Octobre 2010

# Principes d'application sectoriels de l'Autorité de contrôle prudentiel relatifs aux virements de fonds

Les principes d'application sectoriels, élaborés par l'Autorité de contrôle prudentiel (ACP), répondent à une demande des organismes financiers soumis au contrôle de l'ACP en vue de préciser les attentes de celle-ci relatives aux vigilances de lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT) en matière de virements de fonds.

Les principes d'application sectoriels ont ainsi pour objet :

- d'expliciter, dans un souci pédagogique, les textes en vigueur concernant les informations exigibles en matière de virements de fonds et de paiements de couverture et, en particulier, de préciser l'articulation des dispositions règlementaires européennes et celles du *Code monétaire et financier* (CMF) en matière LCB-FT telles qu'issues de la transposition de la troisième directive [1] ;
- de reprendre au compte de l'ACP et mettre à disposition, en français, les documents interprétatifs européens et du Comité de Bâle relatifs aux virements de fonds.

Les principes d'application adoptés par l'ACP sont publics. Ils ont fait l'objet d'une concertation préalable à leur adoption au sein de la Commission consultative Lutte contre le blanchiment instituée par l'ACP en application de l'article L. 612-14 du CMF, qui a donné son avis le 7 juillet 2010.

Ces principes d'application pourront faire l'objet d'adaptations par la suite pour tenir compte de l'expérience de l'ACP et des sujets que les membres de la Commission consultative LCB-FT souhaiteront approfondir, ainsi que des changements législatifs ou réglementaires éventuels ou encore des recommandations internationales intervenues le cas échéant dans le domaine des virements transfrontaliers et des paiements de couverture.

***Plan***



[1] Directive 2005/60/CE du 26 octobre 2005 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme.

Les principes d'application sont à destination des organismes financiers qui ont une activité de transferts de fonds, c'est-à-dire les établissements de crédit [2] mais aussi les établissements de paiement [3], dont l'activité professionnelle comprend la fourniture de services de virements de fonds. L'ensemble de ces personnes est désigné sous le terme « prestataires de services de paiement » (PSP) dans la suite des présentes lignes directrices.

Ces principes concernent les virements de fonds couverts par le Règlement (CE) n° 1781/2006, c'est-à-dire, conformément à l'article 2 de ce règlement, toute opération effectuée par voie électronique pour le compte d'un donneur d'ordre par l'intermédiaire d'un PSP en vue de mettre des fonds à la disposition d'un bénéficiaire auprès d'un PSP, le donneur d'ordre et le bénéficiaire pouvant être ou non la même personne. Les principes d'application sectoriels ne concernent pas les virements non couverts par le règlement, c'est-à-dire les opérations à faible risque LCB-FT mentionnées au considérant 9 et aux points 2 à 5 et 7 de l'article 3 du règlement n° 1781/2006 [4].

# 1. Présentation des textes pertinents relatifs aux virements de fonds

## 1.1 Les textes législatifs et réglementaires

***Le Règlement (CE) n° 1781/2006*** *du 15 novembre 2006 relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds électronique (« le Règlement »)*

Le Règlement, entré en vigueur le 1er janvier 2007, transpose en droit européen, la Recommandation spéciale VII (RS VII) du Groupe d'action financière (GAFI) sur les virements électroniques. La RS VII prévoit que les pays devraient prendre des mesures afin d'obliger les institutions financières à inclure des renseignements complets, exacts et utiles relatifs au donneur d'ordre (nom, adresse et numéro de compte) concernant les transferts de fonds et l'envoi des messages qui s'y rapportent. Les renseignements devraient accompagner le transfert ou le message qui s'y rapporte tout au long de la chaîne de paiement. En outre, la recommandation du GAFI prévoit que les pays prennent des mesures pour s'assurer que les institutions financières mettent en œuvre une surveillance approfondie et un suivi aux fins de détection des activités suspectes de transferts de fonds non accompagnés de renseignements complets sur le donneur d'ordre.

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 États membres de l'Espace Économique Européen, il a été décidé de procéder à la mise en œuvre au niveau européen, et de manière identique dans tous les États membres, de la RS VII.

Le Règlement est d'application directe dans les États membres de l'Union européenne (UE) et dans les États parties à l'accord sur l'Espace Économique Européen (EEE). Ses dispositions sont par conséquent directement applicables aux PSP en France métropolitaine, dans les départements d'Outre-mer ainsi qu'à Saint Martin et à Saint Barthélémy.

Les obligations découlant du Règlement ont été étendues aux collectivités françaises qui n'appartiennent pas à l'Union européenne (Pays et Territoires d'Outre-mer français ou P.T.O.M.) [5] par l'ordonnance n° 2009-102 du 30 janvier 2009 relative aux informations sur le donneur d'ordre qui doivent accompagner les virements de fonds, insérés aux articles L. 713-1 et suivants du CMF.

Le Règlement s'applique aux virements de fonds internationaux, en toutes monnaies, qui sont envoyés ou reçus par un PSP établi dans l'Espace économique européen (EEE).

---

[2] Tels que définis à l'article L. 511-1 du CMF.

[3] Tels que définis à l'article L. 522-1 du CMF.

[4] « Sont exclus du champ d'application du présent règlement les virements de fonds qui représentent un faible risque de blanchiment de capitaux ou de financement du terrorisme. Ces exclusions concernent les cartes de crédit ou de débit, les retraits dans les distributeurs automatiques de billets, les prélèvements automatiques, les chèques sous forme d'images-chèques, le paiement de taxes, d'amendes ou d'autres impôts et les virements de fonds pour lesquels le donneur d'ordre et le bénéficiaire sont tous deux des prestataires de services de paiement agissant pour leur compte. ».

[5] Sont concernés les pays et territoires suivants : Mayotte, la Nouvelle Calédonie, la Polynésie Française, Saint-Pierre-et-Miquelon, Wallis et Futuna

Par un courrier du Directeur général du Trésor à la Commission européenne en date du 28 novembre 2007, la Commission bancaire a été désignée en tant qu'autorité compétente pour assurer le contrôle effectif et la prise des mesures nécessaires à la mise en œuvre en France du Règlement, au sens de l'article 5 dudit Règlement. Aujourd'hui c'est à l'ACP qu'incombe cette compétence en matière de contrôle.

***Les dispositions du CMF issues de la transposition de la troisième directive***

Le Règlement fait référence à de nombreuses reprises aux dispositions de la troisième directive, notamment en matière d'identification du donneur d'ordre (article 5), de déclaration de soupçon (article 10). Les dispositions applicables aux prestataires de services de paiement établis en France sont celles qui figurent aux articles L. 561-2 et suivants du CMF (cf. ci-dessous II).

## 1.2 Les autres textes de référence

En matière de virements de fonds, deux documents ont été élaborés au sein de groupes de travail internationaux. Ils ont fait l'objet de consultation avec les organismes financiers. Le Secrétariat général de la Commission bancaire, auquel a succédé le Secrétariat général de l'ACP (SGACP) a participé à l'élaboration de ces documents de référence dont une traduction est jointe en annexe (cf. annexes 2 et 3) aux présents principes d'application sectoriels.

L'ACP attend des prestataires de services de paiement que ces documents soient pris en compte pour la mise en œuvre des vigilances en matière de virements de fonds et pour la définition des procédures internes.

***L'Interprétation commune*** *élaborée par l'AMLTF (Anti Money Laundering Task Force) groupe établi en 2006 par les trois comités de niveau 3 du secteur financier, le Comité européen des contrôleurs bancaires (CECB), le Comité des contrôleurs d'assurances et de pensions professionnelles (CECAPP) et le Comité européen des valeurs mobilières (CEVM), des obligations imposées aux PSP des bénéficiaires des virements par le règlement (CE) n° 1781/2006 (cf. annexe 2*

L'Interprétation commune ne doit pas être considérée comme une extension du Règlement qui ajouterait des obligations, mais plutôt comme un éclaircissement des exigences qu'il contient, permettant de fournir aux PSP une interprétation commune des attentes des autorités de supervision de l'UE et de l'EEE, assurant ainsi une égalité de traitement quant à son respect.

L'Interprétation commune concerne les articles 8, 9 et 10 du Règlement, relatifs aux obligations applicables au prestataire de services de paiement du bénéficiaire.

***Les recommandations du Comité de Bâle de mai 2009 (cf. annexe 3) relatives aux obligations de vigilance et de transparence en matière de messages des paiements de couverture dans le cadre de virements internationaux.***

Le traitement des virements de fonds internationaux nécessite souvent l'intervention de plusieurs prestataires de services de paiement dans la mesure où le PSP du donneur d'ordre et celui du bénéficiaire n'ont pas toujours de relations directes, et utilisent des banques intermédiaires correspondantes.

Les banques utilisent les paiements de couverture pour faciliter les transferts de fonds pour le compte d'un client et à destination d'un bénéficiaire, qui se trouve le plus souvent dans un autre pays, mais qui peut aussi être situé dans le même pays si le paiement s'effectue dans une devise étrangère.

Les recommandations du Comité de Bâle de mai 2009 en matière de vigilance et de transparence pour les messages de paiements de couverture dans le cadre de virements transfrontaliers pointent les pratiques des formats de messages qui n'assurent pas la pleine transparence des informations complètes sur le donneur d'ordre et sur le bénéficiaire aux prestataires de services de paiement intermédiaires de couverture. Elles

décrivent « une conception commune de ce que devraient être les missions des autorités de contrôle… » [6] concernant le rôle respectif des PSP, y compris des banques intermédiaires de couverture, de la chaîne de paiement pour améliorer la transparence des messages des paiements de couverture dans le cadre de virements internationaux.

Les banques intermédiaires peuvent prendre place dans la chaîne d'exécution d'un paiement de couverture qui facilite les virements de fonds entre les comptes des clients. En effet, dans ce cadre, le prestataire de services de paiement du donneur d'ordre donne directement instruction, dans un message d'ordre de virement, en pratique un message de type SWIFT MT 103, au PSP du bénéficiaire de procéder au paiement sur le compte du bénéficiaire. Dans le même temps, le transfert des fonds entre les comptes des PSP du donneur d'ordre et du bénéficiaire transite par les banques intermédiaires de couverture, dans le cadre d'un autre message, SWIFT MT 202. Par ailleurs, conformément à la recommandation spéciale VII du GAFI et à sa note interprétative, tout PSP dans la chaîne des paiements est tenu de vérifier que toutes les informations exigées en cas de virement et relatives au donneur d'ordre sont bel et bien transmises avec les ordres de transfert.

Les banques intermédiaires recevant des messages de type SWIFT MT 202 ne disposaient pas d'informations relatives au donneur d'ordre et au bénéficiaire du virement alors que ces informations étaient incluses dans le message envoyé à la banque du bénéficiaire (message de type SWIFT MT 103). Cette absence d'information à propos du donneur d'ordre et du bénéficiaire dans les transferts de fonds pouvait entraver ou restreindre la capacité d'une banque intermédiaire à évaluer précisément les risques associés aux opérations effectuées. La banque intermédiaire n'était pas non plus en mesure de vérifier les informations relatives au donneur d'ordre en les comparant avec les listes de personnes physiques et morales dont les actifs doivent être bloqués, rejetés ou gelés aux termes de la législation locale. Cette impossibilité pouvait se révéler particulièrement problématique lorsque la liste établie dans le pays de la banque intermédiaire est plus complète que celle du pays du donneur d'ordre (ou du bénéficiaire).

Des travaux ont été engagés par le secteur privé afin que des informations plus détaillées sur les donneurs d'ordre et les bénéficiaires des transferts de fonds soient mises à la disposition des banques intermédiaires et permettent de renforcer la transparence des virements internationaux.

En novembre 2009, un nouveau type de messages, MT 202 COV, a été mis en place par SWIFT, qui permet de mettre à la disposition des banques intermédiaires une information sur le donneur d'ordre et sur le bénéficiaire du virement de fonds, en pratique une information identique à celle qui figure le MT 103. La mise en œuvre de la solution technique développée par SWIFT permet de renforcer la transparence tout au long de la chaîne de paiements. D'autres normes pourraient également être définies pour permettre d'assurer la transparence des messages.

## 2. La mise en œuvre des obligations de vigilance relatives aux informations exigibles en matière de virements de fonds

Le Règlement prévoit des obligations spécifiques pour les prestataires de services de paiement selon leur place dans la chaîne de paiement (PSP du donneur d'ordre, du bénéficiaire et PSP intermédiaires). Par ailleurs, les documents élaborés par l'AMLTF et le Comité de Bâle précisent les modalités de mise en œuvre de ces obligations.

Conformément à l'article 2 du Règlement, il faut entendre par :

- **donneur d'ordre**, 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 au PSP d'effectuer un virement de fonds ;
- **bénéficiaire**, la personne physique ou morale qui est le destinataire final prévu des fonds virés ;
- **prestataire de services de paiement intermédiaire**, un PSP qui n'est ni celui du donneur d'ordre ni celui du bénéficiaire du virement de fonds et qui participe à l'exécution du virement de fonds.

[6] Recommandations de Bâle, mai 2009, §7.

## 2.1 La mise en œuvre des obligations du prestataire de services de paiement du donneur d'ordre

### 2.1.1 Le Principe

Les articles 4, 5.1 et 7.1 du Règlement prévoient que les prestataires de services de paiement du donneur d'ordre d'un virement de fonds s'assurent que les virements de fonds sont accompagnés d'informations complètes sur le donneur d'ordre, c'est-à-dire de son nom, adresse et de son numéro de compte. S'agissant d'un donneur d'ordre personne morale, le nom s'entend comme la dénomination ou la raison sociale de la personne morale qui donne l'ordre d'effectuer un virement de fonds

Avant d'exécuter le virement de fonds, le PSP du donneur d'ordre doit vérifier les informations complètes relatives au donneur d'ordre sur la base de documents, de données ou d'informations obtenus à partir d'une source fiable et indépendante, en application de l'article 5.2 du Règlement. L'identité du client donneur d'ordre doit être vérifiée par la présentation d'un document officiel en cours de validité portant photographie conformément aux articles L.561-5 et R.561-5 du *Code monétaire et financier,* et dans les conditions de l'article R.561-10 II 3° pour un client occasionnel, dès le premier euro.

Il convient de rappeler que l'article 5.3 du Règlement dispose, toutefois, que la vérification de l'identité du client donneur d'ordre est présumée faite si le donneur d'ordre est titulaire d'un compte, à partir duquel est effectué le virement de fonds, et que son identité a déjà fait l'objet d'une vérification lors de l'ouverture du compte ; sous réserve par ailleurs que les documents justificatifs obtenus à cette occasion aient été conservés dans les conditions de l'article L.561-12 du *Code monétaire et financier,* et sans préjudice, le cas échéant, de l'identification du bénéficiaire effectif [7] lors de l'entrée en relation d'affaires.

Le PSP du donneur d'ordre doit veiller à ce que les messages qu'il envoie à une banque intermédiaire contiennent les informations, telles qu'exigées par le Règlement, sur le donneur d'ordre et sur le bénéficiaire. Les informations transmises relatives au donneur d'ordre doivent être complètes conformément au Règlement [8].

