CBFA

COMMISSION BANCAIRE, FINANCIÈRE ET DES ASSURANCES

Circulaire CBFA_2009_17 du 7 avril 2009

Services financiers via internet : exigences prudentielles

Champ d'application:

Établissements de crédit, entreprises d'assurances, entreprises d'investissement et sociétés de gestion d'organismes de placement collectif de droit belge, ainsi que les succursales belges de ces établissements qui relèvent du droit d'un État non membre de l'Espace économique européen (EEE). La circulaire est également portée à la connaissance des établissements établis en Belgique qui relèvent du droit d'un État membre de l'EEE.

Résumé/Objectifs:

La première partie de la circulaire expose les principes de base qui servent de cadre de référence à la CBFA dans son évaluation du caractère adéquat de l'organisation des établissements financiers qui fournissent leurs services via internet. Elle commente en particulier les risques ainsi que les exigences en matière d'organisation et de contrôle interne. Elle attire ensuite l'attention sur le respect des règles de conduite ainsi que sur l'impact éventuel des opérations transfrontalières via internet.
La seconde partie de la circulaire, qui en constitue l'annexe, est consacrée spécifiquement aux saines pratiques en matière de gestion des risques de sécurité des opérations via internet.

Madame,
Monsieur,

1. Justification

Les établissements de crédit, les entreprises d'assurances, les entreprises d'investissement et les sociétés de gestion d'organismes de placement collectif, ci-après dénommés collectivement "établissements financiers", doivent disposer d'une organisation appropriée à leur activité[1].

Les établissements financiers sont très nombreux à offrir des services financiers via internet dans le cadre desquels les clients peuvent effectuer des opérations et communiquer avec leur établissement.

La présente circulaire donne une série de recommandations et explique les principales dispositions du cadre réglementaire et prudentiel en vigueur qui s'appliquent spécifiquement à la fourniture de services financiers via internet.

Ces recommandations s'inspirent notamment d'un ensemble de normes internationales[2] en matière de gestion des risques qui peuvent être utiles comme cadre de référence pour la pratique belge.

[1] Voir les articles 20 et 20bis de la loi du 22 mars 1993 (établissements de crédit), l'article 14bis de la loi du 9 juillet 1975 (entreprises d'assurances), et les articles 62 et 62bis de la loi du 6 avril 1995 (entreprises d'investissement). Pour les sociétés de gestion d'organismes de placement collectif, voir l'article 153 de la loi du 20 juillet 2004 relative à certaines formes de gestion collective de portefeuilles d'investissement.

[2] "Risk Management Principles for Electronic Banking", Groupe sur la banque électronique du Comité de Bâle sur le contrôle bancaire, juillet 2003, et "Management and Supervision of Cross-Border Electronic Banking Activities", Groupe sur la banque électronique du Comité de Bâle sur le contrôle bancaire, juillet 2003.

Une annexe distincte porte spécifiquement sur les bonnes pratiques de gestion en matière de gestion des risques de sécurité liés à l'offre de services financiers via internet.

La circulaire D1 2000/2 de la CBF du 5 mai 2000 concernant les services financiers via internet, adressée aux établissements de crédit et aux entreprises d'investissement, est abrogée.

2. Champ d'application

A. Ratione personae

Les saines pratiques de gestion s'appliquent aux établissements de crédit, aux entreprises d'assurances, aux entreprises d'investissement et aux sociétés de gestion d'organismes de placement collectif de droit belge.

Elles s'appliquent également aux succursales belges d'établissements de crédit, d'entreprises d'assurances, d'entreprises d'investissement et de sociétés de gestion d'organismes de placement collectif qui relèvent du droit d'un État non membre de l'EEE.

Sans préjudice des compétences des autorités de contrôle du pays d'origine en ce qui concerne le contrôle de l'organisation et du contrôle interne, il a par ailleurs été jugé utile de porter les recommandations de la présente circulaire à la connaissance des succursales des établissements financiers qui relèvent du droit d'autres états de l'EEE. Elles serviront de référence dans le contrôle par la CBFA de ces succursales.

