécessité de le déclarer à sa CRF (Cellule de renseignement financier). L'appréciation du caractère suspect devra se conformer aux directives et aux exigences en vigueur.

19. En fonction des critères de risque définis par le prestataire de services de paiement conformément à l'approche fondée sur les risques, le caractère incomplet ou non pertinent des informations peut entraîner ou non la nécessité de considérer l'opération comme suspecte. Si l'opération trouve son origine dans un pays n'appartenant pas à l'EEE que les États membres de l'UE considèrent comme équivalent aux normes de la directive 2005/60/CE de l'UE, le risque peut être considéré comme moins élevé. Les prestataires de services de paiement doivent effectuer cette appréciation dans le respect des obligations en vigueur et de leurs processus, procédures et politiques internes.

3.1.3 Le prestataire de services de paiement choisit d'exécuter le virement

20. Sachant que le virement est incomplet ou assorti d'informations non pertinentes, le prestataire de services de paiement choisit de l'exécuter avant de demander les informations complètes ou pertinentes au prestataire du donneur d'ordre.

21. Après avoir exécuté le virement, il doit demander les informations complètes.

La demande d'informations complètes

22. En la matière, le prestataire de services de paiement doit définir les critères qu'il utilisera pour déterminer à quelle fréquence il adressera une demande d'informations complètes au prestataire du donneur d'ordre.

23. De plus, un délai maximum entre la réception du paiement et la formulation de la demande d'informations complètes ou pertinentes doit être fixé, par exemple 7 jours ouvrés.

24. Après avoir formulé sa demande d'informations complètes ou pertinentes, le prestataire de services de paiement doit fixer un délai raisonnable, par exemple 7 jours ouvrés, ou davantage pour les messages en provenance de pays extérieurs à l'EEE, pour la réception de ces informations puis, si le niveau de risque le justifie, apprécier le caractère suspect du virement ou de toute opération liée et, à défaut de réponse satisfaisante à sa demande d'informations complémentaires, effectuer un suivi de cette demande.

L'appréciation du caractère suspect

25. Comme mentionné au 3.1.2, les prestataires de services de paiement doivent effectuer cette appréciation dans le respect des obligations en vigueur et conformément à leurs processus, procédures et politiques internes. En fonction des critères de risque définis par le prestataire de services de paiement conformément à l'approche fondée sur les risques, le facteur de risque découlant du caractère incomplet ou non pertinent des informations peut entraîner ou non une transmission interne destinée au responsable de la lutte contre le blanchiment de capitaux et le financement du terrorisme pour appréciation du caractère suspect de l'opération.

26. En outre, il convient de garder à l'esprit que le considérant 16 du règlement spécifie notamment que le prestataire de services de paiement du donneur d'ordre reste responsable de la fourniture d'informations exactes et complètes relatives au donneur d'ordre. Par conséquent, les prestataires de services de paiement des bénéficiaires ne peuvent être tenus pour responsables du manque d'informations accompagnant les virements qu'ils reçoivent, y compris s'ils exécutent de bonne foi un virement assorti d'informations incomplètes relatives au donneur d'ordre alors qu'ils ne l'auraient pas exécuté si les informations complètes avaient été fournies.

Suivi de la demande d'informations complètes

27. Le prestataire de services de paiement doit définir des politiques et mettre en place des procédures et des processus afin d'effectuer un suivi approprié de ses demandes d'informations complètes ou pertinentes. Le prestataire de services de paiement doit être à même de démontrer à son autorité de surveillance que ces politiques, processus et procédures sont de nature à permettre la réalisation de leurs objectifs, et sont effectivement appliqués. Le prestataire de services de paiement doit garder trace de sa demande, y compris de toute absence de réponse, et tenir ce dossier à disposition des autorités.

28. Par exemple, si le prestataire de services de paiement du bénéficiaire n'a pas reçu de réponse satisfaisante à sa demande d'informations complètes ou pertinentes à l'issue du délai souhaité, il doit adresser un rappel, également assorti d'un délai souhaité pour l'obtention d'une réponse, lorsque la première échéance est dépassée. Le prestataire de services de paiement peut choisir de grouper ses relances adressées aux prestataires qui n'ont pas répondu.

29. Le rappel doit également notifier au prestataire de services de paiement émetteur que, faute de réponse satisfaisante dans les délais, il fera l'objet à l'avenir d'un suivi des risques élevés en interne (cf. 2.2 supra) et sera traité selon les conditions de l'article 9 (2) du règlement (CE) n° 1781/2006. Le prestataire de services de paiement peut également choisir de spécifier cette disposition dans ses conditions générales.

3.1.4 *Le prestataire de services de paiement choisit de bloquer les fonds (si la législation nationale l'y autorise)*

30. La section 3.1.1 du présent document décrit la procédure à suivre par le prestataire de services de paiement en présence d'un virement incomplet ou d'un virement assorti d'informations non pertinentes. Comme cela est évoqué dans cette section, il convient de souligner qu'un prestataire de services de paiement peut temporairement suspendre l'exécution du virement, et donc bloquer les fonds, si le cadre juridique ou réglementaire qui le régit l'exige ou le permet. Toutefois, outre la suspension du virement sur la base de l'option consistant à demander des informations complètes, définie dans le règlement (CE) n° 1781/2006, il peut être nécessaire de « geler » les fonds pour une durée indéterminée, conformément aux mesures de « gel » des fonds et aux sanctions économiques pertinentes (comme celles définies par les règlements 2580/2001 et 881/2002), avec obligation de s'abstenir d'effectuer les transactions déclarées suspectes (article 24(1) de la directive 2005/60/CE) et ordre des autorités compétentes de différer ces transactions (article 24(1) de la directive 2005/60/CE). En outre, l'accent est également mis sur le fait que les prestataires de services de paiement devront en particulier limiter le risque juridique et de conformité en cas de blocage des fonds ou de rejet du virement, compte tenu notamment de leurs obligations contractuelles.

31. Cette option apparaît comme étant particulièrement appropriée lorsqu'il est nécessaire d'éclaircir la situation sur le plan interne ou avec d'autres membres du groupe, avec des bases de données ou avec la cellule de renseignement financier afin de confirmer ou de rejeter les soupçons de blanchiment de capitaux.

32. Lorsque le prestataire de services de paiement choisit de bloquer les fonds, il doit en tout premier lieu effectuer une demande d'informations complètes ou pertinentes.

La demande d'informations complètes

33. En la matière, le prestataire de services de paiement doit définir les critères qu'il utilisera pour déterminer à quelle fréquence il doit adresser une demande d'informations complètes ou pertinentes au prestataire du donneur d'ordre. Ces procédures doivent cependant garantir que le prestataire adresse, dans l'idéal une fois tous les sept jours ouvrables (ou davantage dans le cas des paiements en provenance des pays hors EEE), une demande d'informations complètes ou pertinentes auprès de chaque prestataire ayant effectué au moins un virement assorti d'informations incomplètes au cours des sept jours ouvrables précédents. On attire l'attention du prestataire sur le fait que même si le délai maximal autorisé est identique à celui de la section 3.1.3, c'est à lui qu'il appartient de définir les critères déterminant à quelle fréquence envoyer la demande. Dans la présente section, ces critères définis en interne doivent prendre en compte le fait que le prestataire n'est, en principe, pas en mesure de décider du rejet ou de l'exécution du virement tant qu'il n'a pas reçu de réponse à la demande d'informations complètes ou pertinentes.

34. La demande d'informations complètes ou pertinentes doit préciser le délai souhaité pour la réponse du prestataire de services de paiement du donneur d'ordre. Un délai maximal, de trois jours ouvrables par exemple, ou davantage pour les paiements en provenance de pays hors EEE, doit être fixé. Cependant, les prestataires de services de paiement des bénéficiaires peuvent décider de définir un délai plus court. Ce délai pourrait figurer dans les conditions générales du prestataire de services de paiement destinataire.

35. Une fois que le prestataire de services de paiement a envoyé sa demande d'informations complètes ou pertinentes, il doit attendre l'expiration du délai fixé, de trois jours ouvrables par exemple, pour la réception de ces informations.