### 2.1.2 Les dérogations

***a) Les virements au sein de l'Union européenne et de l'EEE***

Le Règlement prévoit une dérogation au principe d'exigence de transmission, par le prestataire de services de paiement du donneur d'ordre, des informations complètes sur le donneur d'ordre accompagnant un virement de fonds, concernant les virements de fonds intra-communautaires, posé à l'article 5.1. En effet, en application de l'article 6.1 du Règlement, les virements de fonds au sein de l'Union européenne et de l'EEE doivent seulement être accompagnés d'informations simplifiées concernant le donneur d'ordre, c'est-à-dire du numéro de compte du donneur d'ordre ou d'un identifiant unique permettant d'assurer la traçabilité de l'opération quant au donneur d'ordre.

L'obligation du prestataire de services de paiement du donneur d'ordre de vérifier les informations relatives au donneur d'ordre avant d'exécuter le virement de fonds prévue à l'article 5.2 demeure. Elle s'applique dans les conditions de l'article 6.1. L'obligation de vérification porte alors non pas sur les informations complètes mais sur les informations simplifiées, c'est-à-dire sur le numéro de compte du donneur d'ordre ou l'identifiant unique.

Toutefois les informations complètes sur le donneur d'ordre doivent être mises à la disposition du PSP du bénéficiaire qui en fait la demande, par le prestataire de services de paiement du donneur d'ordre, dans un délai de trois jours ouvrables suivant la réception de la demande (article 6.2 du Règlement). Le prestataire de services de paiement du donneur d'ordre doit donc disposer de procédures internes lui permettant de répondre à la demande d'informations complètes relatives au donneur d'ordre, dans le délai prescrit des trois jours ouvrables, pour un virement de fonds au sein de l'Union européenne et de l'EEE.

[7] Tel que défini à l'article L. 561-2-2 du CMF

[8] Recommandations de Bâle, mai 2009, § 20 et 21

***b) Les virements avec des prestataires de services de paiement établis dans des territoires ou des pays ne faisant pas partie de l'Union européenne ni de l'EEE***

L'article 17 du Règlement concernant les accords avec des territoires ou des pays ne faisant pas partie du territoire de la Communauté dispose que :

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

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

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

*et*

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

À ce jour, les cas suivants sont prévus :

- **les virements à destination et en provenance des P.T.O.M. français**

  La Commission européenne a autorisé la France par une décision du 26 novembre 2009 [9] à traiter les virements entre la France membre de l'Union européenne et Saint-Pierre-et-Miquelon, Mayotte, la Nouvelle-Calédonie, la Polynésie française et Wallis-et-Futuna comme des virements de fonds à l'intérieur de la France membre de l'Union européenne, conformément notamment à l'article 17 du Règlement.

  À ce titre, les virements de fonds à destination et en provenance des P.T.O.M. français doivent seulement être accompagnés du numéro de compte du donneur d'ordre ou d'un identifiant unique ;

- **les virements entre la Principauté de Monaco et la France**

  La décision de la Commission européenne en date du 4 mai 2010 [10] a autorisé la France à traiter les virements avec la Principauté de Monaco comme des virements de fonds à l'intérieur de la France. Les virements de fonds peuvent être accompagnés d'informations simplifiées concernant le donneur d'ordre et ne comporter que le numéro de compte du donneur d'ordre ou un identifiant unique comme le prévoit le Règlement pour les virements au sein de l'Union européenne.

Les mesures décrites ci-dessus au a) relatif à la dérogation concernant l'information complète doivent être mises en œuvre en cas de virement en direction d'un prestataire de services de paiement établi dans un PTOM français ou dans la Principauté de Monaco.

## 2.2 La mise en œuvre des obligations des prestataires de services de paiement intermédiaires

Le Règlement impose aux PSP intermédiaires, intervenant dans une chaîne de virements, une obligation de veiller à ce que toutes les informations reçues sur le donneur d'ordre accompagnant un virement de fonds soient conservées avec ce virement (article 12). Il en découle que les PSP doivent transmettre les éléments d'information accompagnant les virements de fonds tels que reçus sans modification, ni suppression, à l'exclusion des situations de limites techniques mentionnées à l'article 13 du Règlement, dans le but d'assurer la traçabilité complète des informations concernant le donneur d'ordre.

[9] Décision de la Commission européenne du 26 novembre 2009, JOUE L. 312 du 27.11.2009, p. 71 et s.

[10] Décision de la Commission européenne du 4 mai 2010, JOUE L.112 du 5.05.2010, p.23 et s.

## 2.3 La mise en œuvre des obligations du prestataire de services de paiement du bénéficiaire

### 2.3.1 La détection d'informations manquantes sur le donneur d'ordre (article 8 du Règlement [11])

Le prestataire de services de paiement du bénéficiaire est tenu de détecter les informations manquantes dans les champs des messages concernant le donneur d'ordre du virement. À cette fin, le PSP du bénéficiaire doit mettre en œuvre des procédures efficaces permettant de détecter si les informations requises d'une part par l'article 6 pour les virements de fonds au sein de l'Union européenne, les virements entre les P.T.O.M. et la France, et entre Monaco et la France en application de l'article 17 du Règlement (cf. supra 2.1 (informations simplifiées) et d'autre part par l'article 4 dans les autres cas, sont présentes.

Parmi les mesures aux fins de détection préconisées dans l'Interprétation commune de l'AMLTF, notamment:

- au moment de la réception du virement, les PSP sont incités à mettre en œuvre des mesures de contrôle (« filtres ») des champs relatifs aux informations concernant le donneur d'ordre, directement sur la plate forme Swift de l'établissement, permettant de détecter les informations manquantes, incomplètes ou clairement non pertinentes. En pratique « …il est avéré qu'il est très difficile d'évaluer l'exhaustivité de tous les messages de virements, les PSP des bénéficiaires mettent en œuvre des contrôles après réception » ;
- *a posteriori*, dans un souci de suivi permanent des informations d'identification concernant le donneur d'ordre, il est recommandé aux PSP de « soumettre [a posteriori] les flux de paiements entrants à une surveillance appropriée afin de détecter les virements incomplets ou fournissant des informations non pertinentes, en procédant à un échantillonnage aléatoire ». Il est indiqué qu'une surveillance appropriée peut être modulée selon une approche par les risques, pour risques élevés, « notamment en accordant une attention particulière (…) aux PSP identifiés comme omettant régulièrement de fournir les informations requises ».

Ces mesures de détection et de suivi des informations d'identification manquantes, concernant le donneur d'ordre dans les messages de virements de fonds internationaux, s'inscrivent dans les procédures relatives aux obligations de vigilance prévues aux chapitre Ier et II du titre VI du livre V du Code monétaire et financier, notamment au chapitre II, relatif au gel des avoirs, dont se dote le prestataire de services de paiement en tenant compte des risques identifiés par sa classification des risques (point 4 de l'article 11-7).

À cet égard, l'article 11-7 du règlement n° 97-02 du 21 février 1997 modifié relatif au contrôle interne des établissements de crédit, des établissements de paiement et des entreprises d'investissement prévoit l'obligation de se doter de dispositifs de suivi et d'analyse des relations d'affaires adaptés aux activités, aux clientèles, aux implantations de l'entreprise assujettie et aux risques identifiés par la classification des risques de blanchiment et de financement du terrorisme. L'objectif de cette obligation est la détection de toute anomalie au regard du profil de la relation d'affaires ou de toute opération au bénéfice d'une personne ou d'une entité faisant l'objet d'une mesure de gel des avoirs (point 2.2 de l'article 11-7).

[11] Interprétation commune du 16 octobre 2008, §2, p.3 et s.

### 2.3.2 Les mesures à mettre en œuvre en cas d'informations manquantes ou incomplètes (article 9)

– En application de l'article 9.1 [12], si les informations sur le donneur d'ordre sont manquantes ou incomplètes, le PSP du bénéficiaire doit, au moment de la réception du virement de fonds, soit refuser le virement, soit, en attendant les informations complètes demandées, conserver les fonds ou exécuter le virement.

  L'Interprétation commune de l'AMLTF (cf. annexe 2) indique, à cette fin, que le prestataire de services de paiement doit adopter des procédures internes qui font l'objet d'un réexamen régulier, afin de définir son action et d'assurer le suivi de la demande d'informations complètes. Il devra notamment définir « les critères sur lesquels les procédures internes s'appuieront afin de distinguer les virements qu'il exécute directement de ceux qui feront l'objet d'un blocage et/ou d'un rejet », dans le cadre d'une approche fondée sur les risques. Les procédures internes mises en place en cohérence avec la classification des risques du PSP devront faire l'objet d'une approbation à un niveau hiérarchique approprié, conformément aux attentes des superviseurs européens [13].

– En application de l'article 9.2 premier alinéa [14], plusieurs obligations, à la charge du PSP du bénéficiaire, sont prévues. Leur mise en œuvre est graduée.

  Dans un premier temps, si un prestataire de services de paiement du donneur d'ordre omet régulièrement de fournir les informations complètes requises sur le donneur d'ordre, le PSP du bénéficiaire prend des mesures progressives visant à y remédier (avertissements, fixation d'échéances). Dans un deuxième temps, il a la possibilité, soit de rejeter tout nouveau virement du PSP en cause, soit d'engager une démarche visant à restreindre le champ de la relation commerciale ou de rompre la relation commerciale avec ce PSP régulièrement défaillant.

### 2.3.3 Les mesures de suivi permanent et d'évaluation des risques (l'article 10) [15]

L'article 10 du Règlement requiert du prestataire de services de paiement du bénéficiaire qu'il considère les informations manquantes ou incomplètes sur le donneur d'ordre comme un facteur à prendre en compte dans l'évaluation des risques LCB-FT, en particulier pour l'appréciation du caractère éventuellement suspect du virement de fonds ou de toutes opérations liées à ce virement. À cet égard, il en est de même de l'analyse conduisant le cas échéant, à effectuer une déclaration de soupçon auprès de TRACFIN conformément à l'article L.561-15 du *Code monétaire et financier*. En effet, la déclaration à l'ACP de manquements réguliers d'un PSP à fournir les informations complètes requises, conformément à l'article 9-2du Règlement n'exonère pas les organismes financiers de procéder, le cas échéant, à la déclaration d'opérations suspectes à TRACFIN.

L'Interprétation commune précise à cet égard que l'appréciation du caractère suspect doit s'effectuer en fonction de critères de risques définis par le prestataire de services de paiement conformément à l'approche par les risques, dans le cadre de ses procédures internes, et dans le respect des obligations en vigueur.

Il ne saurait être question dans ce cadre, que le PSP effectue des déclarations automatiques auprès de TRACFIN du seul fait de la détection de virements de fonds internationaux reçus sans information sur le nom du donneur d'ordre. La mise en œuvre des obligations de déclaration de soupçon auprès de TRACFIN en application de l'article L.561-15 repose en principe sur une analyse au cas par cas des anomalies détectées, comme développé dans les lignes directrices conjointes de l'ACP et de TRACFIN sur la déclaration de soupçon.

12 Interprétation commune du 16 octobre 2008, §3, p.5 et s.
13 Interprétation commune du 16 octobre 2008, §15
14 Interprétation commune du 16 octobre 2008, §3, p.11 et s.
15 Interprétation commune du 16 octobre 2008, §3, pages 5, 6, 7, 8, 9 et 11.

#### 2.3.4 Les dispositions du Règlement relatives au prestataire de services de paiement du bénéficiaire et l'approche par les risques

Conformément à l'approche par les risques, les PSP classent selon leur propre analyse et critères d'évaluation, leurs activités selon le niveau de risque qu'elles présentent (L.561-32 et R.561-38 du CMF et art. 11-7 du règlement n° 97-02).

Les PSP doivent prendre en compte dans leur analyse et leur classification des risques, le risque lié à la surveillance spécifique des virements internationaux notamment au regard du respect des exigences relatives aux éléments d'information sur le donneur d'ordre dans les conditions d'application du Règlement, afin de déceler d'éventuelles anomalies dans leurs opérations et mettre en œuvre notamment les dispositions des articles 9 et 10 du Règlement.

En outre, ils doivent notamment prendre en compte dans leur classification des risques et la mise en œuvre de leurs vigilances, notamment les facteurs d'alerte suivants concernant le PSP intervenant dans l'exécution d'un virement international :

- relation avec un PSP situé dans un pays non membre de l'UE ou qui n'est pas Partie à l'accord sur l'EEE ou dans un pays tiers qui n'impose pas des obligations équivalentes en matière de LCB-FT ;
- relation avec un PSP ayant déjà fait l'objet d'une déclaration en application de l'article 9.2 du Règlement.

## 3. La mise en œuvre de l'obligation de déclaration à l'ACP en cas de réception de virements d'un même prestataire de services de paiement avec omission régulière des informations sur le donneur d'ordre

L'article 9.2 du Règlement impose une obligation de déclaration d'un prestataire de services de paiement qui omet régulièrement de fournir les informations requises sur le donneur d'ordre.

### 3.1 Les conditions de mise en œuvre de l'obligation de déclaration prévue à l'article 9-2 du Règlement

Ainsi que le rappelle le considérant 18 du Règlement, le prestataire de services de paiement du bénéficiaire devrait faire preuve d'une vigilance particulière, en fonction du risque, lorsqu'il constate que les informations sur le donneur d'ordre sont manquantes ou incomplètes. À ce titre, le PSP du bénéficiaire doit, selon une approche par les risques, mettre en œuvre l'obligation de déclaration posée dans son principe à l'article 9.2 du Règlement.

En effet, le dispositif prévu par l'article 9.2 du Règlement ne prévoit pas qu'il y ait de déclaration systématique d'un PSP qui omet régulièrement de fournir les informations requises sur le donneur d'ordre, mais la mise en œuvre de mesures graduées prévues au premier alinéa de l'article précité.

Dans une première étape, l'obligation de déclaration est conditionnée à la mise en œuvre de mesures graduées ; l'article 9.2 fait mention à titre non exhaustif des mesures qui peuvent être prises : « 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… ». Le PSP du bénéficiaire doit ainsi définir une politique de mesures de relance qu'il met en œuvre en fonction de son appréciation des risques encourus en regard du PSP défaillant.

Dans une deuxième étape, en fonction de l'issue des mesures de relance précitées, le prestataire de services de paiement du bénéficiaire décide, soit de rejeter tout nouveau virement de fonds provenant du PSP en cause, soit, le cas échéant, de restreindre voire éventuellement de rompre la relation commerciale avec ce PSP. La mise en œuvre éventuelle de ces mesures relève de la libre appréciation et de la responsabilité du PSP du bénéficiaire en cohérence avec sa classification des risques.

Enfin, il revient au prestataire de services de paiement du bénéficiaire de définir des critères pertinents et concrets, qui lui permettront de déterminer les situations et seuils significatifs en termes d'évaluation et de gestion des risques LCB-FT applicables au PSP qui omet régulièrement de fournir les informations requises sur le donneur d'ordre.

À cet égard, l'Interprétation commune de l'AMLTF (cf. annexe 2) précise que le prestataire de services de paiement doit déterminer les critères de mise en œuvre de cette obligation, et notamment le critère de fréquence des omissions permettant d'établir si le PSP du donneur a régulièrement omis de fournir les informations requises sur le donneur d'ordre [16]. Des exemples de critères, de seuils notamment, sont exposés dans ce document à titre indicatif afin d'encadrer la mise en œuvre de l'obligation de déclaration [17]. Il pourra être tenu compte, par exemple, d'un critère de risque pays en fonction de la situation géographique d'établissement de ce PSP.