B. Ratione materiae

Les exigences prudentielles portent tant sur les informations et conseils fournis via internet que sur les services internet que les établissements financiers fournissent à leurs clients pour consulter et/ou gérer leurs données et effectuer des opérations.

Les établissements financiers recourent généralement pour ce faire à différents types de sites internet. L'on trouve ainsi non seulement des sites purement informatifs sur l'établissement financier, ses services et ses produits, et des sites interactifs proposant du contenu éducatif et des simulations, mais également des sites dits « transactionnels » permettant d'effectuer des services financiers tels que des virements, des paiements, des demandes de crédit, des souscriptions de police d'assurance, de la gestion d'information et des achats et ventes d'instruments de placement.

Les caractéristiques des services financiers via internet est que la communication entre les clients et leur établissement financier en ce qui concerne la consultation d'informations, la consultation de la situation des clients et l'exécution d'opérations, se déroule par l'intermédiaire de l'internet. À cet égard, la prestation des services via internet est généralement, et de plus en plus, automatisée du début à la fin de l'opération (*straight through processing*), et ce sans contrôle humain ; il est de ce fait primordial que les contrôles internes (identification du client, état des comptes, possession des valeurs mobilières vendues, limites,...) et externes nécessaires (conformité de l'opération aux règles de la bourse ou de l'infrastructure de paiement à laquelle elle est destinée) soient intégrés aux services via internet. Cette nécessité est encore renforcée par la tendance à faire se dérouler de plus en plus d'opérations, notamment boursières et en matière de paiements, en temps réel, ce qui limite à des délais extrêmement réduits le temps disponible pour effectuer les contrôles souhaités.

En raison des risques qui y sont liés, ce sont particulièrement les services transactionnels via internet qui méritent la plus grande attention sur le plan prudentiel.

3. Exigences prudentielles

A. Principes et risques liés à la fourniture de services financiers via internet

Les établissements financiers qui fournissent ou exécutent des services financiers via internet doivent, de manière générale - tout comme en cas d'utilisation d'autres canaux de distribution - respecter l'ensemble des dispositions légales et réglementaires qui s'appliquent à ces opérations.

Ces établissements doivent en outre disposer d'une structure et d'une organisation adéquates, de mécanismes de contrôle et de sécurité dans le domaine informatique ainsi que de procédures de contrôle interne appropriées, afin de couvrir adéquatement les risques spécifiques liés à l'utilisation de l'internet.

Ces risques - dont la réalisation peut avoir un impact important sur la situation financière et la réputation de l'établissement - englobent notamment :

a) ***risques juridiques*** : l'utilisation de l'internet oblige l'établissement à examiner une série de situations juridiques parfois inédites, en Belgique ou à l'étranger, qui requièrent un encadrement adéquat, alors que le cadre légal ou réglementaire est, le cas échéant, totalement nouveau, incertain, incomplet, voire inexistant ;

b) ***risques opérationnels :*** l'utilisation de l'internet dans la prestation de services suppose des systèmes et des procédures informatiques et de sécurité adaptés pour le suivi, par les collaborateurs de l'établissement, lesquels doivent être formés à cet effet, des opérations de clients ou des prestations de fournisseurs de services tiers ;

c) ***risques de réputation :*** l'établissement peut connaître une dégradation de sa réputation si sa prestation de services via internet est déficiente, peu sûre ou pas fiable, si elle ne répond pas aux attentes des utilisateurs et du public, ou si elle présente des lacunes ou comporte des infractions au regard des dispositions légales et réglementaires belges et/ou étrangères en la matière.

B. Exigences en matière d'organisation et de contrôle interne

1. Généralités

Avant de fournir des informations ou des services via internet, l'établissement financier doit identifier les risques que cela implique, adapter en conséquence son organisation et ses contrôles internes, et soumettre, au besoin, le résultat à des tests. Il y a lieu à cet égard de tenir compte de la nature, de la complexité et du volume des services fournis.