36. Ensuite, s'il reçoit une réponse satisfaisante à sa demande d'informations complètes, il doit apprécier le caractère suspect de la transaction et décider, au terme de cette appréciation, d'exécuter le virement, de le rejeter ou d'envoyer une déclaration de soupçon à la cellule de renseignement financier et bloquer les fonds.

37. Le prestataire de services de paiement doit définir des politiques et mettre en place des processus et des procédures lui permettant d'assurer un suivi approprié de ses demandes d'informations complètes ou pertinentes. Il faut, en particulier, définir la marche à suivre en l'absence d'une réponse valide dans le délai requis, ainsi que les processus d'envoi d'un rappel aux prestataires ayant manqué à cette obligation. En outre, le prestataire de services de paiement doit être à même de démontrer à son autorité de supervision que ces politiques, processus et procédures sont de nature à permettre la réalisation de ses objectifs, et qu'ils sont effectivement appliqués.

38. Par exemple, s'il ne reçoit pas de réponse satisfaisante à la demande d'informations complètes ou pertinentes, il doit procéder à un suivi de la demande. Cela peut consister à envoyer un rappel, trois jours ouvrables, par exemple, après l'expiration du premier délai. Ce rappel doit fixer un délai au prestataire émetteur, par exemple trois jours ouvrables après que la première échéance est dépassée. Le rappel peut également notifier au prestataire de services de paiement émetteur que, à défaut de réponse satisfaisante dans les délais, il fera l'objet à l'avenir du suivi des risques élevés en interne (cf. 2.2 supra) et sera traité selon les conditions de l'article 9 (2) du règlement (CE) n° 1781/2006. Le prestataire de services de paiement peut également choisir de le spécifier dans ses conditions générales.

39. De plus, le rappel doit indiquer que le virement concerné est en attente. Après l'expiration du délai fixé dans le rappel, qu'il ait reçu ou non une réponse satisfaisante, le prestataire de services de paiement bénéficiaire doit apprécier le caractère suspect de la transaction et décider, à l'issue de cette appréciation, d'exécuter le virement, de le rejeter ou d'envoyer une déclaration de soupçon à la cellule de renseignement financier et bloquer les fonds. S'il décide d'exécuter le virement, il doit prendre en compte les facteurs qui l'ont amené à bloquer les fonds dans un premier temps. Pour de plus amples détails concernant l'« appréciation du caractère suspect » de la transaction, veuillez vous reporter à la section 3.1.3.

3.2 Le prestataire de services de paiement constate que le virement est incomplet après l'avoir exécuté

40. Lorsque le prestataire de services de paiement constate, après avoir exécuté le paiement, que celui-ci contenait des informations non pertinentes ou incomplètes, soit à l'issue d'un contrôle aléatoire soit d'une autre façon, il doit :

a) considérer le caractère incomplet ou non pertinent des informations comme facteur à prendre en compte dans l'appréciation du caractère éventuellement suspect du virement ou de toute autre transaction liée et, le cas échéant, de la nécessité de le déclarer à sa cellule de renseignement financier ;

b) envisager de demander les informations complètes ou pertinentes au prestataire de services de paiement du donneur d'ordre ou, le cas échéant, au prestataire de services de paiement

intermédiaire. Dans ce cas, il doit également procéder aux mesures de suivi de la demande précédemment mentionnées.

4. Interprétation commune relative à l'article 9.2

4.1 La fréquence du manquement à l'obligation d'information

41. Le considérant 17 appelle à la définition d'une approche commune concernant l'article 9.2, qui prévoit que les prestataires de services de paiement doivent prendre des dispositions à l'encontre des prestataires qui omettent régulièrement de fournir des informations complètes.

42. Cependant, le règlement ne précise pas la notion de fréquence de cette omission. Une approche commune sur ce point est hautement souhaitable, dans la mesure où une réponse commune des prestataires de services de paiement de l'UE renforcera la crédibilité et l'efficacité de leur réaction et, donc, le respect international de la recommandation spéciale VII du GAFI. C'est au prestataire de services de paiement du bénéficiaire qu'il appartient de déterminer si l'autre prestataire omet régulièrement de fournir des informations complètes. Il peut y avoir diverses raisons à cela, comme par exemple le fait d'omettre régulièrement d'insérer les informations complètes relatives au donneur d'ordre et/ou de ne pas répondre en temps voulu aux demandes. En outre, le degré d'omission peut varier selon l'approche fondée sur les risques du prestataire de services de paiement du bénéficiaire.

43. En conséquence, le prestataire de services de paiement du bénéficiaire détermine les critères permettant d'établir si le prestataire de services de paiement du donneur d'ordre a régulièrement omis de fournir des informations complètes. En attendant que le prestataire de services de paiement du bénéficiaire dispose de suffisamment de données pour analyser sa propre expérience en la matière, les critères suivants peuvent, par exemple, être utilisés :

a. le degré de coopération du prestataire de services de paiement du donneur d'ordre à l'égard des demandes d'informations complètes ou utiles qui lui sont envoyées ;

b. un seuil défini comme un pourcentage de virements incomplets ou des virements assortis d'informations non pertinentes envoyés par un prestataire donné ;

c. un seuil défini comme un pourcentage de virements toujours incomplets au cours d'une période définie ou assortis d'informations non pertinentes, après réception par le prestataire de services de paiement du donneur d'ordre d'un certain nombre de demandes d'informations complètes ou pertinentes ;

d. un seuil défini par le nombre absolu de virements incomplets ou de virements assortis d'informations non pertinentes envoyés par un prestataire donné ; et

e. un seuil déterminé par le nombre absolu de virements toujours incomplets ou assortis d'informations non pertinentes au cours d'une période définie, après réception par le prestataire de services de paiement du donneur d'ordre d'un certain nombre de demandes d'informations complètes ou utiles ;

4.2 Les dispositions à prendre

44. Dès lors qu'un prestataire de services de paiement a été identifié comme omettant régulièrement de fournir les informations requises, le prestataire de services de paiements du bénéficiaire doit lui adresser un avertissement, afin d'attirer son attention sur le fait que, conformément à la présente interprétation commune, il a été identifié comme omettant régulièrement de fournir les informations requises.

4.3 Transmission aux autorités

45. Selon les dispositions de l'article 9 §2, dès lors qu'un prestataire de services de paiement a été identifié comme omettant régulièrement de fournir les informations requises, le prestataire du bénéficiaire déclare ce fait aux « autorités responsables de la lutte contre le blanchiment de capitaux et le financement du terrorisme ». L'identification des « autorités responsables » reste du ressort de dispositions nationales, et elles doivent recevoir ces informations. Ces « autorités » sont encouragées à échanger les informations avec les autorités nationales de supervision.

46. La transmission de ces informations doit être nettement différenciée d'une déclaration de soupçon. En effet, l'objectif de cette transmission est de signaler qu'un prestataire de services de paiement donné remplit les critères qui définissent l'omission régulière d'informations dans le cadre de la présente interprétation commune, ce qui indique une difficulté à respecter la recommandation spéciale (RS) VII. Cette transmission n'implique pas que le prestataire de services de paiement soit suspecté de blanchiment de capitaux ou de financement du terrorisme. Elle implique que le prestataire peut manquer au respect de ses obligations au titre de la RS VII. Certains pays ont choisi de développer un format spécifique pour les « déclarations au titre de l'article 9 §2 ». La perception de cette distinction par les prestataires de services de paiement semble avoir ainsi été améliorée.

Les prestataires de services de paiements établis en Belgique sont invités à transmettre à la CBFA les informations visées à l'article 9, § 2, du règlement (CE) n° 1781/2006 et aux paragraphes 45 et 46 du « *common understanding* ».

Dans l'hypothèse cependant où les circonstances qui conduisent un PSP à procéder à une telle transmission d'information à la CBFA seraient simultanément de nature à faire naître la suspicion que les manquements réguliers constatés pourraient être liées au blanchiment de capitaux ou au financement du terrorisme, la transmission d'une information à la CBFA quant à ces manquements réguliers n'exonère pas l'organisme financier de procéder également à la transmission d'une déclaration d'opération suspecte à la CTIF, par application des articles 23 et suivants de la loi.