Les prestataires de services de paiement doivent être particulièrement vigilants avec les PSP dont le siège est dans un État ou territoire dont les déficiences importantes du dispositif LCB/FT ont été constatées, voire appellent à des contre-mesures, et rendues publiques par le GAFI, par une autre instance internationale intervenant en matière de LCB/FT ou par le Ministre chargé de l'économie [18] en cohérence avec leur classification des risques. Il est attendu des prestataires de services de paiement du bénéficiaire qu'ils prennent en considération ces éléments dans leur système d'évaluation et de gestion des risques conformément à l'approche par les risques (point 3 de l'article 11-7 du règlement n° 97-02 précité).

Sur la base des déclarations des prestataires de services de paiement, l'ACP pourra porter à l'attention de superviseurs étrangers les informations concernant les PSP régulièrement défaillants afin qu'il soit mis un terme à ces comportements.

## 3.2 Les modalités pratiques de déclaration relevant de l'article 9.2 du Règlement

Au terme de son analyse, et des diverses relances effectuées auprès du prestataire de services de paiement défaillant, dans le cadre de l'approche par les risques, le PSP du bénéficiaire procède à une transmission d'information au SGACP en vue de déclarer un PSP qui omet régulièrement de fournir les informations requises.

Un modèle de formulaire de déclaration est joint en annexe 1 des présents principes d'application sectoriels.

La transmission de la déclaration sera mise en œuvre selon une périodicité semestrielle.

Il ne sera pas transmis au SGACP de document de déclaration quand celui-ci est à néant, ou qu'il ne répond pas aux critères pertinents et concrets de déclaration au regard de l'évaluation et de la gestion des risques de LCB-FT développées par le prestataire de services de paiement du bénéficiaire.

Aux fins d'assurer une mise en œuvre efficace de l'article 10 du Règlement, quant à l'appréciation du caractère suspect de l'omission totale ou partielle ou de la non-pertinence des informations concernant le donneur d'ordre de virement, y compris au regard de situations relevant de l'article 9.2 du Règlement dans lesquelles le PSP du donneur d'ordre omet régulièrement de fournir les informations complètes sur le donneur d'ordre, il paraît souhaitable que les déclarants et correspondants (mentionnés aux articles R561-23 et R561-24 du *Code monétaire et financier*) soient informés des déclarations effectuées. Cela leur permet, d'une part, de disposer d'éléments d'informations nécessaires à l'exercice de leurs fonctions en application de l'article 11-7 du

16 Interprétation commune, p. 12, § 43.

17 Interprétation commune, § 43 et suivants.

18 Cf. les courriers du Ministre chargée de l'économie adressés aux organisations professionnelles en date du 24 mars 2010 relatifs aux listes du GAFI du 18 février 2010.

règlement n° 97-02, et, d'autre part, de procéder, le cas échéant, à une déclaration de soupçon en application de l'article L.561-15 du *Code monétaire et financier*.

## 4. Les paiements de couverture

### 4.1 Les recommandations du Comité de Bâle de mai 2009 applicables au prestataire de services de paiement du donneur d'ordre

Le PSP du donneur d'ordre dispose de procédures internes permettant d'assurer que sont adressées dans le message de paiement de couverture accompagnant le virement de fonds, quand le format de message utilisé est le MT 202 COV, les informations concernant le donneur d'ordre et le bénéficiaire du virement aux PSP intermédiaires de couverture.

### 4.2 Les recommandations applicables aux prestataires de services de paiement intermédiaires de couverture

Quand un ou plusieurs prestataires de services de paiement intermédiaires interviennent dans un paiement de couverture, et que l'information sur le donneur et le bénéficiaire du virement est mise à la disposition du PSP intermédiaire, notamment en cas d'utilisation d'un format de message SWIFT MT 202 COV, ils doivent mettre en œuvre des procédures de détection des éléments d'information manquants, afin, en particulier, d'effectuer les vérifications nécessaires au respect des obligations en matière de gel des avoirs (cf. notamment § 26 des recommandations du Comité de Bâle) et l'évaluation des risques associés aux relations de correspondance bancaire.

L'ACP s'assurera que les prestataires de services de paiement ne recourent pas à des formats de message qui ne contiennent pas toute l'information requise sur le donneur d'ordre et qu'ils utilisent de manière adaptée le format de message qui répond aux exigences de transparence, en l'occurrence le MT 202 COV.

## 5. Cas pratiques de mise en œuvre des textes relatifs aux virements de fonds

L'annexe 4 décrit cinq cas de mise en œuvre pratique par les PSP en matière de virements de fonds, élaborés par les professionnels. Ces cas recouvrent les différentes situations dans lesquelles un (ou plusieurs) PSP UE, notamment français, sont partie prenante : virements en provenance d'un PSP hors UE en euro, à destination d'un PSP hors UE en euro, entre deux PSP UE en euro, entre deux PSP hors UE en euro et entre deux PSP UE en devise. Ils illustrent notamment la problématique de gel des avoirs.

Il est rappelé à cet égard que, conformément aux dispositions relatives au gel des avoirs (articles L562-1 et suivants, article 11-7 du règlement CRBF n° 97-02 relatif au contrôle interne), les prestataires de services de paiement se dotent de dispositifs permettant de détecter toute opération au bénéfice d'une personne ou d'une entité faisant l'objet d'une mesure de gel des fonds, instruments financiers et ressources économiques.

Cette obligation ne s'applique pas en cas de transfert en provenance :

- d'un État membre de l'Union européenne ou d'un État partie à l'accord sur l'Espace économique européen si les PSP n'ont pas connaissance de l'identité du donneur d'ordre en application de l'article 6 du Règlement (dans ce cas le virement est accompagné du numéro de compte du donneur d'ordre ou d'un identifiant unique) ;
- d'un État ou territoire associé au titre de l'article 17 du règlement 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 (disposition qui rend applicable l'usage de l'identifiant unique ou numéro de compte) ; en pratique, il s'agit de la Principauté de Monaco (cf. point 2-1) ;

- de Saint-Pierre-et-Miquelon, de Mayotte, de la Nouvelle-Calédonie, de la Polynésie française et des îles Wallis et Futuna si les entreprises assujetties n'ont pas connaissance de l'identité du donneur d'ordre en application de l'article L.713-5 du *Code monétaire et financier* (de même, il s'agit du droit d'utiliser un identifiant unique ou le numéro de compte. Voir aussi le point 2.1).

# 6. Les modalités de contrôle de la mise en œuvre du Règlement

## 6.1 Compétence de l'ACP pour assurer l'application du Règlement

Le Règlement fait référence dans plusieurs dispositions (articles 9.2, 14 et 15) aux missions et compétences des « autorités responsables » ou des « autorités compétentes » en matière de lutte contre le blanchiment des capitaux et le financement du terrorisme, tant en matière de contrôle et de sanction que de transmission des informations.

### 6.1.1 En matière de contrôle

Les modalités de mise en œuvre des obligations définies par le Règlement seront examinées avec attention tant dans le cadre du contrôle sur pièces que du contrôle sur place définis à l'article L.612-23 du CMF.

Le contrôle sur pièces s'effectue en particulier dans le cadre de la remise des tableaux blanchiment, définis par les instructions n° 2000-09 pour les établissements de crédit et n° 2010-08 pour les établissements de paiement relatives aux informations sur le dispositif de prévention du blanchiment de capitaux et du financement des activités terroristes. Les instructions comportent en annexe les tableaux blanchiment (B1 à B7) qui déclinent en questions les textes législatifs et règlementaires applicables ainsi que les recommandations internationales pertinentes en matière LCB-FT. Le tableau B4 regroupe les questions relatives aux procédures internes qui comprennent les questions relatives aux obligations de vigilance en matière de virements de fonds.

### 6.1.2 En matière de sanction

En application de l'article L.612-39 du *Code monétaire et financier*, la commission des sanctions de l'ACP pourrait prononcer une ou plusieurs sanctions disciplinaires dans les conditions définies à l'article L.612-38 du CMF.

## 6.2 Transmission des informations

D'une manière générale, en application de l'article 14 du Règlement, tout prestataire de services de paiement a l'obligation de répondre, de manière exhaustive et sans délai, aux demandes adressées par l'ACP concernant les informations relatives au donneur d'ordre accompagnant les virements et les informations conservées correspondantes, dans le respect de l'article L.612-24 du CMF.

Cette obligation de transmission des informations en application de l'article 14 du Règlement s'exerce également à destination de TRACFIN dans les conditions de l'article L.561-26 I du CMF.

Annexe 1 Modèle de formulaire de déclaration prévue à l'article 9.2 du Règlement 1781/2006/CE.

Annexe 2 Interprétation commune élaborée par l'AMLTF relative aux obligations imposées aux prestataires de services de paiement des bénéficiaires par le règlement (CE) n° 1781/2006.

Annexe 3 Les recommandations du Comité de Bâle relatives aux obligations de vigilance et de transparence en matière de messages des paiements de couverture dans le cadre de virements internationaux.

Annexe 4 Cas pratiques de mise en œuvre des obligations des prestataires de services de paiement en matière de virements de fonds et de paiements de couverture.

Annexe 1

## Modèle de formulaire de déclaration prévue à l'article 9.2 du Règlement 1781/2006/CE

Déclaration relative aux virements de fonds reçus d'un prestataire de services de paiement pour lesquels les informations sur le donneur d'ordre sont régulièrement manquantes ou incomplètes conformément à l'article 9 § 2 du Règlement (CE) n° 1781/2006 relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds.

### Nom du prestataire de services de paiement déclarant :

| Code BIC (ou IBAN) du PSP du donneur d'ordre (PSP A) | Pays du PSP A | Nombre de virements de fonds reçus du PSP A pour lesquels des informations sont manquantes ou incomplètes | Pourcentage de virements de fonds pour lesquels des informations sont manquantes ou incomplètes par rapport au nombre total de virements reçus du PSP A et observations complémentaires éventuelles |
|---|---|---|---|
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

Cette déclaration doit être adressée au Secrétariat général de l'Autorité de contrôle prudentiel à l'adresse suivante : 2783-sdlabci-ut@acp.banque-france.fr.

Annexe 2

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

# Interprétation commune des obligations imposées par le règlement (CE) n° 1781/2006 relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds aux prestataires de services de paiement des bénéficiaires

## Contexte

1. Le règlement (CE) n° 1781/2006 relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds aux prestataires de services de paiement des bénéficiaires, qui est entré en vigueur le 1er janvier 2007, vise à mettre en œuvre au sein de l'Union européenne (UE) la recommandation spéciale VII du Groupe d'action financière internationale (GAFI). Ce règlement prévoit que les prestataires de services de paiement (comme les banques et les services de transfert de fonds électroniques) doivent veiller à ce que les virements de fonds qu'ils effectuent par des moyens électroniques sont accompagnés des informations complètes sur le donneur d'ordre. Ils doivent également vérifier les informations accompagnant les virements reçus. L'objectif de ce règlement est de faciliter, pour les autorités, la traçabilité des virements de fonds lorsque cela est jugé nécessaire.

2. Ce règlement complète un ensemble plus large de réglementations européenne et nationale visant à lutter contre le blanchiment de capitaux et le financement du terrorisme en imposant, par exemple, aux institutions financières de respecter les sanctions décrétées par les Nations Unies, l'UE et les différents pays, de respecter le devoir de vigilance relatif à l'identification de leurs clients lors des ouvertures de comptes, d'opérer un suivi permanent du comportement de la clientèle, et de procéder à une déclaration aux autorités lorsqu'elles soupçonnent la possibilité d'une activité criminelle ou terroriste.

3. Le groupe de travail pour la lutte contre le blanchiment de capitaux (*Anti Money Laundering Task Force*, AMLTF) reconnaît l'importance de ce règlement au sein de cet ensemble plus vaste. Par exemple, lorsqu'une banque vérifie les informations accompagnant les virements reçus, elle peut constater que les informations concernant le donneur d'ordre sont manquantes ou incomplètes : cela peut constituer un des éléments contribuant à la décision d'effectuer une déclaration de soupçon auprès des autorités.

4. L'attention de l'AMLTF a été attirée sur le fait que les prestataires de services de paiement des bénéficiaires rencontrent des difficultés de mise en œuvre de ce règlement en ce qui concerne les informations sur le donneur d'ordre accompagnant les virements de fonds. En outre, le Comité sur la prévention du blanchiment de capitaux et du financement du terrorisme, présidé par la Commission européenne et comprenant des représentants de tous les États membres, a demandé à l'AMLTF de travailler sur ce sujet, en collaboration avec le secteur privé. La Commission européenne travaille également en coopération avec les organismes compétents, eux aussi, en matière de paiement. L'AMLTF a également analysé l'éventualité d'un conflit entre ce règlement et l'obligation de geler les fonds au titre d'autres dispositions.

4. Le présent document [1] vise à refléter une interprétation commune pour le traitement des paiements dépourvus des informations exigées par ce règlement : ce consensus a été élaboré par l'AMLTF, grâce à une consultation informelle du secteur privé, notamment une réunion de travail qui s'est déroulée en

[1] Le document original en langue anglaise est accessible sur le site du Comité européen des contrôleurs bancaires. Dans un souci de fidélité vis-à-vis de cette publication, les numéros de paragraphes ont été conservés.

janvier 2008, et a été soumis à une consultation publique de trois mois lancée en avril 2008, comprenant une audition publique en date du 6 mai 2008.

5. Cette interprétation commune, qui se fonde sur le fonctionnement actuel des systèmes de paiement, de messagerie et de règlement, a pour objectif d'assurer une égalité de traitement entre les prestataires européens de services de paiement et de garantir la traçabilité [2] des virements. Ce document prend en compte le niveau actuel de conformité avec la recommandation spéciale VII du GAFI en dehors de l'UE et le fait que l'activité de virements de fonds est une activité de gros volumes. Une annexe décrit certaines pratiques existantes, identifiées en liaison avec le secteur privé. Cette annexe passe en revue certaines mesures actuellement utilisées par les prestataires de services de paiement.

6. L'AMLTF a été mis en place au second semestre 2006 par le Comité européen des contrôleurs bancaires, le Comité européen des superviseurs de marché et le Comité européen des superviseurs des assurances (les trois comités de niveau 3), en vue de fournir une contribution des autorités de surveillance aux questions de lutte contre le blanchiment des capitaux et le financement du terrorisme, en mettant notamment l'accent sur la troisième directive relative à la prévention du blanchiment de capitaux. L'AMLTF est composé d'autorités compétentes, venant de toute l'Europe et exerçant des responsabilités de surveillance à l'égard des prestataires de services de paiement.

7. L'AMLTF reconnaît qu'il existe d'autres autorités compétentes ayant ces responsabilités, qui ne sont pas représentées dans son comité. L'AMLTF suggère que ce document représenterait néanmoins une ressource utile pour ces autorités.

## 1. Introduction

1. Ce document a pour objet de refléter l'interprétation commune des autorités de surveillance européennes en ce qui concerne l'application du chapitre III du règlement (CE) n° 1781/2006 relatif aux informations concernant le donneur d'ordre accompagnant les virements de fonds aux prestataires de services de paiement des bénéficiaires (ci-après dénommé le « règlement »).