Les attentes prudentielles en la matière sont exposées ci-dessous. Elles portent notamment sur la politique générale de l'établissement, ainsi que sur les aspects spécifiques de l'organisation en matière de fourniture de services via internet, tels que l'encadrement juridique et opérationnel de l'activité, la sécurité, le rôle éventuel des intermédiaires, l'identification et l'authentification des clients, la sous-traitance et les *audit trails*.

2. Aspects relatifs à la politique

La direction effective, le cas échéant le Comité de direction, est responsable de l'élaboration d'une politique et d'une stratégie en matière de fourniture de services via internet, ainsi que de l'organisation et du suivi en la matière. Cette politique devrait être soumise à l'organe légal d'administration pour approbation. Dans le cadre de cette politique, les points suivants peuvent être mentionnés :

a) la définition d'une politique générale, financière et commerciale ;

b) la détermination des objectifs de marketing et du contenu du site internet ;

c) la fixation des objectifs et options techniques sur le plan de la sécurité tels qu'exposés plus en détail en annexe à la présente circulaire ;

d) la détermination de la gestion des risques et de l'implication des différents niveaux de contrôle de l'établissement (contrôle interne, audit interne, réviseur) ;

e) la détermination des exigences de *reporting* interne, compte tenu des risques ainsi que des menaces et incidents de sécurité constatés ;

f) l'examen et la maîtrise des implications et risques juridiques ;

g) la détermination des moyens et des procédures en matière de conservation des données ;

h) l'harmonisation du système de contrôle interne par rapport à l'organisation de la fourniture de services via internet.

La fonction d'audit interne se penche sur le fonctionnement et l'application de la politique internet dans le cadre de son programme et de ses activités d'audit, et procède à leur évaluation. Des programmes et techniques d'audit appropriés sont mis en œuvre à cet effet.

L'activité figure dans le *reporting* annuel de la direction effective concernant l'évaluation du système de contrôle interne[3].

3. Relations contractuelles

Les établissements financiers qui permettent à leur client de consulter et de gérer leur données et d'effectuer des opérations via internet concluent préalablement une convention en la matière avec leurs clients. Une telle convention spécifique n'est pas nécessaire pour les besoins d'un site internet purement informatif ne permettant pas de consulter des données personnalisées.

Cette convention doit traiter de la nature et de la portée de la fourniture de services ainsi que de l'encadrement spécifique et des modalités spécifiques de l'utilisation de l'internet. Elle doit notamment comprendre une description et une délimitation précises des responsabilités des parties dans l'utilisation des technologies mises à disposition ou recommandées par l'établissement pour les besoins de l'identification et de l'authentification du client et de la validation des opérations.

Le respect de la législation en matière de prévention du blanchiment implique en outre que l'établissement doit pouvoir être en mesure de suspendre l'exécution d'opérations pour le compte d'un client aux fins d'un contrôle de régularité, et/ou de refuser l'exécution d'une telle opération.
Il y a lieu en outre de prévoir une convention appropriée si, pour la mise à disposition, le développement, la gestion ou le soutien des sites et des services internet, il est fait appel à des fournisseurs, ainsi que dans les relations avec les contreparties et les marchés réglementés ou non participant à la fourniture des services via internet.

4. Sécurité

Les établissements financiers qui utilisent l'internet pour fournir leurs services sont exposés à différents risques en matière de sécurité.

L'annexe à la présente circulaire expose les saines pratiques de gestion que la CBFA s'attend à voir suivre par les établissements financiers dans l'adaptation de leurs plans de sécurité. Ces saines pratiques de gestion distinguent des points d'attention et des recommandations liés à la sécurité de :

- l'infrastructure informatique propre (infrastructure informatique interne, pare-feu, serveurs courriel et internet, ...) face aux menaces de l'internet, d'une part, et ;
- les opérations financières, les consultations et les actes de gestion via internet, d'autre part.

[3] Voir la circulaire CBFA_2008_12 du 9 mai 2008 sur le rapport de la direction effective concernant l'évaluation du système de contrôle interne et déclaration de la direction effective concernant le *reporting* prudentiel périodique.