4.4 Décision de restreindre ou de mettre fin à la relation commerciale avec un prestataire de services de paiement déclaré comme omettant régulièrement de transmettre les informations requises

47. Le règlement stipule que le prestataire de services de paiement du bénéficiaire décide s'il doit ou non restreindre ou mettre fin à sa relation commerciale avec un prestataire omettant régulièrement de fournir les informations requises.

48. Pour le prestataire de services de paiement d'un bénéficiaire, mener seul une action à l'encontre d'un prestataire défaillant peut se révéler commercialement déstabilisateur, en particulier dans le cas où ce prestataire est une contrepartie importante.

49. En outre, on attend également des superviseurs qu'ils partagent leurs observations relatives aux prestataires omettant de fournir des informations et étudient les dispositions à prendre.

50. Il convient de souligner que, lorsque le prestataire de services de paiement omettant de fournir des informations est également une banque correspondante d'un pays tiers, la décision prise conformément à la présente section et l'application de l'obligation de vigilance accrue conformément à l'article 13 §3 de la troisième directive relative à la prévention du blanchiment de capitaux pourraient être entièrement intégrées au processus de gestion de la relation transfrontière avec la banque correspondante.

5. Collecte et déclaration des données en interne

51. Les prestataires de services de paiement doivent être en mesure de démontrer à leurs autorités de supervision qu'ils disposent de politiques et de procédures efficaces en matière de collecte et de déclaration des données en interne de nature à assurer le respect des exigences réglementaires. De plus, les politiques et les procédures internes de contrôle et d'audit destinées à lutter contre le blanchiment de capitaux et à combattre le financement du terrorisme doivent être soumises à une surveillance appropriée par des responsables de haut niveau.

6. Seuil

52. Il convient de garder à l'esprit, pour l'application du règlement et de la présente interprétation commune, que certains pays extérieurs à l'UE peuvent avoir conçu leur propre règlement en intégrant un seuil de 1000 dollars ou de 1000 euros au-dessous duquel la fourniture d'informations exhaustives relatives aux paiements émis n'est pas requise. Une telle disposition est autorisée par la note interprétative de la RS VII. Cela n'empêche pas les prestataires de services de paiement européens de demander, le cas échéant, les informations complètes si elles n'ont pas été fournies. L'existence d'un tel seuil, bien que pertinente pour ce qui concerne la décision fondée sur le risque d'exécuter, de bloquer ou de rejeter l'opération ainsi que pour la détermination de la régularité de l'omission d'informations, n'exclut pas l'application des procédures définies aux points 3 et 4 supra.

53. Tout seuil d'un montant supérieur ne serait pas conforme à la RS VII et tout virement associé devra être considéré comme incomplet.

8.1.5. Obligations des prestataires de services de paiement intermédiaires

Article 12 du règlement (CE) n° 1781/2006 - 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 du règlement (CE) n° 1781/2006 - Conservation des informations sur le donneur d'ordre avec le virement

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.*

8.1.6. Obligations générales et compétences en matière d'exécution

Article 14 du règlement (CE) n° 1781/2006 - 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 du règlement (CE) n° 1781/2006 - 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 font obligation aux autorités compétentes d'exercer un contrôle effectif et de prendre les mesures nécessaires pour garantir le respect des dispositions du présent règlement.*

8.2. Cover payments

Indépendamment des règles définies par le règlement (CE) n° 1781/2006 commenté ci-dessus, des initiatives complémentaires ont été prises afin d'accroître la transparence relative aux parties concernées par les « *cover payments* », lorsque ceux-ci constituent une alternative aux paiements « *séquentiels* » [57] et permettent de procéder au transfert d'une somme d'un donneur d'ordre à un bénéficiaire, lorsque ces personnes sont établies dans des pays différents, ou lorsque l'opération porte sur des devises étrangères, et lorsque la banque du donneur d'ordre et celle du bénéficiaire n'ont pas de relations directes entre elles.

Afin d'accélérer l'exécution du transfert, en particulier lorsque les différentes banques qui seraient appelées à intervenir dans un transfert séquentiel sont établies dans des fuseaux horaires différents, un « *cover payment* » permet à la banque du donneur d'ordre de donner une instruction directe de paiement à la banque du bénéficiaire (au moyen d'un message Swift MT 103), d'une part, et de lui faire

57 A savoir, un paiement recourant à l'intermédiation successive de banques correspondantes afin de faire parvenir les fonds, accompagnés des informations requises, à la banque du bénéficiaire sans qu'aucune instruction ou communication ne soit directement adressée par la banque du donneur d'ordre à celle du bénéficiaire.

simultanément mais séparément parvenir la « couverture » de ce paiement en recourant à des banques correspondantes intermédiaires, d'autre part.

Conformément au règlement (CE) n° 1781/2006 du 15 novembre 2006 commenté à la section 8.1 ci-dessus, la banque du donneur d'ordre est tenue de communiquer à la banque du bénéficiaire toutes les informations requises concernant le donneur d'ordre. En revanche, les messages Swift accompagnant la « couverture » ne comportait pas ces informations.

Afin d'accroître la transparence de ces opérations, la Communauté Swift a décidé de modifier les messages accompagnant les couvertures (MT 202cov), afin d'y prévoir des champs spécifiques destinés à fournir les données relatives au donneur d'ordre et au bénéficiaire. De plus, ces messages ne pourront être effectivement traités par le système que si ces champs sont effectivement complétés. Ce nouveau message MT 202cov est entré en application en novembre 2009.

Cette initiative a reçu le soutien explicite du Comité de Bâle qui, dans sa « Newsletter Nr 12 » [58] d'octobre 2007, a encouragé l'utilisation efficace et effective des nouvelles solutions proposées en vue d'améliorer la transparence de ces opérations. Il y annonçait en outre avoir chargé son groupe d'experts en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme d'examiner les questions de surveillance liées aux "*cover payments*" à cette initiative du secteur privé afin d'atteindre un consensus sur des principes susceptibles de guider la politique de surveillance et les priorités en vue de la mise en œuvre des nouvelles règles de transparence.

Sur la proposition de ce groupe d'experts, et tenant compte des observations formulées par toutes les parties intéressées dans le cadre de la procédure de consultation publique menée de juillet à septembre 2008, le Comité de Bâle a adopté en date du 12 mai 2009 « *Due diligence and transparency regarding cover payment messages related to crossborder wire transfers* » [59].

Par ce document, le Comité de Bâle n'entend pas ajouter de nouvelles obligations à charge des organismes financiers par rapport à ceux qui leur sont d'ores et déjà applicables en vertu de leur droit national et en particulier, pour les établissements européens, en vertu du règlement (CE) n° 1781/2006 précité. Le Comité de Bâle a cependant estimé utile de commenter la façon dont les standards existants devraient trouver à s'appliquer dans le cas spécifique des « cover payments ».

8.3. Commerce des devises

8.3.1. Bordereaux

Outre les dispositions de la loi du 11 janvier 1993, il convient en cette matière de prendre également en considération le chapitre II de l'arrêté royal du 27 décembre 1994 relatif aux bureaux de change et au commerce de devises. Ces dispositions réglementaires imposent aux organismes financiers d'établir un bordereau d'achat ou de vente lors de tout achat ou vente au comptant de devises sous forme d'espèces ou de chèques libellés en devises ou par l'utilisation d'une carte de crédit ou de paiement. Cette obligation générale s'applique aussi aux établissements de crédit et aux entreprises d'investissement.

Le bordereau doit être numéroté à l'avance ou de façon automatique et doit mentionner notamment les renseignements suivants :

1° le nom ou la dénomination de l'organisme;

2° les montants en devises de l'opération concernée;

3° le cours appliqué;

4° les charges et commissions éventuellement prélevées;

5° la date de l'opération.

Un exemplaire du bordereau doit être remis au client.

Lorsque l'opération porte sur un montant dont la contre-valeur s'élève à 10.000 € ou plus, en une seule ou en plusieurs opérations entre lesquelles un lien semble exister, l'organisme doit mentionner l'identité du client sur le bordereau, et le lui faire signer.