2. Cette interprétation commune, qui se fonde sur le fonctionnement actuel des systèmes de paiement, de messagerie et de règlement, a pour objectif d'assurer une égalité de traitement entre les prestataires européens de services de paiement (ci-après dénommés les PSP). Elle prend en compte le niveau actuel de conformité avec la recommandation spéciale VII en dehors de l'UE et le fait que l'activité de virements de fonds est une activité de gros volumes.

3. Cette interprétation commune ne doit pas être considérée comme une extension de ce règlement qui ajouterait des obligations, mais plutôt comme un éclaircissement des exigences contenues dans ce règlement, permettant de fournir aux PSP une interprétation commune des attentes des autorités de surveillance quant au respect de ce règlement.

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

4. Les PSP devront disposer de procédures efficaces afin de détecter si, dans le système de messagerie, de paiement ou 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. Il est attendu que les PSP remplissent cette obligation en mettant en œuvre les deux mesures suivantes.

5. En premier lieu, comme le prévoit le règlement, le prestataire du bénéficiaire doit détecter si, dans le système de messagerie, de paiement ou de règlement utilisé pour effectuer un virement de fonds, les

[2] Considérant 6 du règlement (CE) n° 1781/2006 : La traçabilité complète des virements de fonds peut être un instrument particulièrement précieux et utile en matière de prévention, d'enquête et de détection des activités de blanchiment de capitaux ou de financement du terrorisme. Il convient donc, afin d'assurer une bonne transmission des renseignements sur le donneur d'ordre tout au long de la chaîne des paiements, de prévoir un système qui impose aux prestataires de services de paiement l'obligation de veiller à ce que les virements de fonds soient accompagnés d'informations exactes et utiles sur le donneur d'ordre.

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.

6. Cette première mesure découlera en général de la simple application des règles de validation de ce système, si celles-ci empêchent l'envoi ou la réception de 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 PSP sont en outre incités, en se fondant sur leur expérience, à utiliser des filtres permettant de détecter les informations à l'évidence non pertinentes, comme des informations 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 pertinentes 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 cette première mesure au moment de la réception du virement.

9. En deuxième lieu, à moins que le prestataire n'ait détecté le caractère incomplet de tous les virements à réception de ceux-ci, il devrait, en plus du respect de l'article 8.1, soumettre les flux de paiements 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 PSP 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.

## 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 PSP 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 des articles 9-1 et 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 (CE) n° 2580/2001 et (CE) n° 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 devrait 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 PSP 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 PSP doivent s'attacher à appliquer une combinaison du point 3.1.3 avec le 3.1.4 et/ou le 3.1.2. Sans préjudice de toute autre législation ou de toute autre règlementation éventuellement applicable, le prestataire de services de paiement ne devrait pas exécuter systématiquement tous les virements incomplets ou assortis d'informations non pertinentes.

15. Les PSP 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 et/ou d'un rejet. Les PSP définiront ces processus et procédures internes en tenant compte de toutes les obligations applicables. Ils devront en particulier atténuer le risque de conformité en cas de blocage des fonds ou de rejet du virement. En outre, les PSP respecteront notamment les règlements (CE) n° 2580/2001 et (CE) n° 881/2002 ainsi que toute autre liste qu'il leur est fait obligation d'appliquer dans 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 tiers équivalent, cela peut être pris en compte dans l'appréciation du risque. Les PSP 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 devrait 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 virement et l'envoi de la demande d'informations complètes ou pertinentes devrait être fixé, par exemple 7 jours ouvrés.

24. Après avoir envoyé sa demande d'informations complètes ou pertinentes, le prestataire de services de paiement devrait 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 concernant le virement en question, effectuer un suivi de cette demande.

***L'appréciation du caractère suspect***

25. Comme mentionné au 3.1.2, les PSP 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 risque induit par le caractère incomplet ou non pertinent des informations peut donner lieu ou non à une transmission interne 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 PSP 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 devrait être à même de démontrer à son autorité de contrôle 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 devrait 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 devrait 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 PSP qui n'ont pas répondu.

29. Le rappel devrait 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 en interne pour risques élevés (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 en demandant des informations complètes, ainsi que prévu par 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 (CE) n° 2580/2001 et (CE) n° 881/2002), avec obligation de s'abstenir d'effectuer les transactions déclarées suspectes (article 24(1) de la directive n° 2005/60/CE) et exigence des autorités compétentes de différer ces transactions (article 24(1) de la directive n°2005/60/CE). En outre, les PSP devront en particulier atténuer 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 particulièrement appropriée lorsqu'il est nécessaire d'éclaircir la situation au sein de l'établissement, en échangeant avec d'autres établissements du groupe, en utilisant des bases de données ou en contactant des cellules de renseignement financier afin de confirmer ou de rejeter le soupçon de blanchiment de capitaux.

32. Lorsque le prestataire de services de paiement choisit de bloquer les fonds, il devrait 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 devrait adresser une demande d'informations complètes ou pertinentes au prestataire du donneur d'ordre. Ces procédures et processus devraient cependant garantir que le prestataire adresse, dans au mieux 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. L'attention est attirée sur le fait que même si le délai maximal autorisé est identique à celui de la section 3.1.3, c'est au prestataire du bénéficiaire qu'il appartient de définir les critères déterminant à quelle fréquence il envoie la demande d'informations. Dans la présente section, ces critères définis en interne devraient 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 devrait 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, devrait être fixé. Cependant, les PSP 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 devrait 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 devrait 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 PSP ayant manqué à cette obligation. En outre, le prestataire de services de paiement devrait être à même de démontrer à son autorité de contrôle 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 devrait 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 devrait fixer un délai au prestataire émetteur, par exemple encore une fois trois jours ouvrables. 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 en interne pour risques élevés (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.

39. De plus, le rappel devrait indiquer que l'exécution du virement concerné est suspendue. 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 devrait 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, se 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 PSP doivent prendre des dispositions à l'encontre des PSP 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 PSP 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 répondre en temps voulu aux demandes. En outre, le degré d'omission peut varier en fonction de 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 les informations requises. 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, par exemple, peuvent être utilisés :

    a. le degré de coopération du prestataire de services de paiement du donneur d'ordre s'agissant des demandes d'informations complètes ou pertinentes envoyées ;

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

    c. un seuil défini en pourcentage des 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 pertinentes ;

## 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 devrait 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 devraient recevoir ces informations. Ces « autorités » sont encouragées à échanger les informations avec les autorités nationales de supervision.

46. La transmission de ces informations devrait 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 du donneur d'ordre 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 PSP semble avoir ainsi été améliorée.

### 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 prévoit 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 PSP 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 régulièrement les informations est également une banque correspondante d'un pays tiers, la décision prise conformément à la présente section et l'application de mesures de vigilance renforcées 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 de banque correspondante avec cet établissement.

## 5. Collecte et déclaration des données en interne

51. Les PSP devraient 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 devraient 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 1 000 dollars américains ou de 1 000 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 d'interprétation de la RS VII. Cela n'empêche pas les PSP 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.

## 7. Réexamen de l'interprétation commune

54. Considérant que l'interprétation commune tient compte du niveau actuel de conformité à la RS VII à l'échelle internationale et du fonctionnement actuel des systèmes de paiement, de règlement et de support, elle devrait faire l'objet de révisions en fonction du niveau de conformité atteint par le secteur vis-à-vis de la réglementation et, ce pas plus tard que le réexamen du règlement (CE) n° 1781/2006.

Annexe 1 au document publié le 16/10/2008
CEBS 2008 156/ CEIOPS-3L3-12-08/ CESR/08-773

## Pratiques en vigueur du secteur

La présente annexe décrit certaines pratiques en vigueur, identifiées grâce à nos relations avec le secteur des services financiers. Elle passe en revue certaines mesures actuellement mises en œuvre par les PSP.

- La **banque N** est une grande banque établie dans un État membre de l'UE. Elle traite quotidiennement des dizaines de milliers de virements électroniques. Elle émet et reçoit des paiements entre États membres de l'UE, et pays n'appartenant pas à l'UE, au moyen du système de messages SWIFT. Le système SWIFT interdit le traitement des messages dont certains champs ne sont pas renseignés. Cependant, des données non pertinentes peuvent tout de même être attachées aux paiements : les systèmes de messagerie SWIFT ne peuvent l'empêcher. Aussi, la banque N procède-t-elle à un échantillonnage *a posteriori* des flux de paiements entrants pour identifier les cas où les données peuvent se révéler incomplètes ou non pertinentes. L'échantillonnage se concentre sur certains domaines réputés présenter un risque plus élevé. Au nombre des paiements identifiés à haut risque par la banque N, on trouve par exemple : a) ceux émis par des PSP situés hors de l'UE, notamment ceux dont la juridiction a été identifiée par la banque comme présentant un risque élevé, b) ceux émis par des PSP qui ont été précédemment dans l'incapacité de faire face à leurs obligations et c) les paiements qui sont perçus par le bénéficiaire en espèces sur la base d'un paiement sur demande avec identification (*pay on application and identification basis*).

- La **banque P** est une petite banque privée, établie dans une capitale européenne, qui travaille essentiellement pour des clients appartenant à certains pays hors UE. Elle reçoit très peu de paiements électroniques pour le compte de ses clients. Lorsque ces paiements sont reçus, il n'est pas inhabituel qu'ils aient été émis hors de l'UE, ni qu'ils représentent des montants importants. La banque P est à même de soumettre chacun des paiements à un examen minutieux par un de ses employés. La connaissance qu'a le personnel des pays concernés lui permet par exemple de détecter rapidement que l'adresse du donneur d'ordre ne correspond pas à ce qu'on devrait attendre.

- La **banque Q** est une banque de taille moyenne établie dans un État de l'UE. La banque Q cherche à identifier les données incorrectes en réalisant des vérifications par échantillonnage *a posteriori*. Ainsi, le paiement a-t-il déjà été effectué au moment où la banque Q constate que les informations sont incorrectes. Abstraction faite des aspects pratiques, la banque Q n'est pas certaine qu'il soit souhaitable de rejeter une opération en cours : cela pourrait susciter des contestations juridiques pour rupture de contrat, et faire courir un risque de poursuites judiciaires en vertu des législations nationales qui proscrivent la l'avertissement des criminels. Les mesures suivantes prises par la banque consistent à rechercher des informations complètes concernant le donneur d'ordre. Il s'agit également de déterminer si l'opération présente un caractère suspect, bien qu'il soit difficile de fonder des soupçons sur ces seules informations. La banque Q enregistre les omissions de fourniture d'informations de la part des PSP, et détermine quelles institutions sont insuffisamment fiables ou coopératives pour justifier de nouvelles actions. La banque Q n'a pas exclu de mettre fin à sa relation commerciale avec certains PSP situés hors de l'UE.

- Pour les intermédiaires, beaucoup pensent que le prestataire de services de paiement bénéficiaire devrait adresser une demande relative aux informations manquantes directement au prestataire du donneur d'ordre. Il ne devrait pas être nécessaire de faire intervenir les PSP intermédiaires, hormis lorsque leur aide est nécessaire pour fournir un identifiant d'opération du prestataire donneur d'ordre permettant de suivre la trace du paiement.

- Certaines banques considèrent qu'il suffit de disposer des informations du champ 20 du message standard SWIFT et que cela permet de remplir l'obligation d'identifiant unique, conformément au règlement. Toutefois, dans les paiements hors UE, des informations relatives au compte bancaire doivent figurer dans le champ 50 du message standard SWIFT.

Annexe 3

Comité de Bâle sur le contrôle bancaire
Mai 2009

# Vigilance et transparence pour les messages de paiements de couverture dans le cadre des virements transfrontaliers

Sommaire



1. Le traitement des virements électroniques transfrontaliers [1] passe souvent par plusieurs institutions financières. Outre la banque du donneur d'ordre et celle du bénéficiaire, il n'est en effet pas rare que des banques supplémentaires interviennent également. Ce document examine les cas dans lesquels une ou plusieurs de ces banques intermédiaires de couverture [2] sont situées dans une juridiction autre que celle de la banque du donneur d'ordre et de la banque du bénéficiaire. Il décrit les attentes des autorités de contrôle dans le cadre des initiatives actuelles soutenues par le Comité de Bâle afin d'améliorer la transparence dans les messages de paiement, et qui portent sur les informations à inclure dans les messages accompagnant les paiements de couverture, les divers mécanismes à utiliser pour qu'une information exacte et complète soit incluse dans ces messages, les différents rôles des parties prenantes à ces mécanismes et l'usage qui doit être fait de l'information aux fins de la lutte contre le blanchiment d'argent et le financement des milieux terroristes (LAB/CFT).

2. Les banques utilisent les paiements de couverture pour faciliter les transferts de fonds pour le compte d'un client et à destination d'un bénéficiaire, qui se trouve le plus souvent dans un autre pays, mais qui peut aussi être situé dans le même pays si le paiement s'effectue dans une devise étrangère. Ces

[1] La Note interprétative à la Recommandation Spéciale VII du GAFI définit un virement électronique comme « toute transaction par voie électronique effectuée au nom d'un donneur d'ordre (qu'il s'agisse d'une personne physique ou morale) via une institution financière en vue de mettre à disposition d'un bénéficiaire une certaine somme d'argent dans une autre institution financière. Le donneur d'ordre et le bénéficiaire peuvent être une seule et même personne ». Pour le GAFI, un virement transfrontalier est un virement pour lequel l'institution financière du donneur d'ordre et celle du bénéficiaire sont situées dans des pays différents. Ce terme désigne également toute chaîne de virements électroniques qui comporte au moins un élément transfrontalier. Ainsi, un virement dans lequel le donneur d'ordre et le bénéficiaire se trouvent dans la même juridiction, mais qui fait intervenir un ou plusieurs correspondants situés dans un pays tiers, serait par conséquent considéré comme un virement transfrontalier.

[2] Nous utilisons ici le terme « banque intermédiaire dans les paiements de couverture » afin de marquer la différence entre une banque intermédiaire pour les paiements en série, lesquels ne sont pas traités dans le présent document, et une banque intermédiaire intervenant dans la chaîne des paiements de couverture.

paiements se caractérisent habituellement par (i) une transaction dans une monnaie autre que celle du pays dans lequel est domiciliée la banque du donneur d'ordre ou celle du bénéficiaire, et (ii) l'absence, entre la banque du donneur d'ordre et celle du bénéficiaire, d'une relation qui leur permettrait de procéder directement au règlement entre elles. Dans un tel cas, la banque du donneur d'ordre peut directement donner à celle du bénéficiaire l'instruction de procéder au paiement et l'informer que le transfert des fonds visant à « couvrir » l'obligation interbancaire créée par cet ordre de paiement passe par l'intermédiaire de couverture. C'est souvent le correspondant de la banque du donneur d'ordre dans le pays où la devise nationale est la devise du paiement qui se charge du règlement. Si le correspondant de la banque du donneur d'ordre a une relation avec la banque du bénéficiaire, il peut régler le paiement lui-même. Dans le cas contraire, le règlement passe en général par une autre banque intermédiaire, qui a une relation avec la banque du bénéficiaire. Dans la pratique courante, le bénéficiaire peut faire créditer son compte par sa propre banque avant que le règlement interbancaire ne soit effectué, surtout lorsqu'il existe une relation commerciale solide.