Les saines pratiques de gestion sont pertinentes tant pour les grands que pour les petits établissements, bien que les caractéristiques des services internet fournis, et les menaces qui peuvent se présenter, puissent différer d'un établissement à l'autre. Il est attendu des établissements financiers qu'ils respectent les saines pratiques de gestion ou qu'ils expliquent à la CBFA en quoi et pourquoi ils s'en écartent (*comply or explain*).

Les établissements financiers sont invités à :
- effectuer une analyse delta entre leur organisation (interne) des activités internet et les instructions figurant en annexe à la présente circulaire ;
- établir une planification sur le plan des activités et moyens nécessaires.

Les principales conclusions de cette analyse delta ainsi que la planification évoquée seront transmises à la CBFA pour le **31 août 2009** au plus tard. Y seront adéquatement étayés et commentés (*comply or explain*) tous les points pour lesquels l'établissement aura jugé acceptable de s'écarter des principes de saine gestion exposés en annexe à la circulaire.

Pour les établissements financiers qui font partie d'un groupe, la dimension de groupe peut jouer un rôle important dans la concrétisation de la politique de sécurité des services internet. L'établissement doit, le cas échéant, démontrer que l'organisation du groupe ne porte pas préjudice au caractère approprié de sa politique de sécurité et des mesures qu'il prend en la matière.

La CBFA s'attend à être informée sans délai des incidents représentants des risques significatifs à l'occasion desquels des tiers ont effectivement réussi, via internet, à déjouer la sécurité des services internet ou de l'infrastructure informatique propre.

5. Aspects opérationnels - Disponibilité, continuité et bon déroulement des opérations

Un degré élevé de disponibilité constitue un étalon important, et de grande visibilité pour le monde extérieur, de la qualité et de la fiabilité des sites et services internet fournis. L'établissement détermine en la matière les objectifs de disponibilité poursuivis et s'assure que les mesures organisationnelles et techniques nécessaires en la matière soient prises. L'établissement dispose à cet égard notamment d'une gestion adaptée des incidents afin de remédier aux perturbations éventuelles des sites et services internet dans les limites des objectifs qu'il s'est proposé d'atteindre (sur le plan des délais et de la qualité).

En fonction de la nature et de l'importance des sites et services internet fournis, ainsi que des objectifs de continuité visés, l'établissement dispose également de plans d'urgence et de dispositions d'urgence adaptés afin de faire face à des perturbations de grande envergure dans les prestations de services internet. Les principes énoncés dans la circulaire PPB 2005/2 et PPB/D.256 du 10 mars 2005 concernant les "saines pratiques de gestion visant à assurer la continuité des activités des institutions financières" sont intégralement d'application en la matière.
Dans sa rédaction des plans d'urgence, l'établissement est également attentif, au cours de l'évaluation des risques et de l'analyse d'impact, à ce phénomène encore limité, mais qui prend rapidement de l'ampleur, que constituent les attaques de type "(D)DOS"[4], qui visent à porter atteinte à la disponibilité des sites et services internet fournis, de manière agressive et sur un laps de temps parfois long (quelques heures à, dans des cas exceptionnels, des semaines).

Enfin, l'établissement financier doit assurer un suivi adéquat des opérations qui lui sont transmises par l'internet, en prévoyant des procédures pour le bon déroulement de ces opérations et la maîtrise adéquate des risques inhérents. L'établissement doit veiller à ce que le personnel qui est (ou qui est susceptible d'être) en rapport avec l'application internet ait bénéficié d'une formation suffisante en la matière.

[4] Les attaques (D)DOS (*[Distributed] Denial of Service*) visent à rendre indisponibles les sites internet d'entreprises ou de particuliers, en les inondant, pendant une période déterminée, de messages internet, parfois conçus spécifiquement à ces fins.

6. Implication des prestataires de services externes

Si, dans le cadre de la fourniture de sites internet et/ou de services financiers via internet, certaines activités sont sous-traitées, ou s'il est fait appel à des prestataires de services externes pour le soutien nécessaire, l'établissement financier doit obtenir les garanties nécessaires que ce prestataire de services externe dispose de la compétence et de la qualité nécessaires pour effectuer de manière fiable et professionnelle les tâches sous-traitées, et pour en assurer la continuité.