Les éléments d'identification à mentionner sur le bordereau sont, pour les personnes physiques, le nom, le prénom et l'adresse. Pour les personnes morales, les trusts, ou toutes autres structures juridiques dénuées de personnalité juridique, sont à mentionner leur dénomination sociale, leur siège social et l'identification de leur représentant.

58 cf. *http://www.bis.org/publ/bcbs_nl12.htm*.
59 *http://www.bis.org/publ/bcbs154.pdf?noframes=1*.

Lorsque le client agit pour le compte d'un tiers, tant l'identité du mandataire que celle du mandant sont à mentionner sur le bordereau.

Il est également à souligner que ces obligations sont d'application dès que l'opération porte sur une contre-valeur de 10.000 € ou plus, sans distinction selon qu'il s'agisse d'une opération occasionnelle ou d'une opération nouée avec un client avec lequel l'organisme entretient une relation d'affaires.

8.3.2. Devoir de vigilance

Les préposés en charge de la surveillance de première ligne peuvent éprouver des difficultés particulières à détecter les opérations "atypiques" d'achat et de vente au comptant de devises sous forme d'espèces (« change manuel de devises ») à propos desquelles ils sont tenus d'établir un rapport écrit au sens de l'article 23 de la loi.

Il appartient dès lors aux organismes qui exercent cette activité d'attirer spécifiquement l'attention de ces préposés sur celles de ces opérations qui présentent des caractéristiques telles qu'elles apparaissent particulièrement susceptibles, de par les circonstances qui les entourent, d'être liées au blanchiment de capitaux ou au financement du terrorisme.

Sont notamment visées les opérations de change manuel de devises qui présentent des caractéristiques reprises dans la liste non limitative ci-dessous:

- le fractionnement sans justification acceptable d'une opération de change manuel de devises en plusieurs opérations distinctes, ainsi que les opérations répétées et réalisées en peu de temps et portant chacune sur des montants réduits mais dont la somme totale est importante;
- les opérations portant sur des montants importants de devises en petites coupures; le change de petites coupures en grosses coupures pour des montants importants, ou le change de sommes importantes non comptées à l'avance par le client; la présentation simultanée de diverses devises, pour des montants significatifs;
- le change manuel de devises contre devises (le cas échéant via l'euro) lorsqu'il s'agit de montants importants de devises peu répandues en Belgique sans justification acceptable;
- le recours à des courriers, c'est-à-dire soit des personnes réalisant sans justification plausible des opérations de change manuel importantes pour compte de tiers ou dont il y a des raisons de croire qu'elles sont réalisées pour compte de tiers, soit des personnes accompagnées par un tiers qui surveille l'opération et refuse d'être identifié;
- les opérations de change manuel qui comportent l'usage de documents d'origine douteuse, voire de fausses pièces d'identité, ou pour lesquelles existent des problèmes lors de l'identification du client;
- les opérations de change manuel portant sur des montants importants et réalisées, spécialement en espèces, par une personne physique, et qui sont sans justification économique au regard de l'activité professionnelle déclarée par le client ou sans proportion avec cette activité;
- les opérations de change manuel de devises qui pourraient être réalisées pour le compte de sociétés écrans;
- les opérations de change manuel de devises dont il n'y a apparemment pas d'intérêt économique ou de justification plausible à les réaliser en Belgique;
- les opérations de change manuel de devises qui sont inhabituelles au regard des activités courantes de l'établissement de crédit ou de l'agence sollicitée, par exemple par leur importance et/ou par la nature des devises traitées, et pour lesquelles le client refuse de fournir une explication claire sur la justification de telles opérations;
- les opérations de change manuel de devises qui s'accompagnent d'une attitude suspecte du client comme, par exemple, le manque d'intérêt pour le cours de change ou les commissions perçues alors qu'il s'agit de montants importants.

Les programmes de formation doivent préciser qu'il appartient aux préposés des organismes confrontés à des opérations reprises dans cette liste, d'examiner avec une attention toute particulière si elles justifient l'établissement d'un rapport écrit à l'attention du responsable de la prévention du blanchiment de capitaux et du financement du terrorisme, que ces opérations soient occasionnelles ou à conclure avec des clients avec lesquels l'organisme entretient des relations d'affaires.

8.4. Limitation des paiements en espèces

Article 21 de la loi

Le prix de la vente par un commerçant d'un ou de plusieurs biens pour un montant de 15.000 euros ou plus, ne peut être acquitté en espèces, que la vente soit effectuée en une opération ou sous la forme opérations fractionnées qui apparaissent liées.

En tant que telle, cette disposition légale ne doit pas être appliquée lors du paiement de la contrepartie d'une opération financière, même si elle porte sur des billets de banque, de l'or, ou des instruments financiers qui peuvent être qualifiés de meubles corporels.

A cet égard, l'on se réfèrera notamment à l'exposé des motifs de la loi du 18 janvier 2010 qui précise [60] que « *la notion de « bien » à laquelle recourt cette disposition légale vise des biens meubles corporels tels que les véhicules, les bijoux, les meubles, les appareils ménagers, les objets de collection, les antiquités, les pièces de monnaie ancienne, les timbres de collection, les diamants, etc. En revanche, lors de la rédaction de cet article, en 2004, le législateur ne voulait pas viser les institutions financières qui ne commercialisent pas des « biens de grande valeur », mais réalisent ou exécutent des opérations sur instruments financiers au sens large (en ce compris les opérations sur titres, sur devises, sur métaux précieux, etc.). Ces organismes financiers demeurent également exclus du champ d'application de la nouvelle disposition.* »

Comme déjà indiqué précédemment (cf. sections 4.2.2.2.1 et 6.1.4.1), les organismes financiers doivent tenir compte de cette limitation dans le cadre de l'exercice de leurs obligations d'identification des clients occasionnels et de leur obligation de vigilance constate.

9. Conservations des données

Article 13 de la loi

Les organismes et les personnes visés aux articles 2, § 1er, 3 et 4 conservent, sur quelque support d'archivage que ce soit, pendant cinq ans au moins après la fin de la relation d'affaires visée à l'article 7, § 1er, alinéa 1er, 1° ou après la réalisation de l'opération visée à l'article 7, § 1er, alinéa 1er, 2° ou 3°, les données d'identification du client et, le cas échéant, de ses mandataires et de ses bénéficiaires effectifs ainsi qu'une copie des documents probants ayant servi à la vérification de l'identité de ces personnes conformément aux articles 7 à 9.

Article 15 de la loi

Sous réserve de l'application de l'exigence formulée à l'article 6, alinéa 4 de la loi du 17 juillet 1975 relative à la comptabilité des entreprises, les organismes et les personnes visés aux articles 2, § 1er, 3, 1° et 5° et 4 conservent, pendant une période d'au moins cinq ans à partir de l'exécution des opérations, une copie sur quelque support d'archivage que ce soit, des enregistrements, bordereaux et documents des opérations effectuées et ce, de façon à pouvoir les reconstituer précisément. Ils enregistrent les opérations effectuées de manière à pouvoir répondre aux demandes de renseignements visées à l'article 33, dans le délai prévu à cet article.

Ils conservent pendant la même période les rapports écrits visés à l'article 14, § 2.

Article 34, alinéa 2, du règlement

L'analyse du rapport écrit et la décision à laquelle elle a conduit par application des articles 23 à 25, 27 et 28 de la loi sont conservés conformément aux modalités définies à l'article 15, alinéa 2, de la loi.

La copie des documents probants au moyen desquels l'organisme a vérifié l'identité du client ou de son mandataire peut être prise sur support électronique qui peut aussi être utilisé pour en assurer la conservation. Les mêmes obligations de conservation sont applicables aux documents au moyen desquels l'organisme a procédé à la vérification de l'identité des bénéficiaires effectifs ou, à défaut, de la justification que cette vérification ne s'est pas révélée raisonnablement possible.