3. Ce mécanisme de paiement de couverture, dans lequel les banques intermédiaires ne voient pas forcément toutes les informations envoyées à la banque du bénéficiaire, diffère de la chaîne de paiement en série directe envisagée dans la Recommandation spéciale VII du GAFI sur les virements électroniques, dans laquelle l'information envoyée à la banque du bénéficiaire passe par les différents intermédiaires (voir graphique ci-après). Il est le plus souvent utilisé pour éviter les retards résultant des différences de fuseaux horaires entre la banque du donneur d'ordre et celle du bénéficiaire, et afin de réduire les coûts des transactions commerciales.

4. Les pratiques existantes n'assurent pas la pleine transparence des messages accompagnant les virements facilités par les banques intermédiaires de couverture. La transparence est limitée lorsque le format du message utilisé pour le règlement du paiement interbancaire (dans l'exemple ci-dessous, un SWIFT MT 202) ne contient pas d'informations relatives au donneur d'ordre et au bénéficiaire. Ces informations sont toutefois incluses dans le message envoyé à la banque du bénéficiaire (dans l'exemple ci-dessous, un SWIFT MT 103). Cette absence d'informations à propos du donneur d'ordre et du bénéficiaire dans les transferts de fonds peut entraver ou restreindre la capacité d'une banque intermédiaire de couverture à évaluer précisément les risques associés aux opérations de correspondant et de compensation. Par ailleurs, la banque intermédiaire de couverture n'est pas non plus en mesure de vérifier les informations relatives au donneur d'ordre en les comparant avec les listes de personnes physiques et morales dont les actifs doivent être bloqués, rejetés ou gelés aux termes de la législation locale. Cette impossibilité pourrait se révéler particulièrement problématique lorsque la liste établie dans le pays de la banque intermédiaire est plus complète que celle du pays du donneur d'ordre (ou du bénéficiaire). Il existe aussi un risque que ces formats de messages puissent être choisis dans le but de dissimuler le nom des parties à une transaction. Pour pouvoir se conformer aux dispositions locales, et par exemple bloquer, rejeter ou geler les actifs des personnes physiques et morales désignées, les banques intermédiaires de couverture ont donc besoin de recevoir des informations sur le donneur d'ordre et le bénéficiaire.

5. Des informations plus détaillées sur les donneurs d'ordre et les bénéficiaires des transferts de fonds peuvent améliorer la conformité aux dispositions locales (par exemple le blocage, le rejet ou le gel des actifs des personnes physiques et morales désignées et la surveillance des activités suspectes), ainsi que les processus de gestion des risques d'une banque dans le cadre des transferts de fonds. Une initiative lancée par le groupe de Wolfsberg et la Clearing House Association vise à renforcer la transparence par (i) l'adoption de certaines règles communes pour les messages des paiements dans le secteur bancaire (les « normes des messages ») et (ii) la création d'un format de message de paiement SWIFT amélioré pour les paiements de couverture des banques intermédiaires, format qui contiendra des informations sur le donneur d'ordre et le bénéficiaire [3]. Dans le sillage de cette initiative, la communauté des membres de SWIFT est en train d'élaborer une solution technique qui permettra de transmettre de manière standardisée des informations complètes sur le donneur d'ordre et le bénéficiaire avec les paiements de couverture. La mise en œuvre de cette solution est prévue pour novembre 2009. D'autres normes pourraient également être définies pour permettre une plus grande transparence dans les messages.

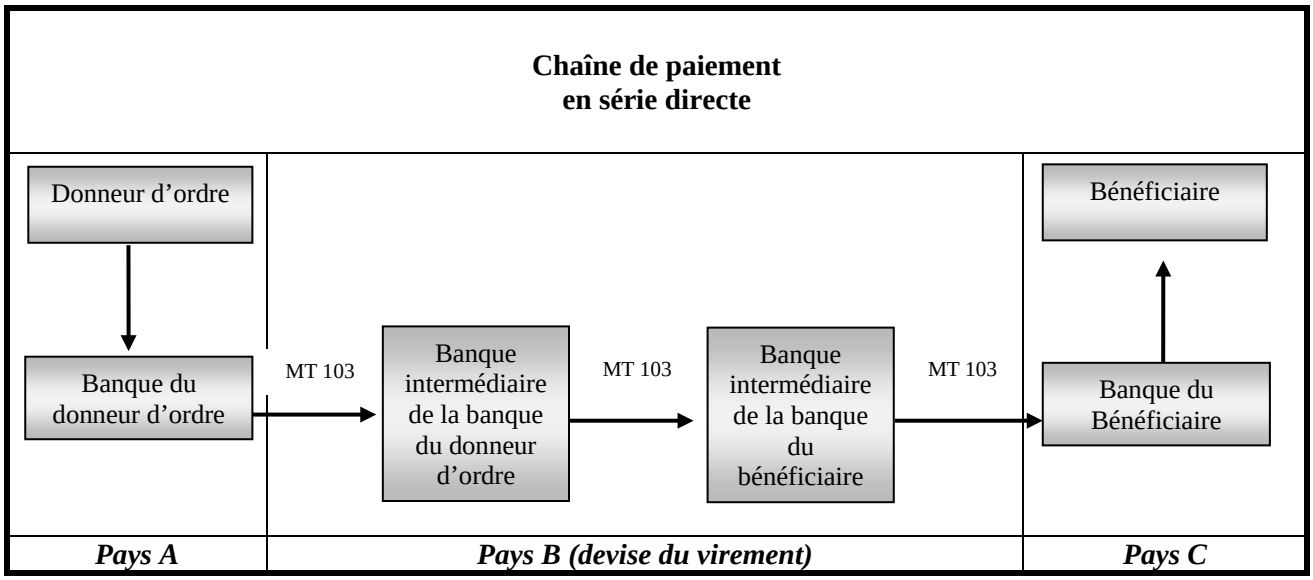
[3] Groupe de Wolfsberg, *Clearing House Statement on Payment Message Standards*

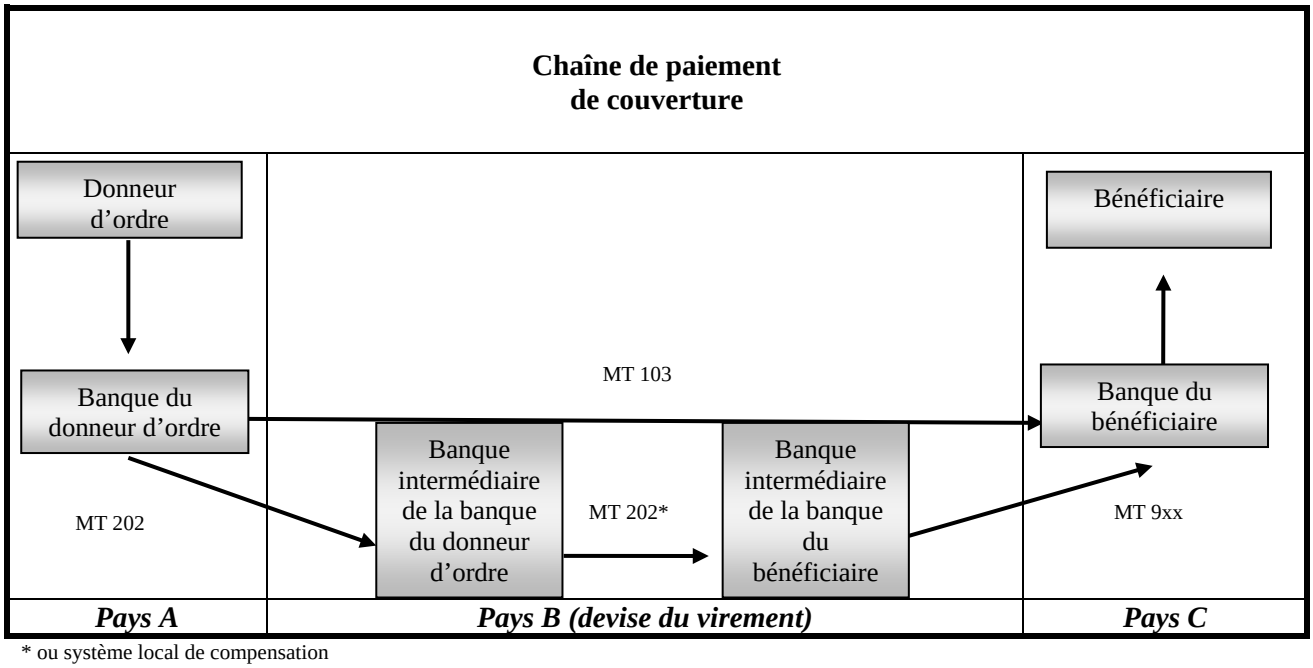
6. Dans son bulletin d'information d'octobre 2007 [4], le Comité de Bâle a encouragé cette évolution pour tous les formats de message pertinents. Il a également annoncé à cette occasion son intention d'étudier l'évolution des politiques de contrôle afin d'appuyer la mise en œuvre des efforts de transparence dans le secteur.

7. Le Comité appelle à une utilisation efficace et conforme des solutions techniques conçues pour renforcer la transparence. En fait, l'amélioration de la transparence dans les messages de paiements ne dépend pas uniquement des normes définies pour ces messages, mais aussi de la mise en œuvre de pratiques adéquates par les banques participant au traitement des virements, en vue du bon fonctionnement des systèmes de paiement. Le secteur travaille déjà à l'élaboration de bonnes pratiques [5]. Les autorités de contrôle ont un rôle à jouer dans la surveillance d'une mise en œuvre efficace et cohérente des règles renforçant la transparence des messages accompagnant les paiements dans le monde entier. Le présent document, qui fait suite aux travaux antérieurs du Comité de Bâle consacrés à l'harmonisation des méthodes de supervision du devoir de vigilance à l'égard de la clientèle (Customer Due Diligence, CDD) et de lutte contre le blanchiment d'argent et le financement des milieux terroristes (LCB/FT), décrit donc les attentes communes des autorités de contrôle concernant l'information qui devrait être jointe aux messages de paiements de couverture, ainsi que les rôles respectifs de la banque du donneur d'ordre, des banques intermédiaires de couverture et de la banque du bénéficiaire à propos de cette information. Il décrit également une conception commune de ce que devraient être les missions des autorités de contrôle concernant la transparence des messages des paiements de couverture dans le cadre des virements transfrontaliers.

[4] Bulletin d'information n °12 du Comité de Bâle, *Transparency in payments messages* (www.bis.org/publ/bcbs_nl12.htm)

[5] Par exemple, le groupe de Wolfsberg, *Clearing House Statement on Payment Message Standards* (cf. note de bas de page 3 ci-dessus) et Payments Market Practice Group, *Market Practice Guidelines for use of the MT 202 COV1 (Version 1.0, septembre 2008, http://pmpg.webexone.com/login.asp?loc=&link=).*




* ou système local de compensation

*Moment de la mise en œuvre*

8. La mise en œuvre de solutions techniques adaptées, telles que celles mentionnées ci-dessus, constitue le préalable à une plus grande transparence et au respect des attentes y afférentes des autorités de contrôle, telles que décrites dans le présent document. Il est attendu des banques qu'elles reprennent l'information décrite à la Section I et qu'elles agissent conformément à ce qui est décrit dans la Section II aussi rapidement que les moyens techniques le permettent.

*Champs d'application*

9. Le Comité de Bâle considère que ces principes directeurs valent pour toutes les autorités de contrôle dans le monde. Ils correspondent à l'application des normes, lois et réglementations existantes au cas spécifique des paiements de couverture. S'ils ne créent pas d'obligations nouvelles, puisque les obligations des banques sont définies par leur propre législation nationale transposant les normes internationales et nationales, ils expriment la conception commune des membres du Comité concernant le renforcement de la transparence pour les paiements de couverture internationaux, ainsi que les

attentes communes des autorités de contrôle relatives à ce surcroît de transparence au niveau international.

10. Ces principes directeurs sont destinés à traiter les problèmes pertinents pour la coopération internationale, et donc à s'appliquer aux banques intermédiaires de couverture situées dans une juridiction autre que celles dans lesquelles la banque du donneur et la banque du bénéficiaire sont situées. Par conséquent, ils n'ont pas vocation à s'appliquer aux autres banques intermédiaires dans le domaine des paiements. Par exemple, ils ne concerneraient pas des banques intermédiaires de couverture situées dans la même juridiction que celle de la banque du donneur d'ordre ou que celle de la banque du bénéficiaire [6]. Par ailleurs, ces principes directeurs ne s'appliqueraient qu'à la première banque intermédiaire de couverture située dans la même juridiction, et non aux suivantes. Les banques intermédiaires de couverture sortant du champ d'application des présents principes directeurs seront régies uniquement par leur législation nationale, qui transpose les normes internationales et nationales.

11. L'Union européenne (UE) et l'Espace économique européen (EEE) sont considérés ici comme formant une seule et même juridiction, conformément à la décision du GAFI de février 2008 [7]. Par conséquent, les présents principes directeurs ne s'appliquent à aucune chaîne de virements qui se déroule entièrement à l'intérieur des frontières de l'UE/EEE.

12. S'il existe un seuil minimum dans la juridiction du donneur d'ordre mais pas dans celle de la banque intermédiaire de couverture, il apparaît qu'une solution semblable à celle énoncée dans la Note interprétative à la Recommandation spéciale VII du GAFI [8] doive s'appliquer et que les pays puissent néanmoins demander à ce que les messages des paiements de couverture transfrontaliers entrants contiennent des informations complètes et exactes sur le donneur d'ordre et le bénéficiaire.

## I. Flux d'informations

13. Le GAFI définit dans des termes généraux l'information relative au donneur d'ordre qui doit accompagner les virements internationaux. Les normes du GAFI ne traitent pas directement des paiements de couverture et le présent document clarifie, entre autres, les attentes des autorités de contrôle concernant les informations qui doivent être communiquées aux banques intermédiaires qui traiteront des paiements de couverture après l'adoption des nouvelles normes sur les messages, qui introduisent une plus grande transparence. Ce document entend donc être en ligne avec la Recommandation du GAFI sur les virements électroniques ainsi qu'avec sa Note interprétative.

14. Dans sa Recommandation spéciale VII, le GAFI précise que « les pays devraient prendre des mesures afin d'obliger les institutions financières, y compris les services de remise de fonds, à inclure des renseignements exacts et utiles relatifs au donneur d'ordre (nom, adresse et numéro de compte [9]) concernant les transferts de fonds et l'envoi des messages qui s'y rapportent. Les renseignements devraient accompagner le transfert ou le message qui s'y rapporte tout au long de la chaîne de paiement ». La Note interprétative du GAFI spécifie aussi que les institutions financières agissant comme intermédiaires dans la chaîne des virements électroniques doivent s'assurer que toutes les informations relatives au donneur d'ordre qui accompagnent le virement électronique sont conservées avec le virement. Cette norme a pour but de « s'assurer que les informations essentielles relatives au donneur d'ordre du virement électronique sont rendues immédiatement disponibles [aux autorités

---

6 La référence à une juridiction unique concerne aussi les cas dans lesquels deux pays ou plus sont considérés comme une seule juridiction.