Si l'établissement sous-traite à une tierce partie la gestion de sites et/ou services internet, la direction effective, le cas échéant le Comité de direction, veille par ailleurs à ce que le prestataire de services externe fasse effectuer les examens indépendants de sécurité nécessaires (voir les points 2.2.9 et 3.2.7 de l'annexe), à ce que l'établissement soit informé des résultats de ces examens, et à ce que le prestataire de services évalue périodiquement et aussi souvent que nécessaire la sécurité des services internet fournis, en restant attentif aux évolutions des menaces. Si le prestataire de services n'accomplit pas toutes les tâches de sécurité précitées, l'établissement s'en charge lui-même, et les responsabilités des parties concernées sont clairement déterminées dans le contrat conclu avec le prestataire de services externe. Par ailleurs, l'établissement financier doit prévoir, dans la convention conclue avec le prestataire de services, qu'il a le droit de faire réaliser à sa propre initiative un audit de sécurité.

Les principes énoncés dans les circulaires PPB 2004/5 et PPB 2006/1 du 22 juin 2004 et du 6 février 2006 respectivement, concernant les "saines pratiques de gestion en matière de sous-traitance" par les établissements de crédit, les entreprises d'investissement et les entreprises d'assurances, restent intégralement d'application.

7. Identification du client à distance

L'établissement peut, par l'intermédiaire de l'internet, atteindre des personnes qui ne peuvent être identifiées facilement par un contact "face à face" pour des raisons de distance géographique.

Pour l'identification du client à distance, les établissements sont tenus de respecter les dispositions de la loi du 11 janvier 1993, et notamment de l'article 6bis, ainsi que du règlement de la CBFA du 27 juillet 2004 approuvé par arrêté royal du 8 octobre 2004, et notamment des articles 8, § 2, 34 et 37, lesquels obligent l'établissement à disposer d'un système de surveillance permettant de détecter les opérations atypiques.

Ce régime est décrit dans les différentes circulaires de la CBFA relatives 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[5].

C. Exigences en matière de respect des règles de conduite

La relation à distance qui, en cas de prestation de services en ligne, peut être une donnée constante tant lors de la conclusion de la relation d'affaires que par la suite lors de l'exécution des transactions, exclut un certain nombre de contacts et d'interventions "humaines" classiques qui, dans d'autres cas, peuvent assurer l'échange d'informations entre l'intermédiaire et l'investisseur.

Il est dès lors important que l'établissement s'assure, lors de la conclusion de la relation d'affaires, que les services fournis à distance (l'ensemble de l'offre ou certaines parties de celle-ci) ne conduisent pas à délaisser l'échange d'informations et l'accompagnement du client.

Les établissements de crédit, les entreprises d'investissement et les sociétés de gestion d'OPC se référeront en particulier aux dispositions suivantes :
- la loi du 14 juillet 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur, et en particulier la section de cette loi qui concerne les contrats à distance ;
- les dispositions des articles 27, 28 et 28bis de la loi du 2 août 2002 ;

[5] Voir notamment la circulaire PPB 2004/8 du 22 novembre 2004 telle que modifiée par la circulaire PPB 2005/5 du 12 juillet 2005.

- l'arrêté royal du 3 juin 2007 portant les règles et modalités visant à transposer la directive concernant les marchés d'instruments financiers.

Lors de la fourniture de services d'investissement via internet portant sur des instruments financiers non complexes, l'établissement financier peut se trouver dans la situation particulière dans laquelle cette prestation de services se limite à l'exécution d'ordres ou à la réception et la transmission d'ordres (*execution only*). Dans de tels cas, l'établissement peut, en application de l'article 27, § 6, de la loi du 2 août 2002, s'abstenir de demander au client des informations sur ses connaissances et sur son expérience.

Il importe que les établissements vérifient en permanence si les conditions sont réunies pour pouvoir fournir des services dans le cadre de ce régime. Cela implique notamment qu'aucune initiative ne soit prise à l'égard du client pour inciter celui-ci à répondre à l'offre de l'établissement concernant certaines opérations.