Les organismes sont en outre tenus de conserver pendant cinq ans à dater de l'exécution des opérations, une copie, sur quelque support d'archivage que ce soit, des enregistrements, bordereaux et documents des opérations effectuées. L'obligation de conserver ces données vise à permettre de reconstituer ces opérations avec précision. Elle implique dès lors que les organismes prennent les mesures nécessaires afin de pouvoir répondre de manière complète et adéquate et avec rapidité aux demandes de

60 Chambre des Représentants, 2008-2009, Doc 52 1988/001, p. 53.

renseignements émanant de la CTIF, des autorités judiciaires, ou de la CBFA. L'on notera à ce sujet que l'exposé des motifs de la loi du 12 janvier 2004 qui a modifié cette disposition légale, précise [61] que les organismes qui disposent de réseau décentralisés « *devront veiller à ce que leur organisation et notamment leur système informatique puisse produire les informations nécessaires pour permettre au siège central de satisfaire sans délai auxdites demandes de renseignements ».*

En ce qui concerne le commerce de devises, l'article 15, alinéa 3 de l'arrêté royal précité du 27 décembre 1994, impose que le bordereau constatant une opération d'achat ou de vente au comptant de devises soit conservé en original ou en copie pendant cinq ans au moins à dater de l'opération, lorsque celle-ci porte sur un montant dont la contre-valeur s'élève à 10.000 € ou plus, en une seule ou en plusieurs opérations entre lesquelles un lien semble exister.

Compte tenu des obligations de conservation en vigueur par application de l'article 15 de la loi du 11 janvier 1993, la particularité à souligner dans ce domaine d'activité consiste dans l'obligation de conserver un exemplaire du bordereau lui-même, soit en original, soit en copie, sur un support approprié qui permette aussi la conservation de l'identification et de la signature du client et, le cas échéant, l'identification du mandant pour compte de qui l'opération a été réalisée. La seule conservation de l'enregistrement de l'opération de façon à pouvoir la reconstituer précisément et répondre aux demandes de renseignements est donc insuffisante pour satisfaire aux obligations spécifiques en la matière.

L'obligation de conservation des documents définie par la loi et précisée par l'article 34, alinéa 2 du règlement, couvre également les rapports écrits relatifs aux opérations atypiques et faits suspects transmis au responsable de la prévention du blanchiment de capitaux et du financement du terrorisme, ainsi que les analyses de ces opérations et de ces faits qu'il a réalisées et les décisions qu'il a prises sur cette base.

Par ailleurs, l'article 11bis du règlement (CE) n° 329/2007 du Conseil du 27 mars 2007 concernant l'adoption de mesures restrictives à l'encontre de la République populaire démocratique de Corée et l'article 23.1, c) du règlement (UE) n° 961/2010 du Conseil du 25 octobre 2010 concernant l'adoption de mesures restrictives à l'encontre de l'Iran et abrogeant le règlement (CE) n° 423/2007, déjà évoqués précédemment [62], contiennent également des obligations complémentaires et spécifiques relatives à la conservation des données relatives aux opérations pendant cinq ans, et à l'obligation de les mettre, sur demande, à la disposition des autorités nationales.

10. Organisation et contrôle interne

10.1. Principe général

Article 16, § 1er, de la loi

Les organismes et les personnes visés aux articles 2, § 1er, 3 et 4 mettent en œuvre des mesures et des procédures de contrôle interne adéquates en vue d'assurer le respect des dispositions de la présente loi ainsi que des procédures de communication et de centralisation des informations afin de prévenir, de détecter et d'empêcher la réalisation d'opérations liées au blanchiment de capitaux et au financement du terrorisme. Les procédures de contrôle interne prendront spécifiquement en compte le risque accru de blanchiment de capitaux et de financement du terrorisme dans les cas visés à l'article 12 ou précisés par le Roi en application de l'article 37.

Plus largement, la CBFA s'attend à ce que ces procédures et ces contrôles internes soient établis de telle sorte qu'ils leurs permettent de s'assurer du respect effectif de l'ensemble de leurs obligations commentées dans la présente circulaire, en ce compris également celles relatives aux embargos financiers et au gel des avoirs de certaines personnes (voir notamment les sections 5.1 et 6.1.1), celles relatives à la prévention de la prolifération des armes de destruction massive (voir notamment les sections 6.1.2 et 7.2 supra), et celles relatives aux informations devant accompagner les virements électroniques de fonds (voir la section 8.1 supra).

En matière d'embargos financiers et de gel des avoirs de certaines personnes, cette organisation devrait notamment permettre à chaque établissement de tenir compte dans les plus brefs délais des modifications apportées aux listes en vigueur de personnes visées par ces mesures.

61 Chambre des Représentants, 2003-2004, Doc 51 0383/001, p. 37.
62 Cf. sections 5.1, 6.1.2.2 et 7.2 supra.

10.2. Désignation et rôles du responsable de la prévention

Article 18, alinéa 1er, de la loi

Les organismes et personnes visés aux articles 2, § 1er et 4 désignent une ou plusieurs personnes responsables de l'application de la présente loi au sein de leur organisme ou profession. Ces responsables sont chargés principalement de la mise en œuvre des mesures et procédures visées aux articles 16 et 17 ainsi que de l'examen des rapports écrits établis conformément à l'article 14, § 2, alinéa 2 afin d'y réserver, si nécessaire, les suites requises en vertu des articles 23 à 28.

Article 29, alinéa 1er, de la loi

La transmission d'informations visée aux articles 20, 23 à 28, est effectuée normalement par la personne désignée au sein des organismes et personnes visés aux articles 2, § 1er, 3 et 4, conformément à l'article 18 de la présente loi ou à défaut, en ce qui concerne les personnes visées à l'article 3, par ces personnes elles-mêmes.

Article 34, alinéa 1er, du règlement

Les organismes mettent en œuvre les moyens requis et établissent les procédures appropriées permettant de procéder dans les plus brefs délais à l'analyse, sous la responsabilité du responsable de la prévention du blanchiment de capitaux et du financement du terrorisme visé à l'article 18 de la loi, des rapports écrits visés à l'article 14, § 2, de la loi qui lui sont transmis conformément aux articles 31 et 32 du présent règlement, et de déterminer s'il y a lieu de procéder à la communication de ces opérations ou de ces faits à la Cellule de traitement des informations financières, conformément aux articles 23 à 25, 27 et 28 de la loi.

Article 35 du règlement

§ 1er Le ou les responsables de la prévention du blanchiment de capitaux et du financement du terrorisme visés à l'article 18 de la loi sont désignés par l'organe de direction effective de chaque organisme, après s'être assuré que la ou les personnes concernées disposent de l'honorabilité professionnelle adéquate nécessaire pour exercer ces fonctions avec intégrité.

§ 2 Le ou les responsables désignés conformément au § 1er doivent disposer de l'expérience professionnelle, de la connaissance du cadre légal et réglementaire belge en matière de prévention du blanchiment de capitaux et du financement du terrorisme, du niveau hiérarchique et des pouvoirs au sein de l'organisme, ainsi que de la disponibilité qui sont nécessaires à l'exercice effectif et autonome de ces fonctions.

§ 3 Le ou les responsables de la prévention du blanchiment de capitaux et du financement du terrorisme veillent, d'une manière générale, au respect par l'organisme de l'ensemble de ses obligations de prévention du blanchiment de capitaux et du financement du terrorisme, et, notamment, à la mise en place de l'organisation administrative et des mesures de contrôle interne requises en vertu de l'article 16 de la loi. Ils disposent du pouvoir de proposer de leur propre initiative à la direction effective de l'organisme toutes mesures nécessaires ou utiles à cet effet, en ce compris la libération des moyens requis.

Ils organisent en particulier, et mettent en application sous leur autorité les procédures d'analyse des rapports écrits établis conformément à l'article 14, § 2, de la loi et de communication d'informations à la Cellule de traitement des informations financières, conformément aux articles 23 à 25, 27 et 28 de la loi.

Ils veillent à la formation et à la sensibilisation du personnel conformément à l'article 17 de la loi et à l'article 36 du présent règlement.

Ils sont les personnes de contact privilégié, le cas échéant en concertation avec le compliance officer, avec la Commission bancaire, financière et des assurances et la Cellule de traitement des informations financières pour toutes questions relatives à la prévention du blanchiment de capitaux et du financement du terrorisme.