7 Cf. la note à l'intention des évaluateurs au niveau du critère VII.3, méthodologie du GAFI, p. 69, http://www.fatfgafi.org/dataoecd/16/54/40339628.pdf

8 http://www.fatf-gafi.org/document/53/0,3343,en_32250379_32236947_34261877_1_1_1_1,00.html#INSRVII, paragraphe 4b.

9 La Note interprétative du GAFI indique que « les informations accompagnant les virements électroniques transfrontaliers qualifiés comme tels doivent toujours inclure le nom du donneur d'ordre et, lorsqu'un compte existe, le numéro de ce compte. En l'absence d'un compte, un numéro de référence unique doit être inclus. Les informations accompagnant les virements électroniques qualifiés comme tels devraient aussi inclure l'adresse du donneur d'ordre. Cependant, les pays peuvent autoriser les institutions financières à remplacer l'adresse par un numéro d'identité national, par un numéro d'identification du client ou par la date et le lieu de naissance ». Les pays « peuvent fixer un seuil minimum (n'excédant pas 1000 EUR ou USD). Pour les virements transfrontaliers n'atteignant pas ce seuil : (i) les pays ne sont pas obligés d'exiger des institutions financières qu'elles identifient, vérifient et enregistrent ou transmettent des informations sur le donneur d'ordre. (ii) Les pays peuvent néanmoins exiger que les virements électroniques transfrontaliers entrants comportent des informations complètes et précises sur le donneur d'ordre ».

publiques et] aux institutions financières du bénéficiaire afin de faciliter la détection et la déclaration des opérations suspectes ».

15. Le Comité de Bâle considère que l'information sur les donneurs d'ordre et les bénéficiaires devrait être incluse dans tous les messages envoyés aux banques intermédiaires de couverture et qui traitent des virements transfrontaliers liés aux transactions de certains clients. Cette application permettra d'améliorer la transparence pour toutes les banques qui participent à l'opération et favorisera la pleine conformité à toutes les normes applicables. Comme noté dans l'introduction, elle suppose la mise en œuvre de normes techniques adéquates pour les messages de paiements de couverture.

## II. Rôle des banques traitant les virements transfrontaliers

16. Cette section a pour objectif d'exposer les attentes des autorités de contrôle concernant les rôles respectifs de la banque du donneur d'ordre, des banques intermédiaires de couverture et de la banque du bénéficiaire s'agissant du traitement d'un paiement de couverture transfrontalier dans le cadre d'un virement. La banque du donneur d'ordre devrait veiller à ce que des informations adéquates accompagnent le virement, tandis que les autres intervenants dans la chaîne de paiement doivent traiter le paiement sur la base de ces informations.

17. Le Comité de Bâle encourage toutes les banques à appliquer des normes instaurant un degré élevé de transparence, en pleine conformité avec toutes les lois et réglementations nationales applicables, dans le contexte des paiements de couverture engagés pour régler la transaction d'un client. En particulier :

- des informations adéquates devraient être incluses dans les messages de paiements conformément à ce qui est décrit dans le présent document. Les institutions financières ne devrait pas omettre, effacer ou modifier les informations contenues dans les messages de paiements dans le but d'éviter que ces informations ne soient détectées par toute autre institution financière participant à la chaîne de paiement ;
- les institutions financières ne devrait pas faire usage d'un message de paiement dans le but d'éviter que l'information puisse être détectée par toute autre institution financière participant au processus de paiement ;
- sous réserve de toute législation applicable, les institutions financières devraient coopérer aussi pleinement que possible avec les autres institutions financières participant à la chaîne de paiement lorsque cette coopération est nécessaire pour la communication d'informations sur les parties en présence ;
- dans leurs relations avec leurs correspondants, les institutions financières devraient tenir compte des pratiques de ces derniers en matière de transparence.

18. Concernant les flux d'informations, il relève de la responsabilité de la banque du donneur d'ordre de veiller à ce que des informations complètes soient incluses pour chaque virement. Cependant, la banque du bénéficiaire et les banques intermédiaires de couverture doivent, elles aussi, veiller à ce que les flux d'informations soient appropriés.

19. La surveillance des clients constitue un aspect essentiel pour des procédures de LCB/FT efficaces [10]. Cependant, une surveillance efficace aux fins de la LCB/FT suppose que les banques aient une bonne vision des activités normales et raisonnables qui se déroulent sur les comptes de leurs clients, de manière à pouvoir repérer les transactions atypiques. Cette nécessité influe sur les responsabilités en matière de surveillance, qui ne sont pas les mêmes pour les banques qui disposent d'informations directes sur leurs clients non bancaires et pour les banques intermédiaires de couverture, qui ne font que gérer une relation commerciale avec d'autres banques dans le but d'effectuer des paiements et qui ne sont donc pas censées être en mesure de surveiller les clients finaux (cf. *infra*, paragraphe 21).

[10] Comité de Bâle sur le contrôle bancaire, *Devoir de diligence des banques au sujet de la clientèle*, octobre 2001, paragraphe 53.

## A. Responsabilité de la banque du donneur d'ordre

20 Comme l'indique la Note interprétative du GAFI, l'institution financière du donneur d'ordre doit s'assurer que les informations relatives au donneur d'ordre contenues dans le virement électronique sont complètes [11]. L'institution financière du donneur d'ordre est responsable du devoir de vigilance à l'égard du donneur d'ordre. Elle doit vérifier l'exactitude de l'information et assurer la conformité de cette information à la réglementation locale qui transpose les normes du GAFI.

21. La banque du donneur d'ordre doit veiller à ce que les messages qu'elle envoie à la banque intermédiaire de couverture contiennent des informations sur le donneur d'ordre et sur le bénéficiaire. Les informations relatives au donneur d'ordre devraient être conformes à la règlementation locale transposant la Recommandation spéciale VII du GAFI ainsi que sa Note interprétative. Les informations relatives au bénéficiaire devraient au moins mentionner son nom et un numéro d'identification (tel qu'un Business Entity Identifier [12]), ainsi que les autres informations relatives au bénéficiaire envoyées directement à la banque de ce dernier, le cas échéant. Il convient d'encourager les banques à inclure, dans la mesure du possible, d'autres informations concernant le bénéficiaire, lorsque ces données supplémentaires sont nécessaires pour limiter le risque que les actifs des clients ne soient indûment gelés, bloqués ou rejetés ou que le paiement de couverture ne soit indûment retardé. Les informations relatives au bénéficiaire devront être obtenues auprès du donneur d'ordre. La politique de la banque du donneur d'ordre devrait couvrir les aspects suivants :

   – la conservation des données,

   – la vérification des informations sur le donneur d'ordre,

   – les formats des messages et les circonstances dans lesquelles ces formats devraient être utilisés,

   – les informations à inclure dans les messages.

22. Selon les standards SWIFT, l'inclusion dans le message du paiement de couverture (MT 202COV) des informations relatives au donneur d'ordre et au bénéficiaire contenues dans le MT 103 sera obligatoire. SWIFT rejettera les messages dont un champ obligatoire ne sera pas rempli.

23. Conformément aux normes du GAFI et au document intitulé *Devoir de diligence des banques au sujet de la clientèle* du Comité de Bâle, la banque du donneur d'ordre devrait inclure les virements internationaux dans ses mesures actuelles de vigilance mise en œuvre dans sa relation avec le donneur d'ordre et pour l'examen approfondi des transactions tout au long de cette relation, dans le but de vérifier que les transactions effectuées sont conformes à ce que l'institution connaît de son client, de son activité et de son profil de risque, et aussi, si nécessaire, de l'origine des fonds [13]. De nombreuses juridictions autoriseront les banques à recourir à une approche fondée sur l'évaluation du risque, qui devra être auditée régulièrement, ce qui permettra d'en évaluer l'efficacité.

## B Responsabilité des banques intermédiaires de couverture

24. Comme indiqué plus haut, aux termes de la Recommandation spéciale VII du GAFI, les banques intermédiaires qui interviennent dans des paiements en série ont pour responsabilité première de « s'assurer que toutes les informations relatives au donneur d'ordre qui accompagnent le virement électronique sont conservées avec le transfert ». De plus, la Recommandation 7 du GAFI portant sur les correspondants bancaires et les paragraphes 49 à 52 du document *Devoir de diligence des banques au sujet de la clientèle* établi par le Comité de Bâle définissent les mesures de vigilance que les intermédiaires devraient mettre en œuvre concernant les banques qui proposent des services de correspondant bancaire. Le présent document ne vise pas à changer ces principes, mais à mettre en

[11] Cf. note de bas de page 8.

[12] Il est possible d'utiliser un code d'identification (tel qu'un *Business Entity Identifier*) à la place d'un nom à condition que ce code permette à la banque intermédiaire de trouver facilement et en toute fiabilité le nom du bénéficiaire et de procéder à une vérification automatisée sur la base d'une liste de noms.

[13] " Le degré et la nature de la surveillance exercée par une institution financière dépendront de la taille de cette dernière, de son exposition au risque de LCB/FT, de la méthode de surveillance utilisée (manuelle, automatisée ou combinant les deux) et du type d'activité faisant l'objet de cette surveillance, GAFI, *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing*, juin 2007, paragraphe 3.12.

lumière les questions spécifiques liées aux paiements de couverture transfrontaliers effectués par l'intermédiaire de correspondants bancaires.

### *1. Surveillance destinée à éviter que des champs des messages ne soient laissés à blanc*

25. Comme indiqué plus haut, les messages de paiements de couverture dans lesquels les champs relatifs au donneur d'ordre et au bénéficiaire sont laissés en blanc seraient rejetés par le système SWIFT. Si les banques agissant en qualité d'intermédiaire recourent à d'autres systèmes ou procédures qui ne veillent pas à ce que les champs relatifs au donneur d'ordre et au bénéficiaire soient remplis, elles devraient :

    – disposer de politiques raisonnables leur permettant de s'assurer en temps réel que les champs relatifs au donneur d'ordre et au bénéficiaire dans les messages de paiements de couverture transfrontaliers ne sont pas laissés à blanc ;

    – si ces champs sont laissés à blanc, prendre des mesures appropriées, conformément à la législation nationale applicable. Ces mesures pourraient consister, par exemple, (i) à refuser de traiter la transaction concernée, (ii) à obtenir les informations manquantes auprès de la banque du donneur d'ordre ou de la banque intermédiaire précédente [14] et/ou (iii) à adresser une déclaration de soupçon aux autorités locales ;

    – motiver par écrit les décisions qu'elles ont prises.

### *2. Surveillance sur la base de listes de noms*

26. Contrairement aux intermédiaires dans les chaînes de paiements en série, qui disposent déjà de ces informations, l'accès aux informations relatives au donneur d'ordre et au bénéficiaire constituera une nouveauté pour les banques intermédiaires de couverture. Lorsque les changements techniques auront été effectués, une banque intermédiaire dans un paiement de couverture transfrontalier devra, afin de se conformer à la législation nationale dont elle relève, procéder au filtrage des noms du donneur d'ordre et du bénéficiaire en les comparant aux listes établies dans la juridiction de cette banque qui répertorient les personnes physiques et morales dont les actifs doivent être bloqués, rejetés ou gelés. L'obligation de bloquer, rejeter ou geler des actifs ne peut pas reposer sur une procédure fondée sur une évaluation du risque [15] .

27. Certaines banques intermédiaires de couverture sont susceptibles de se retrouver dans une situation où le filtrage qu'elles effectuent en comparant les noms du donneur d'ordre et du bénéficiaire aux listes répertoriant les personnes physiques et morales dont les actifs doivent être bloqués, rejetés ou gelés serait redondant avec le filtrage effectué par la banque du donneur d'ordre. Cette situation pourrait se produire dans les cas suivants :

    – la liste applicable aux banques est la même dans les différentes juridictions intervenant dans le virement électronique ;

    – la banque du donneur d'ordre et la banque intermédiaire de couverture font partie du même groupe, toutes les entités de ce groupe recourent, pour le filtrage, à une liste unifiée établie par le siège, conformément au document Consolidated KYC Risk Management [16] du Comité de Bâle, et cette liste comporte les noms applicables dans chacun des sites du groupe [17] ;

    – la banque du donneur d'ordre filtre de sa propre initiative les noms des donneurs d'ordre et des bénéficiaires des virements transfrontaliers sortants, en les comparant aux listes en vigueur dans la

---

[14] Dans les cas (i) et (ii), la banque intermédiaire dans le paiement de couverture devrait prendre des mesures raisonnables pour informer la banque du donneur d'ordre et celle du bénéficiaire, le plus rapidement possible, du rejet ou du report du paiement de couverture.

[15] GAFI, *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing*, juin 2007, paragraphe 1.40 : L'obligation de geler les actifs de personnes physiques ou morales identifiées, dans les juridictions où cette obligation existe, est indépendante de toute évaluation du risque. Il s'agit d'une obligation absolue, qui ne peut pas être influencée par une procédure fondée sur une évaluation du risque.

[16] Comité de Bâle sur le contrôle bancaire, *Consolidated KYC Risk Management*, octobre 2004, paragraphe 19.

[17] Dans ce cas, la banque du donneur d'ordre devrait prendre en considération, identifier, évaluer et atténuer son risque juridique et son risque de non-conformité d'après les obligations énoncées dans la législation nationale applicable dont elle relève.

juridiction de la banque intermédiaire de couverture [18] , et ne procède aux virements que si aucune contrepartie ne figure sur la liste en vigueur dans cette juridiction. La banque du donneur d'ordre pourrait avoir, par exemple, pour objectif d'éviter les problèmes juridiques susceptibles de se poser si des personnes physiques ou morales qui n'ont pas été ciblées dans la juridiction dont relève le donneur d'ordre ou le bénéficiaire ont été répertoriées dans la juridiction de l'intermédiaire et si les fonds ont été gelés dans cette dernière [17].

28. Confrontée à cette situation ou à une situation analogue, une banque intermédiaire de couverture peut envisager de confier le filtrage nécessaire à l'institution qui est sa correspondante. Dans les juridictions qui autorisent cette délégation de tâche, une banque intermédiaire qui est encline à recourir à cette solution devrait le faire en ayant conscience qu'elle demeure responsable de la conformité à la législation nationale, même si elle a externalisé une fonction de filtrage. Les mesures de vigilance plus poussées, décrites dans la Recommandation 7 du GAFI et au paragraphe 50 du document *Devoir de diligence des banques au sujet de la clientèle*, donnent des principes directeurs utiles sur les dispositions que la banque intermédiaire de couverture devrait envisager de mettre en œuvre pour déterminer s'il est opportun qu'elle confie le filtrage à une institution correspondante. En particulier, les responsabilités respectives de chaque institution devraient être clairement définies. Avant d'établir une relation de banque correspondante, ainsi que périodiquement au cours de cette relation, la banque intermédiaire devrait évaluer les procédures de filtrage et les contrôles connexes appliqués par l'institution correspondante Elle pourrait, par exemple, soumettre un échantillon de virements sur la base d'une évaluation du risque, à un filtrage *a posteriori*, des noms du donneur d'ordre et du bénéficiaire.