Par ailleurs, ce régime n'exonère pas l'établissement financier de son obligation générale d'agir d'une manière honnête, équitable et professionnelle dans l'intérêt de ses clients[6], notamment en ce qui concerne son obligation de prendre des dispositions en matière de conflits d'intérêts[7] et son obligation d'atteindre le meilleur résultat possible dans l'exécution des ordres[8].

Dans l'exécution d'ordres ou la réception et la transmission d'ordres portant sur des instruments financiers complexes, l'établissement financier doit avoir préalablement recueilli auprès de son client les informations nécessaires sur ses connaissances et son expérience. Si un service ou un produit n'est pas approprié pour un client donné, l'établissement est tenu de prévoir les systèmes nécessaires pour en avertir le client concerné.

Certains établissements financiers offrent également à leurs clients la possibilité de recevoir par internet des conseils en placements.
Dans ce cas, l'établissement devra respecter le devoir de diligence visé à l'article 27, § 4, de la loi du 2 août 2002. Avant de pouvoir fournir de tels services de conseil en placements, les établissements doivent prendre les mesures nécessaires sur le plan informatique pour s'assurer que ne puissent être effectuées pour le client concerné que des opérations adéquates, compte tenu de ses connaissances, de son expérience, de sa situation financière et de ses objectifs d'investissement.

Les entreprises d'assurances se référeront en particulier aux textes suivants :
- la loi du 14 juin 1991 sur les pratiques du commerce et sur l'information et la protection du consommateur, et en particulier la section de cette loi qui concerne les contrats à distance ;
- l'arrêté royal du 22 février 1991 portant sur le règlement général relatif au contrôle des entreprises d'assurances, en particulier son article 15 ;
- la loi du 27 mars 1995 relative à l'intermédiation en assurances et à la distribution d'assurances, en particulier les articles 12bis à 12quinquies ;
- l'arrêté royal du 14 novembre 2003 relatif à l'activité d'assurance sur la vie, en particulier ses articles 8 et 72.

Pour autant que de besoin, on se référera également au code de bonne conduite relatif à la publicité et à l'information sur les assurances-vie individuelle établi par les associations professionnelles après concertation avec la CBFA.

L'on se référera enfin aux fiches d'information individuelle en matière d'assurance sur la vie et d'autres assurances, établies par les associations professionnelles en exécution de l'article 12bis, § 3, de la loi du 27 mars 1995.

6 Article 27, § 1er, de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers.
7 Article 20bis, § 2, de la loi du 22 mars 1993 relative au statut et au contrôle des établissements de crédit et article 62bis de la loi du 6 avril 1995 relative au statut des entreprises d'investissement et à leur contrôle.
8 Article 28 de la loi du 2 août 2002 relative à la surveillance du secteur financier et aux services financiers.

D. Caractère transfrontalier des services fournis ou exécutés

Un site internet ayant, par définition, une portée internationale, la fourniture et l'exécution de services par ce canal peuvent revêtir un caractère transfrontalier.

En cas de prestation de services transfrontaliers au sein de l'EEE, l'établissement doit tout d'abord se conformer aux obligations de notification telles que prévues dans son statut légal.[9] Concernant l'obligation de notification, la CBFA a, jusqu'à présent, adopté le point de vue suivant : il convient de considérer qu'une prestation de services est transfrontalière non seulement lorsque la prestation caractéristique du service (c.-à-d. la prestation essentielle, pour laquelle le paiement est dû) a lieu sur le territoire d'un autre Etat membre, mais également lorsque l'entreprise sollicite des investisseurs dans cet autre Etat membre soit en se déplaçant, soit en recourant à des techniques de vente à distance ou à des procédés de publicité, autres que la publicité de notoriété.
La question se pose de savoir quelles règles doivent s'appliquer à la prestation de services transfrontaliers. Au stade actuel, une distinction doit être établie en fonction du type de services fournis via internet.