§ 4 Le ou les responsables de la prévention du blanchiment de capitaux et du financement du terrorisme établissent et transmettent une fois par an au moins un rapport d'activité à l'organe de direction effective de leur organisme. Ce rapport doit permettre d'évaluer l'ampleur des tentatives de blanchiment de capitaux ou de financement du terrorisme qui ont été détectées, et d'émettre un jugement sur l'adéquation de l'organisation administrative et des contrôles internes mis en œuvre, et de la collaboration des services de l'organisme à la prévention.

Une copie du rapport annuel d'activité est systématiquement adressée à la Commission bancaire, financière et des assurances et, le cas échéant, au commissaire réviseur agréé de

l'organisme. Toutefois, les organismes visés à l'article 2, § 1er, 5° et 7° de la loi, sont dispensés de cette transmission annuelle, mais tiennent les cinq derniers rapports annuels à la disposition de la Commission bancaire, financière et des assurances, et les lui communiquent sans délai à sa demande.

La désignation d'un responsable de la prévention du blanchiment de capitaux et du financement du terrorisme qui est requise par l'article 18 de la loi, et dont les conditions et modalités de désignation sont précisées à l'article 35 du règlement, constitue un élément central et essentiel de l'organisation que les organismes financiers sont légalement tenus de mettre en œuvre, tenant compte de leurs particularités propres, pour remplir leur obligation générale de collaboration à la lutte contre le blanchiment de capitaux et le financement du terrorisme.

Au sein des établissements de crédit, des entreprises d'investissement et des entreprises d'assurance, la fonction de prévention du blanchiment de capitaux et du financement du terrorisme fait partie intégrante de la fonction de « compliance » [63]. Dès lors, les principes énoncés par les circulaires D1 2001/13 du 18 décembre 2001 aux établissements de crédit, D1/EB/2002/6 du 14 novembre 2002 aux entreprises d'investissement et PPB-2006-8-CPA du 23 mai 2006 aux entreprises d'assurances trouvent à s'appliquer. Ceci vaut notamment en ce qui concerne les responsabilités respectives du conseil d'administration et du comité de direction, et en ce qui concerne le statut du responsable de la prévention du blanchiment de capitaux et du financement du terrorisme, sa place au sein de l'organisation, et les exigences en matière de compétence, d'intégrité et de discrétion.

Le rapport que le responsable de la prévention est tenu d'adresser annuellement à l'organe de direction effective, conformément à l'article 35, § 4, du règlement, constitue un document important pour lui permettre d'assumer correctement ses responsabilités, sur la base d'une évaluation régulière du phénomène constaté, des procédures de prévention et des moyens mis en œuvre à cet effet, et pour favoriser l'adaptation de ces procédures et moyens en fonction des besoins.

Dès lors, la Commission recommande que ce rapport contienne notamment:

- un aperçu structuré de la nature, du nombre et du montant des opérations concernées, des motifs de leur transmission au responsable de la prévention du blanchiment des capitaux et du financement du terrorisme, et des actions qui ont été entreprises, notamment sous la forme d'une transmission à la CTIF;
- une analyse des évolutions ou tendances, des méthodes et des moyens spécifiques éventuellement constatés en rapport avec ces pratiques de blanchiment de capitaux ou de financement du terrorisme, en ce qui concerne, notamment, le type de clientèle, le type d'opérations, les devises concernées, ou tout autre élément pertinent;
- la communication de tout élément utile concernant le fonctionnement des procédures de contrôle interne, en distinguant notamment la surveillance de première ligne et de seconde ligne, et des procédures de transmission, de centralisation et d'analyse des renseignements, en vue de prévenir, d'identifier et dénoncer les pratiques de blanchiment de capitaux ou de financement du terrorisme;
- la mention des nouvelles instructions et/ou procédures, et des initiatives de formation à la problématique du blanchiment de capitaux et du financement du terrorisme à l'attention du personnel, et, le cas échéant, l'évaluation des moyens complémentaires qui sont nécessaires à cet effet.

10.3. Organisation au sein des groupes

10.3.1. Etablissement de filiales, succursales et bureaux de représentation dans des pays faisant l'objet de contre-mesures

Article 19, de la loi

Les personnes visées à l'article 2, § 1er, 4°, 6°, 8°,11°, 13°, 14° et 15°, ne peuvent ouvrir une succursale ou un bureau de représentation domicilié, enregistré ou établi dans un Etat ou un territoire désigné par le Roi en application de l'article 27. Elles ne peuvent acquérir ou créer, directement ou par l'intermédiaire d'une compagnie financière, d'une société holding d'assurances ou d'une compagnie financière mixte, une filiale exerçant l'activité d'un établissement de crédit, d'une entreprise d'investissement ou d'une entreprise d'assurances, domiciliée, enregistrée ou établie dans un Etat ou un territoire susvisé.

63 En ce qui concerne les OPC, cette fonction de prévention fait également partie intégrante de la fonction de compliance visée à l'article 40, § 4, de la loi du 20 juillet 2004, relative à certaines formes de gestion collective de portefeuilles d'investissement.

Outre les obligations étendues de déclaration visées à l'article 27 de la loi (cf. section 7.1.1. supra), les interdictions énoncées à l'article 19 de la loi constituent des contre-mesures à l'encontre des pays et territoires dont la législation est reconnue insuffisante ou dont les pratiques sont considérées comme faisant obstacle à la lutte contre le blanchiment des capitaux et le financement du terrorisme par le GAFI.

10.3.2. Mise en œuvre de mesures cohérentes de vigilance au sein des groupes

Article 16, § 2, de la loi

Sous réserve d'autres législations applicables, les établissements de crédit de droit belge et les entreprises d'investissement de droit belge développent un programme coordonné et mettent en œuvre des procédures et une organisation coordonnées pour l'ensemble qu'ils forment avec leurs filiales et succursales et ce, en ce qui concerne leurs obligations en matière de prévention du blanchiment de capitaux et du financement du terrorisme.

Ainsi que l'indique l'exposé des motifs de la loi du 18 janvier 2010 [64], le nouvel article 16, § 2, de la loi du 11 janvier 1993 vise à créer le cadre juridique permettant aux établissements de crédit et aux entreprises d'investissement de se conformer avec toute la sécurité juridique nécessaire aux standards internationaux émis en octobre 2004 par le Comité de Bâle sur le Contrôle bancaire dans le document intitulé « *Consolidated Know-Your-Customer Risk Management* » [65]. Le Comité de Bâle y souligne en effet que le risque légal et de réputation encouru par des établissements financiers ne disposant pas de politiques adéquates de connaissance de leurs clients visant à empêcher qu'ils soient abusivement utilisés dans le cadre d'activités criminelles (notamment le blanchiment de capitaux et le financement du terrorisme) est un risque global susceptible d'affecter l'ensemble d'un groupe, alors même que l'incident qui ferait surgir le risque serait localisé dans une seule entité de ce groupe. Aussi le Comité de Bâle estime-t-il essentiel que chaque groupe développe un programme global de gestion de ce type de risques, en s'appuyant sur des politiques qui intègrent des standards définis à l'échelon du groupe.

La mise en application de ces principes, en s'appuyant sur l'article 16, § 2, de la loi, appelle les commentaires suivants.

10.3.2.1. Evaluation de l'équivalence des obligations et du contrôle applicables en vertu de la législation locale

Les dispositions de la loi du 11 janvier 1993 et du règlement de la CBFA du 23 février 2010 sont d'application territoriale. Elles ne s'appliquent dès lors pas aux succursales et filiales des organismes de droit belge qui sont établies à l'étranger.

Lorsque ces filiales et succursales sont établies dans d'autres pays membres de l'Espace économique européen, ou dans des pays tiers qui imposent des obligations et un contrôle équivalents à ceux prévus par la 3ème Directive européenne, ces filiales et succursales y sont exclusivement assujetties à la législation et à la réglementation locales en la matière.

Néanmoins, dans la perspective d'une bonne gestion du risque de réputation qui résulterait pour les organismes belges concernés eux-mêmes de l'implication de leurs succursales ou filiales établies dans ces pays dans des opérations de blanchiment de capitaux ou de financement du terrorisme, il importe que les organismes belges s'assurent du respect effectif des législations et réglementations locales applicables en la matière à ces filiales et succursales.