### *3. Surveillance des relations de correspondant bancaire*

29. Les banques intermédiaires de couverture devraient surveiller leurs relations avec leurs correspondants bancaires, suivant les principes adaptés [19]. Cette surveillance leur permettra de déterminer si l'activité de l'institution correspondante et les contrôles de LCB/FT sont conformes aux principes qui ont été définis au début de la relation et qui ont été révisés ultérieurement [20]. Là aussi, de nombreuses juridictions autoriseront les banques à recourir à une approche fondée sur une évaluation du risque. Dans cette approche, et en fonction des dispositions nationales ainsi que de l'évaluation du risque de l'institution concernée, la surveillance serait probablement effectuée après la réalisation de la transaction, et sa fréquence et son étendue dépendraient des résultats de l'évaluation du risque mise en œuvre par la banque intermédiaire sur ses correspondants.

#### *(a) Surveillance visant à repérer des champs d'un message manifestement non pertinents ou incomplets*

30. Dans le cadre de la surveillance des relations de correspondant bancaire et en vertu de la législation nationale dont elles relèvent, les banques intermédiaires de couverture devraient élaborer et mettre en œuvre des politiques et des procédures raisonnables pour surveiller les données des messages des paiements après leur traitement, et régler le cas des champs qui, dans ces messages, sont manifestement non pertinents ou incomplets. Il est entendu que de nombreuses juridictions autoriseront les banques à recourir à une approche fondée sur une évaluation du risque, et les facteurs de risque ont été identifiés par le GAFI et par le groupe de Wolfsberg [21]. Si des champs d'un message sont manifestement non pertinents ou incomplets, il pourrait être décidé, par exemple, (i) de contacter la banque du donneur d'ordre, ou la banque intermédiaire précédente, afin de clarifier ou de compléter les informations reçues dans les champs requis, (ii) de déterminer (en cas d'incidents répétés impliquant le même correspondant ou lorsqu'un correspondant refuse d'apporter des informations supplémentaires) s'il convient de

[18] La banque du donneur d'ordre pourrait également, pour les mêmes raisons, prendre en compte la liste en vigueur dans la juridiction du bénéficiaire. Cependant, nous nous ne nous intéressons ici qu'aux conséquences, pour la banque intermédiaire dans des paiements de couverture, du filtrage effectué par la banque du donneur d'ordre.

[19] Comité de Bâle sur le contrôle bancaire, *Devoir de diligence des banques au sujet de la clientèle*, octobre 2001, paragraphes 49 à 52.

[20] D'après la Recommandation 5 du GAFI, des mesures de vigilance devraient être mises en œuvre sur les relations existantes aux moments opportuns. La Note interprétative à cette recommandation fait référence au document *Devoir de diligence des banques au sujet de la clientèle* publié par le Comité de Bâle en octobre 2001 (paragraphe 24).

[21] Cf. GAFI, *Guidance on the Risk-Based Approach to Combating Money Laundering and Terrorist Financing*, juin 2007, en particulier les paragraphes 1.43 et 3.20, et groupe de Wolfsberg, *Principes anti-blanchiment de Wolfsberg pour les banques correspondantes*, 21 octobre 2002, www.wolfsberg-principles.com. Les banques devraient se concentrer sur les facteurs pertinents pour l'évaluation du risque de virements manifestement non pertinents ou incomplets.

restreindre ou de mettre fin à la relation avec la banque correspondante concernée, ou avec la banque intermédiaire précédente ; en outre, les banques devraient signaler ces cas à l'autorité de contrôle dont elles relèvent, et/ou (iii) adresser une déclaration de soupçon aux autorités locales, lorsque la situation correspond à la définition locale des déclarations obligatoires. Il convient également de justifier par écrit les décisions prises.

***(b) Surveillance visant à déceler des opérations suspectes***

31. Étant donné que ni le donneur d'ordre ni le bénéficiaire ne sont les clients de la banque intermédiaire de couverture, celle-ci n'est généralement pas en mesure de connaître la finalité des transactions concernées ou d'exercer un devoir de vigilance à l'égard de ces personnes. Elle ne pourra donc probablement pas déterminer, après analyse des activités du donneur d'ordre et du bénéficiaire, si la transaction représentée par le paiement de couverture est suspecte ou non. Les intermédiaires peuvent néanmoins surveiller les transactions qu'ils traitent, afin de déceler des activités potentiellement suspectes, de les déclarer conformément à la législation de leur pays ou à la réglementation locale transposant les normes internationales et, si ces activités sont associées à un correspondant bancaire précis, examiner la relation avec ce dernier. La surveillance des paiements de couverture ne devrait pas être considérée comme une procédure qui, pour ces intermédiaires, élargirait les obligations ou ajouteraient des obligations nouvelles aux normes actuelles établies par le Comité de Bâle et le GAFI, mais uniquement comme un autre cas dans lequel s'appliquent des obligations qui existent déjà.

## C. Responsabilité de la banque du bénéficiaire

32. La banque du bénéficiaire doit identifier ce dernier, et vérifier son identité, conformément aux normes régissant le devoir de diligence relatif à la clientèle [22]. C'est également à la banque du bénéficiaire qu'il appartient de surveiller les activités de son client, le bénéficiaire. Aux termes de la Note interprétative à la Recommandation spéciale VII du GAFI, « les institutions financières devraient mettre en place des procédures efficaces fondées sur une évaluation du risque afin d'identifier les virements électroniques pour lesquels l'information complète relative au bénéficiaire fait défaut ».

33. D'après la Note interprétative à la Recommandation spéciale VII, les problèmes de transparence peuvent constituer un élément d'appréciation du caractère suspect d'un virement électronique ou des transactions y afférentes et, le cas échéant, de la nécessité de faire une déclaration de soupçons à la cellule de renseignement financier ou toute autre autorité compétente. Dans certains cas, l'institution financière du bénéficiaire devrait envisager de restreindre ses relations commerciales avec une institution financière qui ne satisfait pas aux normes de transparence, voire d'y mettre un terme. Il convient également de motiver par écrit la décision prise.

## D. Information du client et protection des données

34. La communication de données relatives au client à des tiers aux fins d'exécution d'une transaction, situation qui n'est pas propre aux paiements de couverture, ne devrait pas poser des problèmes spécifiques de protection des données. Dans tous les cas, les banques devraient se conformer à la législation et à la réglementation régissant la protection des données. Elles devraient prendre les mesures nécessaires pour s'assurer que l'information qu'elles reçoivent et traitent n'est utilisée qu'aux fins autorisées par la législation nationale et les normes internationales, et que le client est correctement informé. Il faudrait en particulier empêcher tout manquement à l'obligation de confidentialité ou toute utilisation commerciale de cette information. Les banques devraient s'engager à traiter de manière appropriée l'information apportée et empêcher son utilisation, par elles-mêmes ou par un tiers, à des fins illégitimes.

[22] Comme indiqué dans la Note interprétative à la Recommandation 5 du GAFI, « les mesures dans le cadre du devoir de vigilance relatif à la clientèle qui sont prévues dans la Recommandation 5 n'impliquent pas que les institutions financières identifient chaque client ou vérifient son identité chaque fois qu'elles procèdent à une transaction. L'institution financière peut s'en remettre aux mesures d'identification et de vérification qu'elle a déjà prises, à moins qu'elle ait des doutes quant à la véracité des informations obtenues ». Des exemples de situations qui pourraient conduire une institution à avoir de tels doutes sont également présentés.

### E. Autres considérations

35. Conformément aux principes énoncés par le Comité de Bâle dans le document *Devoir de diligence des banques au sujet de la clientèle*, le devoir de vigilance décrit dans les sections précédentes devrait être pris en compte dans toutes les procédures, tous les systèmes et tous les contrôles pertinents, faire partie de la formation du personnel concerné et être inclus dans les fonctions de la banque relatives à l'audit interne et à la conformité.

36. De plus, sauf dans les cas où, du fait de leur participation à un système de messagerie, de dispositions locales ou d'autres mécanismes équivalents, leurs correspondants se conforment à des normes de transparence appropriées, les banques devraient revoir leurs documents contractuels relatifs aux correspondants bancaires, afin de s'assurer que ces documents sont conformes aux normes de transparence, et n'établir des relations contractuelles qu'avec les banques qui respectent les normes de transparence visées au paragraphe 12.

## III. Rôle des autorités de contrôle

37. Comme indiqué dans le document *Devoir de diligence des banques au sujet de la clientèle* [23], « il incombe aux autorités de contrôle […] de veiller à ce que [les établissements bancaires] observent constamment de saines procédures CC [connaissance clientèle] et des critères éthiques et professionnels ». Les autorités de contrôle doivent, en particulier, avoir l'assurance que les banques élaborent et mettent en œuvre des politiques, procédures et processus appropriés lorsqu'elles agissent en qualité de banque du donneur d'ordre, de banque intermédiaire dans la chaîne des paiements de couverture ou de banque du bénéficiaire.

38. Les autorités de contrôle peuvent prendre plusieurs mesures pour évaluer la façon dont les institutions qu'elles supervisent gèrent le risque en ce qui concerne les paiements de couverture. Les autorités de contrôle devraient examiner avec attention les pratiques de gestion du risque afférentes à ces opérations. Voici des exemples de mesures :

- examiner si l'institution met en œuvre une évaluation du risque qui inclut les activités de paiement, en tenant compte de tous les facteurs pertinents, et notamment des relations avec les banques correspondantes intervenant dans ces opérations, du volume global des transferts de fonds et des juridictions concernées, ainsi que du rôle joué par l'institution dans les transferts de fonds ;
- déterminer si l'institution applique les normes de transparence et dispose de systèmes lui permettant de se conformer en permanence à ces normes, afin de s'assurer, notamment, que les banques ne recourent pas à des formats de message abrégés, par exemple pour les paiements de couverture interbancaires, pour éviter que les correspondants intermédiaires examinent de près les informations relatives au donneur d'ordre et au bénéficiaire ; les autorités de contrôle devraient également avoir l'assurance que les banques des donneurs d'ordre font figurer des informations complètes sur leurs clients dans tous les virements transfrontaliers ;
- évaluer si l'institution dispose de processus lui permettant d'exercer une vigilance adéquate à l'égard des banques correspondantes qui interviennent aussi dans la compensation transfrontalière des transactions afférentes à des paiements de couverture ;
- examiner les processus que l'institution a mis en place pour se conformer à la législation nationale applicable aux transactions qui doivent être bloquées, rejetées ou gelées ; et
- examiner les processus que l'institution a mis en place pour se conformer aux dispositions en vigueur portant sur : l'inclusion de données portant sur les ordres de paiement et la gestion des données à des fins d'analyse ; la surveillance, l'examen et la déclaration des opérations suspectes ; et documenter par écrit les décisions prises en ce qui concerne les transactions et les comptes.

39. Les autorités de contrôle devraient avoir l'assurance que des contrôles internes appropriés sont mis en œuvre pour surveiller les virements, qu'ils sont efficaces et que les banques se conforment aux principes

[23] Comité de Bâle sur le contrôle bancaire, *Devoir de vigilance des banques au sujet de la clientèle*, octobre 2001, paragraphe 61.

directeurs définis par les autorités de contrôle et de réglementation. Comme dans d'autres domaines, les autorités de contrôle devraient, en général, procéder non seulement à un examen des politiques, procédures et processus, mais également à l'échantillonnage de quelques transactions. La fréquence et l'étendue de ces examens devraient correspondre au niveau de risque. Lorsque la situation le justifie, les autorités devraient faire usage de leurs pouvoirs de contrôle pour s'assurer de la transparence des pratiques.

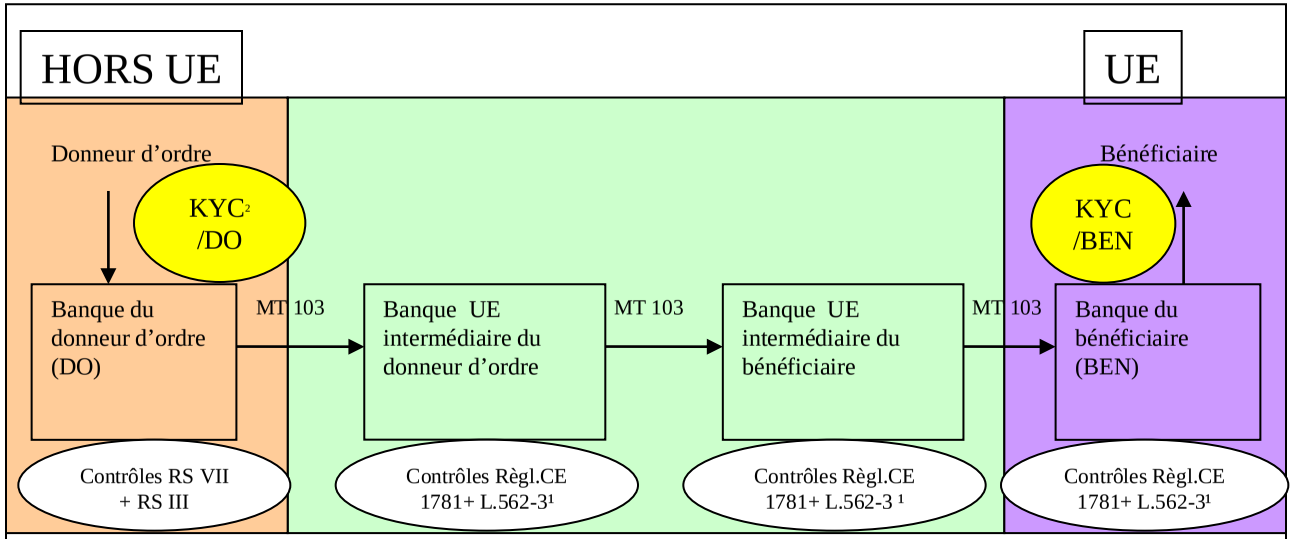
40. Si, au cours de leurs activités de contrôle ou à la suite de rapports émanant de banques, les autorités de contrôle constatent que des banques situées dans d'autres juridictions commettent des manquements graves aux normes de transparence, elles devraient en informer l'autorité de contrôle de la juridiction concernée. Si ces problèmes persistent, ils devraient être portés à l'attention des autorités compétentes.