Pour l'intermédiation en assurance ainsi que pour les services bancaires ou financiers autres que les services d'investissement, l'intermédiaire est tenu de respecter les règles d'intérêt général, en ce compris les règles de conduite, du pays sur le territoire duquel il fournit ou exécute ses services (pays d'accueil ou *host*).

En matière de services d'investissement fournis par les établissements de crédit et les entreprises d'investissement, tant les règles organisationnelles que les règles de conduite du pays d'origine (*home*) trouvent à s'appliquer. Le pays d'accueil (*host*) ne peut imposer ses propres règles en matière de services d'investissement. D'autres règles du pays d'accueil, telles que la législation relative à la prévention du blanchiment et les règles éventuelles en matière d'usage des langues restent toutefois d'application. Dans le projet de directive[10], ces mêmes principes s'appliquent également aux sociétés de gestion d'organismes de placement collectif.

En ce qui concerne plus précisément l'utilisation d'un site internet, plusieurs autorités de contrôle étrangères considèrent que l'offre via internet de services ou d'instruments provenant de l'étranger est réputée avoir lieu sur leur territoire lorsque cette offre est adressée ou mise à la disposition d'investisseurs sur ledit territoire. Pour l'appréciation de ces critères, les dossiers sont en principe examinés au cas par cas, en vue notamment de déterminer si les ressortissants du pays concerné sont spécifiquement visés (langue utilisée, prix dans la monnaie du pays, mention d'adresses de contact locales), si des transactions ou services sont effectivement effectués par l'intermédiaire du site internet, et si les investisseurs sont sollicités par e-mail ou d'autres techniques de communication.

L'établissement doit donc, au préalable, définir clairement ses objectifs commerciaux et veiller, lorsqu'il démarche des clients par l'intermédiaire de son site internet sur le territoire d'un autre Etat, à se conformer aux règles dudit Etat. Pour éviter que ses démarches soient mal comprises dans des pays non visés, l'établissement peut prendre une ou plusieurs des mesures de précaution suivantes :

a) mentionner sur le site internet que celui-ci s'adresse aux investisseurs d'une zone géographique déterminée, dans laquelle l'entreprise opère conformément à la réglementation (mention de notifications, de *warnings and disclaimers*); pour localiser un investisseur et vérifier s'il relève du groupe cible, l'établissement peut faire usage du courrier, de la téléphonie ou de techniques spéciales de localisation ;

b) veiller à ce que le contenu du site internet ou de tout autre outil de promotion (par exemple dans les médias ou la presse) ne soit pas incompatible avec la zone géographique visée (par exemple, si le

---

9 -pour les établissements de crédit, voir l'article 38 de la loi du 22 mars 1993 relative au statut et au contrôle des établissements de crédit ;
-pour les entreprises d'investissement, voir l'article 87 de la loi du 6 avril 1995 relative au statut et au contrôle des entreprises d'investissement et la lettre uniforme aux entreprises d'investissement et aux établissements de crédit de droit belge du 15 octobre 2007 ;
-pour les sociétés de gestion d'OPC, voir l'article 180 de la loi du 20 juillet 2004 relative à certaines formes de gestion collective de portefeuilles d'investissement ;
-pour les entreprises d'assurances, voir l'article 57 de la loi du 9 juillet 1975 relative au contrôle des entreprises d'assurances.

10 Article 18. 3. du projet de directive OPCVM IV.

site internet ne s'adresse pas aux investisseurs britanniques, ne pas mentionner d'adresses en Grande-Bretagne ni de prix en GBP) ;

c) protéger et contrôler l'accès du site en prévoyant des mots de passe pour tout ou partie de celui-ci, ces mots de passe n'étant bien entendu communiqués qu'à des personnes faisant partie du groupe cible ;

d) prendre contact avec les autorités de contrôle locales en vue de s'assurer que le site internet est conforme à la législation locale.

Veuillez agréer, Madame, Monsieur, l'expression de mes sentiments les meilleurs.

Le Président,

Jean-Paul SERVAIS.

Annexe : CBFA_2009_17-1 / Saines pratiques en matière de gestion des risques de sécurité des opérations sur internet.