Les succursales et filiales d'organismes de droit belge établies dans d'autres Etats que ceux visés ci-dessus sont également soumises en premier lieu au cadre légal et réglementaire local. Il y a cependant lieu de tenir compte de ce que, par hypothèse, les obligations et le contrôle auxquels elles y sont assujetties ne sont pas équivalents à ceux requis par la 3ème Directive.

Dès lors, la CBFA considère que, dans ce cas, la gestion appropriée du risque de réputation requiert que les organismes belges mettent en œuvre des mesures renforcées d'encadrement de ces filiales et succursales en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme, sans se limiter à exiger d'elles le respect des exigences légales et réglementaires locales en la matière.

Il convient à cet égard que leur maison mère belge leur impose de mettre en œuvre des dispositifs de prévention équivalents à ceux qui sont requis par la législation et la réglementation belge, si des dispositifs équivalents de prévention ne sont pas mis en œuvre en vertu des exigences légales et réglementaires locales.

64 Chambre des Représentants, 2008-2009, Doc 52 1988/001, p. 48-49.
65 cf. http://www.bis.org/publ/bcbs110.pdf?noframes=1

Si la législation locale s'oppose à l'application de ces dispositifs renforcés, il y a lieu d'en informer la CBFA.

De la même manière, les organismes financiers belges devraient prendre toute mesure appropriée pour empêcher que leurs filiales et succursales qui ne sont pas incluses dans le champ d'application *ratione personae* du règlement (CE) n° 329/2007 du Conseil du 27 mars 2007 et du règlement (CE) n° 423/2007 du Conseil du 19 avril 2007, précités (voir section 5.1, 6.1.2.2, 7.2 et 9, supra) apportent leurs concours direct ou indirect au financement de la prolifération des armes de destruction massive.

10.3.2.2. Procédures et organisation en matière de gestion des risques en relation avec la clientèle au sein des groupes

Lorsqu'un établissement de crédit ou une entreprise d'investissement a établi des filiales et/ou des succursales à l'étranger, un des points cruciaux en vue d'une gestion effective et pertinente du risque légal et de réputation consiste dans la mise en œuvre de standards cohérents de vigilance à l'égard de la clientèle dans l'ensemble du « groupe » que constitue l'établissement belge, ses filiales et ses succursales.

Il importe donc que chaque groupe développe un programme global de gestion des risques en relation avec la clientèle, qui s'appuie sur les politiques et procédures particulières applicables au sein de chaque entité du groupe. Ces dernières devraient mettre en œuvre au niveau de l'entité considérée les standards applicables à l'ensemble du groupe et en assurer l'effectivité, même lorsque des spécificités locales ou liées aux activités exercées requièrent d'être également prises en considération.

Dans le cadre de ce programme global de gestion des risques en relation avec la clientèle, il est dès lors recommandé de mettre en œuvre un processus centralisé visant à coordonner la définition des politiques et procédures de vigilance à l'égard de la clientèle appliquées dans les différentes entités du groupe. Ces politiques et procédures coordonnées ne devraient pas seulement garantir le respect des législations et réglementations applicables à chaque entité du groupe individuellement, notamment en matière de prévention du blanchiment des capitaux et du financement du terrorisme, mais viser aussi, plus largement, à identifier, contrôler et réduire de manière cohérente au sein du groupe dans son ensemble les risques légaux et de réputation en relation avec la clientèle.

De plus la mise en application effective de ces politiques et procédures coordonnées par les différentes entités qui composent le groupe devrait également faire l'objet d'une coordination visant à en assurer la cohérence à travers l'ensemble du groupe.

Le programme global de gestion des risques en relation avec la clientèle doit inclure en particulier les politiques et procédures relatives :
- à l'identification et à la politique d'acceptation des clients ;
- à la surveillance des comptes et transactions ;
- aux mesures d'organisation et de contrôle interne requises pour s'assurer de l'effectivité de la gestion des risques.

10.3.2.2.1. Identification et politique d'acceptation des clients

Les règles applicables dans chaque entité du groupe en matière d'identification des clients, de vérification de leur identité et de conservation des données et documents d'identification doivent être définies en conformité avec les dispositions légales et réglementaires applicable à l'entité considérée et en tenant compte des spécificités liées aux activités qu'elle exerce.

Néanmoins, il apparaît nécessaire que ces règles soient également définies de manière cohérente au sein du groupe afin de s'assurer que chaque entité qui le compose recueille et vérifie l'ensemble des informations qui sont nécessaires pour une application cohérente de la politique d'acceptation des clients.

De plus, les standards applicables à la politique et à la procédure d'acceptation des clients de chaque entité du groupe devraient être définis pour l'ensemble de celui-ci de manière à lui permettre de s'assurer d'une évaluation cohérente des risques que peuvent représenter les clients, quelle que soit l'entité du groupe avec laquelle ils souhaitent entrer en relation. Dans cette perspective, ces standards devraient notamment définir de manière cohérente les catégories de clients susceptibles de présenter des risques supérieurs à la moyenne. Ces standards devraient aussi assurer la cohérence au travers du groupe des règles procédurales relatives à l'examen des demandes et à la décision d'entrée en relation avec les clients, en fonction du niveau de risque qu'ils sont susceptibles de représenter.

10.3.2.2.2. Surveillance des comptes et transactions

En vue d'une gestion cohérente des risques au sein du groupe, il importe également que la surveillance des comptes et des opérations des clients soit assurée avec un niveau équivalent ou identique de vigilance dans toutes les entités du groupe, et selon des modalités cohérentes pour l'ensemble du groupe.

À cet effet, le programme global de gestion des risques en relation avec la clientèle du groupe devrait définir des standards communs applicables au système de surveillance des comptes et transactions mis en œuvre par chaque entité du groupe. Ces standards concerneront les modalités essentielles du système de surveillance, les principaux critères de risque sur lesquels se fonde la surveillance, et les règles procédurales relatives à l'analyse et aux suites à réserver, sur la base de cette analyse, aux opérations atypiques détectées.

10.3.2.2.3. Mesures d'organisation et de contrôle requises pour s'assurer de l'efficacité de la gestion des risques

Le programme global de gestion des risques en relation avec la clientèle du groupe devrait enfin veiller à la mise en place cohérente au sein de toutes les entités du groupe des mesures requises pour garantir l'efficacité de la gestion des risques en relation avec la clientèle.

Ces mesures incluent notamment :

- la mise en œuvre d'une organisation adéquate, respectueuse notamment du principe de séparation des fonctions, en tenant notamment compte de l'application qu'il y a lieu de faire des circulaires relatives à la fonction de *compliance* adressées par la CBFA aux établissements de crédit [66], et aux entreprises d'investissement [67],
- la formation et la sensibilisation du personnel,
- la mise en œuvre de procédures appropriées de contrôle interne,
- l'inclusion effective de la gestion des risques en relation avec la clientèle dans le champ d'investigation de l'audit interne,
- les modalités de surveillance effective de la gestion des risques en relation avec la clientèle par l'organe de direction effective.

Dans ce contexte également, la Commission recommande par ailleurs aux établissements de crédit et entreprises d'investissement belges qui ont établi des filiales ou des succursales à l'étranger qu'ils s'assurent, au besoin par des contrôles sur place effectués par leur département d'audit interne, que ces filiales et succursales disposent effectivement de l'organisation administrative et du contrôle interne requis, non seulement pour se conformer à la législation locale en matière de prévention du blanchiment des capitaux et du financement du terrorisme, mais aussi aux divers standards précités qui sont définis dans le cadre du programme global de gestion des risques en relation avec la clientèle du groupe.

10.3.2.2.4. Echange d'informations au sein des groupes

Afin que les procédures et l'organisation coordonnées au niveau du groupe en matière de gestion des risques en relation avec la clientèle puissent pleinement produire leurs effets, il apparaît également nécessaire que leur mise en œuvre concrète donne lieu à des échanges d'informations entre les entités du groupe.

Un tel échange d'informations apparaît notamment souhaitable :

- pour la mise en application cohérente de la politique d'acceptation des clients, incluant l'évaluation des risques potentiels associés au profil du client;
- pour un exercice cohérent de la vigilance à l'égard des relations d'affaires et des opérations, tenant compte de l'ensemble des relations d'affaires et des opérations nouées par le client avec diverses entités du groupe;
- pour l'analyse des opérations atypiques détectées en vue de satisfaire aux obligations légales de déclaration des opérations suspectes, et assurer un suivi approprié de ces déclarations au sein du groupe.

A cet égard également, les établissements de crédit et les entreprises d'investissement qui ont établi des filiales ou des succursales à l'étranger devraient veiller à développer un encadrement approprié et

66 Circulaire D1 2001/13 du 18 décembre 2001.
67 Circulaire D1/EB/2002/6 le 14 novembre 2002.

coordonné permettant l'échange des informations nécessaires à une gestion adéquate des risques légaux et de réputation au sein du groupe.

Dans la mesure où cet échange d'informations au sein du groupe impliquera généralement la transmission, entre les entités du groupe, de données à caractère personnel concernant les clients, cet encadrement doit être défini dans le respect des dispositions légales relatives à la protection des données à caractère personnel qui sont applicables. Pour ce qui concerne la transmission d'informations à des entités situées dans des pays membres de l'EEE, les flux doivent s'effectuer dans le respect des dispositions de la loi belge du 8 décembre 1992 relative à la protection de la vie privée à l'égard des traitements de données à caractère personnel. En ce qui concerne la transmission d'informations à des filiales et succursales situées dans des pays autres que ceux de l'EEE, cette même loi les subordonne à des conditions complémentaires (notamment celles énumérées par son article 21).

Dès lors que cet échange d'informations au sein des groupes pourra concerner également des déclarations d'opérations suspectes, il convient aussi de se référer à la section 7.1.3.2.2., supra.

11. Qualité, formation et sensibilisation du personnel

Article 17 de la loi

Les organismes et les personnes visés aux articles 2, § 1er, 3 et 4 prennent les mesures appropriées pour sensibiliser leurs employés et leurs représentants aux dispositions de la présente loi. Ces mesures comprennent la participation des employés et des représentants intéressés à des programmes spéciaux pour les aider à reconnaître les opérations et les faits qui peuvent être liés au blanchiment de capitaux et au financement du terrorisme et les instruire sur les procédures à suivre en pareil cas.

Les organismes et les personnes visés aux articles 2, § 1er, 3 et 4 mettent en place des procédures appropriées pour vérifier, lors du recrutement et de l'affectation de leurs employés ou lors de la désignation de leurs représentants, que ces personnes disposent d'une honorabilité adéquate en fonction des risques liés aux tâches et fonctions à exercer.

Article 36 du règlement

§ 1er. L'obligation de formation et de sensibilisation à la prévention du blanchiment de capitaux et du financement du terrorisme visée à l'article 17 de la loi, concerne les membres du personnel des organismes et toute personne qui les représente en qualité d'indépendant,

- *dont les tâches en relation avec les clients ou les opérations les exposent au risque d'être confrontés à des tentatives de blanchiment de capitaux ou de financement du terrorisme,*
- *ou dont les tâches consistent à développer des procédures ou des outils informatiques ou autres applicables à des activités sensibles du point de vue de ce risque.*

§ 2. La formation, la sensibilisation et l'information régulière du personnel visent notamment:

- *à acquérir les connaissances et développer l'esprit critique nécessaires pour détecter les opérations atypiques;*
- *à acquérir la connaissance des procédures qui est nécessaire pour réagir adéquatement face à de telles opérations,*
- *à intégrer adéquatement la problématique de la prévention du blanchiment de capitaux et du financement du terrorisme dans les procédures et outils développés pour être appliqués à des activités sensibles du point de vue de ce risque.*

L'efficacité du dispositif de prévention contre le blanchiment de capitaux et le financement du terrorisme au sein des organismes est grandement tributaire de l'aptitude de leur personnel et de leurs représentants à contribuer à sa mise en œuvre.

Cette aptitude dépend, d'une part, de l'honorabilité de ces personnes (article 17, alinéa 2, de la loi), et d'autre part, de leurs connaissances techniques et leur sensibilisation à l'impérieuse nécessité de prévenir les opérations de blanchiment de capitaux ou de financement du terrorisme (article 17, alinéa 1er, de la loi).

Sur le premier de ces plans, il peut s'avérer utile que le responsable de la prévention désigné conformément à l'article 18 de la loi du 11 janvier 1993 soit associé à l'établissement et à la révision des procédures relatives au recrutement et à l'affectation des employés et des représentants indépendants de l'organisme afin de s'assurer que ces procédures satisfont aux exigences énoncées par l'article 17, alinéa 2, de la loi.

En ce qui concerne les connaissances techniques et la sensibilisation du personnel et des représentants, elles se fondent notamment sur l'expérience acquise dans la pratique par ces personnes, mais également, dans une large mesure, sur la qualité des programmes de formation qui doivent leur être dispensés en vertu de l'article 17, alinéa 1er, de la loi et de l'article 36 du règlement.

En ce qui concerne les préposés en charge de la surveillance de première ligne, cette formation doit notamment leur permettre de détecter avec efficacité les opérations atypiques, et d'établir correctement et dans les délais requis un rapport écrit chaque fois que cela s'impose en vertu de l'article 8 de la loi.

En ce qui concerne les personnes chargées de développer des procédures ou des outils informatiques ou autres applicables à des activités sensibles du point de vue de ce risque, cette formation doit leur permettre d'y intégrer adéquatement la problématique de la prévention du blanchiment de capitaux et du financement du terrorisme.

Dès lors, cette formation devrait utilement porter sur:
- les obligations légales et réglementaires belges applicables à l'organisme, dans leur contexte international;
- l'organisation et les procédures de prévention au sein de l'organisme;
- l'étude du phénomène de blanchiment de capitaux et de financement du terrorisme dans la pratique (typologies, facteurs de risques, etc.);
- les cas particuliers des opérations inhabituelles de change manuel de devises (cf. section 11.2. ci-dessus).

Compte tenu du caractère évolutif des techniques de blanchiment de capitaux et de financement du terrorisme, et des typologies d'opérations suspectes rencontrées, une information régulière et des séances de mise à jour des connaissances des préposés apparaissent nécessaires, sur la base d'une évaluation régulière des besoins en la matière.

12. Sanctions

Article 40 de la loi

Sans préjudice des mesures définies par d'autres lois ou d'autres règlements, l'autorité compétente visée à l'article 38 peut, en cas de non-respect, par les organismes ou par les personnes visés aux articles 2, § 1er, 3 et 4, des dispositions des articles 7 à 20, 23 à 30 et 33 de la loi du 11 janvier 1993, des dispositions du règlement (CE) N° 1781/2006 du Parlement et du Conseil du 15 novembre 2006 relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds ou des arrêtés pris pour leur exécution:

1° procéder à la publication, suivant les modalités qu'elle détermine, des décisions et mesures qu'elle prend;

2° infliger une amende administrative dont le montant ne peut être inférieur à 250 EUR et ne peut excéder 1.250.000 EUR, après avoir entendu les organismes ou les personnes dans leur défense ou du moins les avoir dûment convoqués; l'amende est perçue au profit du Trésor par l'administration de la T.V.A., enregistrement et domaines.

La Cellule est informée par l'autorité compétente des sanctions définitives prononcées en application de l'alinéa 1er.

Ces sanctions peuvent être prononcées par le Ministre des Finances à l'égard des personnes qui bénéficient d'une exemption visée à l'article 2, § 2, et qui ne respectent pas les conditions auxquelles cette exemption est soumise, conformément à l'article 37, § 2, 1°.

L'application par la Commission de sanctions, par application de l'article 40 de la loi, à l'encontre d'un organisme ne remplissant pas ses obligations légales et réglementaires en matière de prévention du blanchiment de capitaux et du financement du terrorisme est soumise aux règles de procédure définies aux articles 70 et suivants de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers.

Le Président,

Jean-Paul SERVAIS