# Virement en provenance d'un PSP hors de l'UE (en Euro)

## MT 103 En série

FLUX ➔

Contrôles sur le MT 103➔

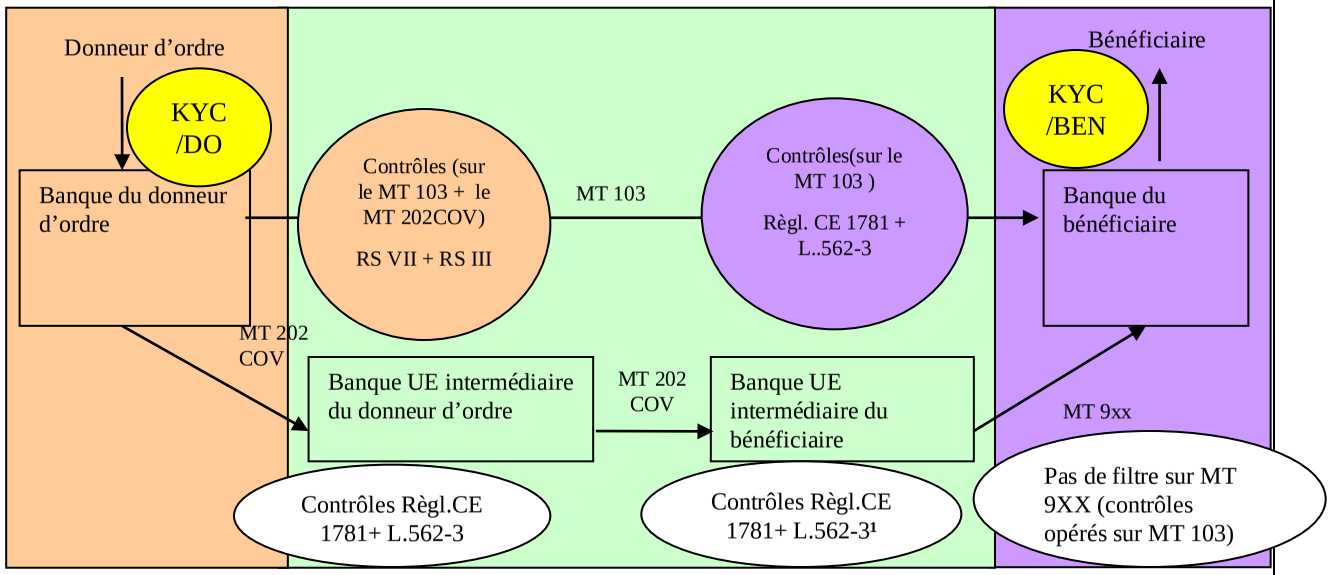



1 Ou autre réglementation locale d'un Etat membre de l'UE si autre pays que la France
2 KYC : know your customer : connaissance de son client

## MT 103 + MT 202 COV

FLUX ➔

Contrôle sur MT 202 COV➔



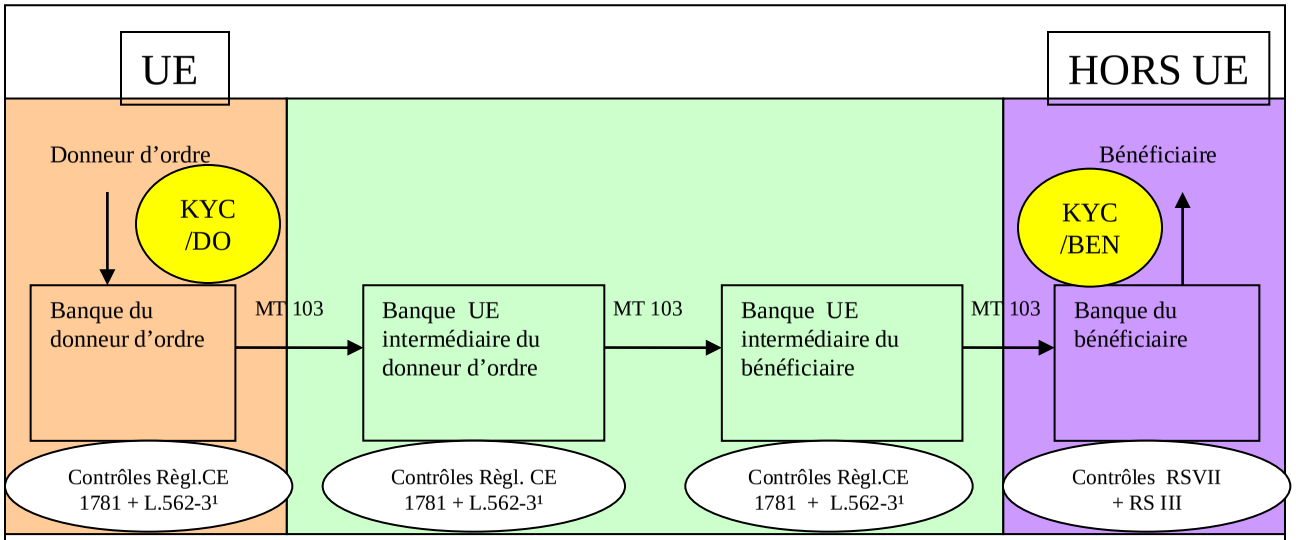

1 Le contrôle est complet (Règl. CE + L.562-3) en cas d'utilisation d'une même plateforme SWIFT. Le contrôle est restreint à BIC banque du DO (banque UE) en cas de rupture de plateforme de messagerie [ou de plateforme intra groupe.]

# Virement à destination d'un PSP hors UE (en Euro)

**MT 103**
**En série**

FLUX ➔

Contrôle sur le MT 103➔



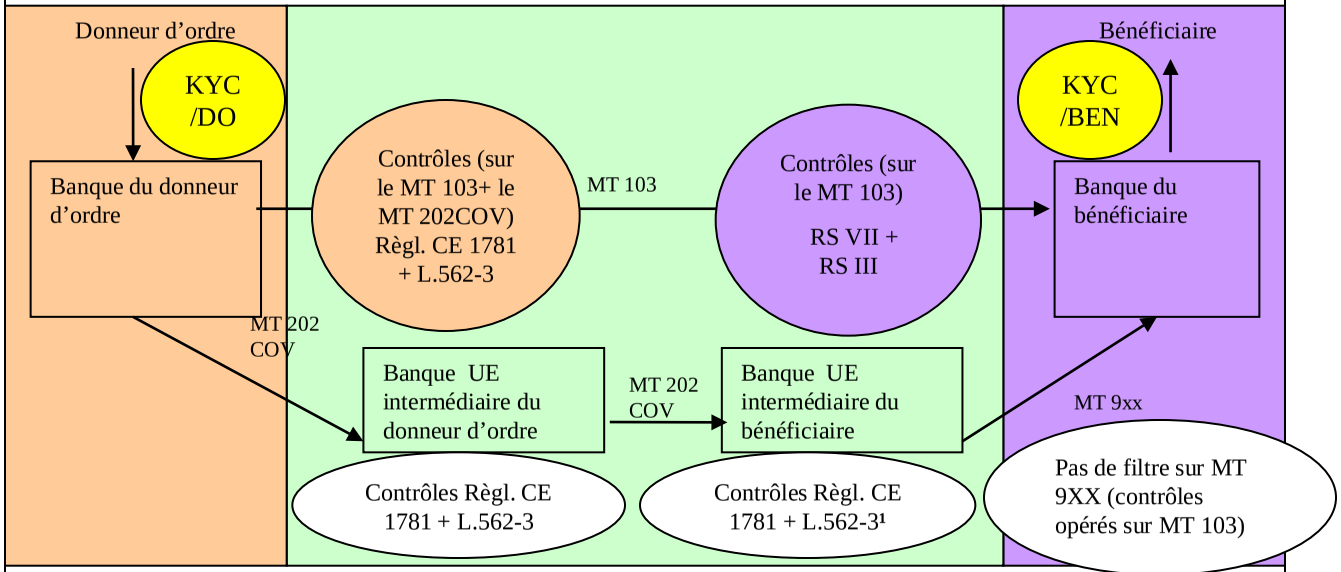

¹ Ou autre réglementation locale d'un Etat membre de l'UE si autre pays que la France.

**MT 103**

**+ MT 202 COV**

FLUX ➔

Contrôle sur MT 202 COV➔



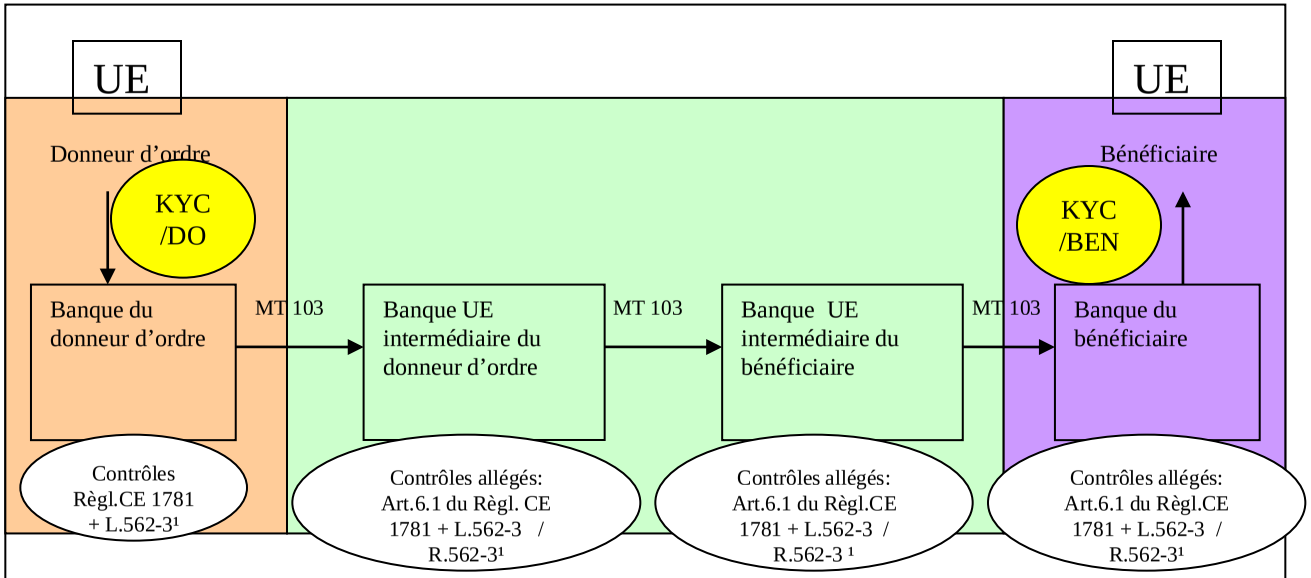

¹ Le contrôle est complet (Règl. CE + L.562-3) en cas d'utilisation d'une même plateforme SWIFT. Le contrôle est restreint à BIC banque du DO (banque UE) en cas de rupture de plateforme de messagerie [ou de plateforme intra groupe.]

# Virement à l'intérieur de l'UE (en Euro)

**MT 103**
**En série**

FLUX ➔

Contrôle sur
le MT 103➔



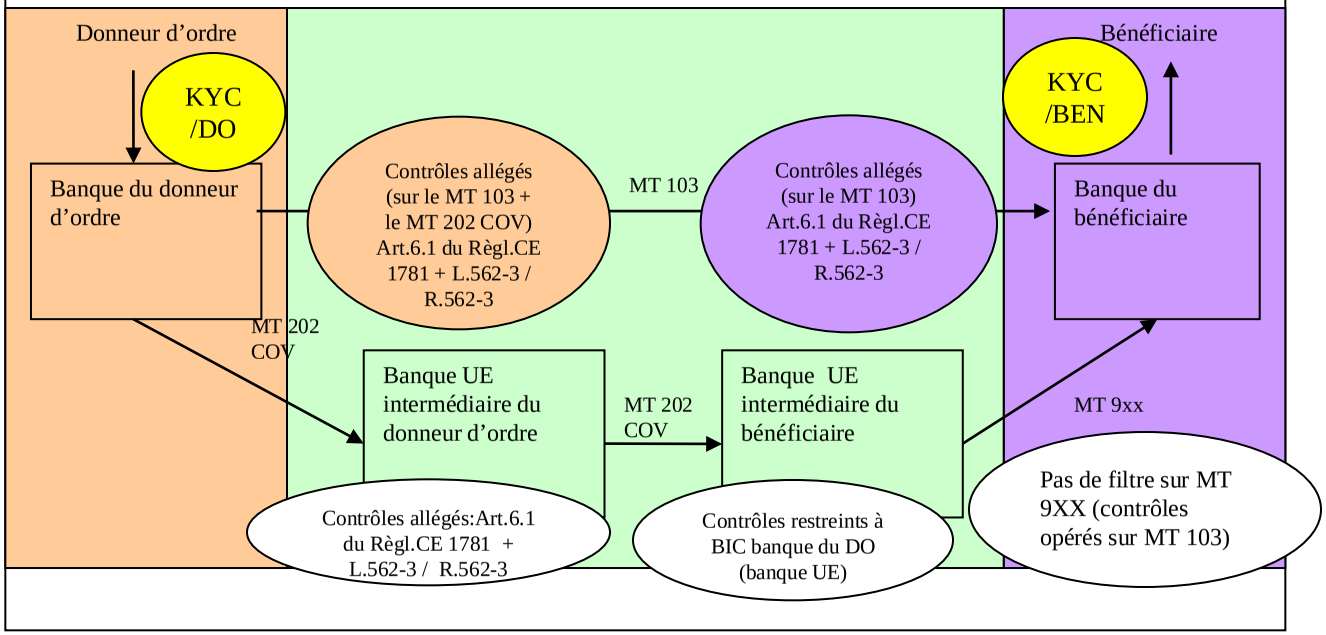

¹ Ou autre réglementation locale d'un Etat membre de l'UE si autre pays que la France.

**MT 103**

**+ MT 202 COV**

FLUX ➔

Contrôle sur
MT 202 COV➔

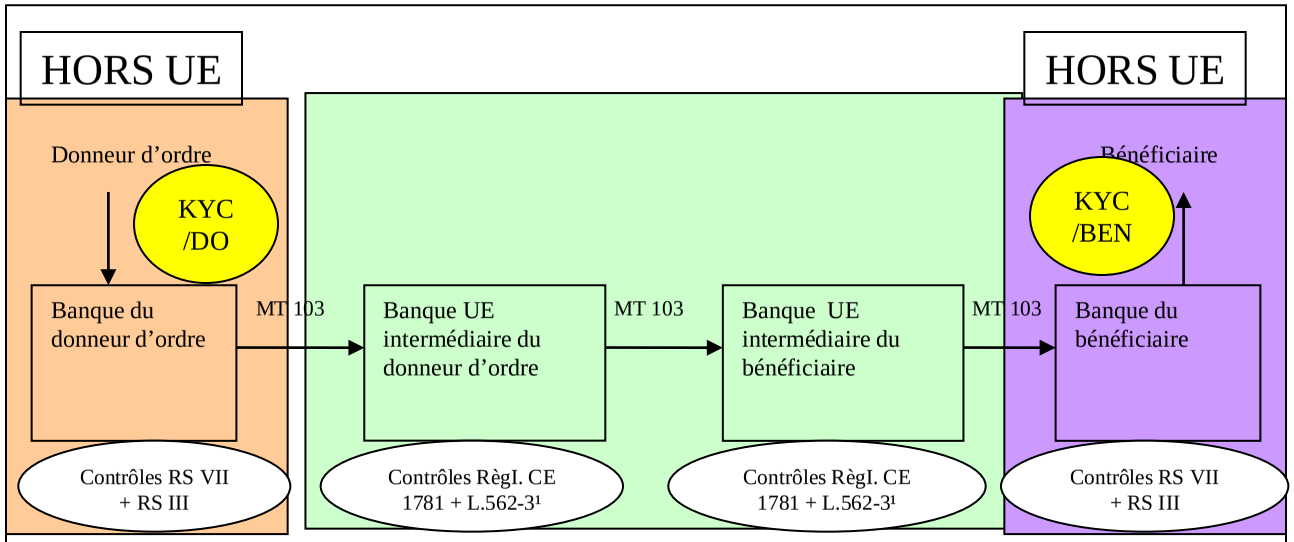


# Virement entre deux PSP hors UE (Euro)

## MT 103 En série

FLUX ➔

Contrôle sur le MT 103➔

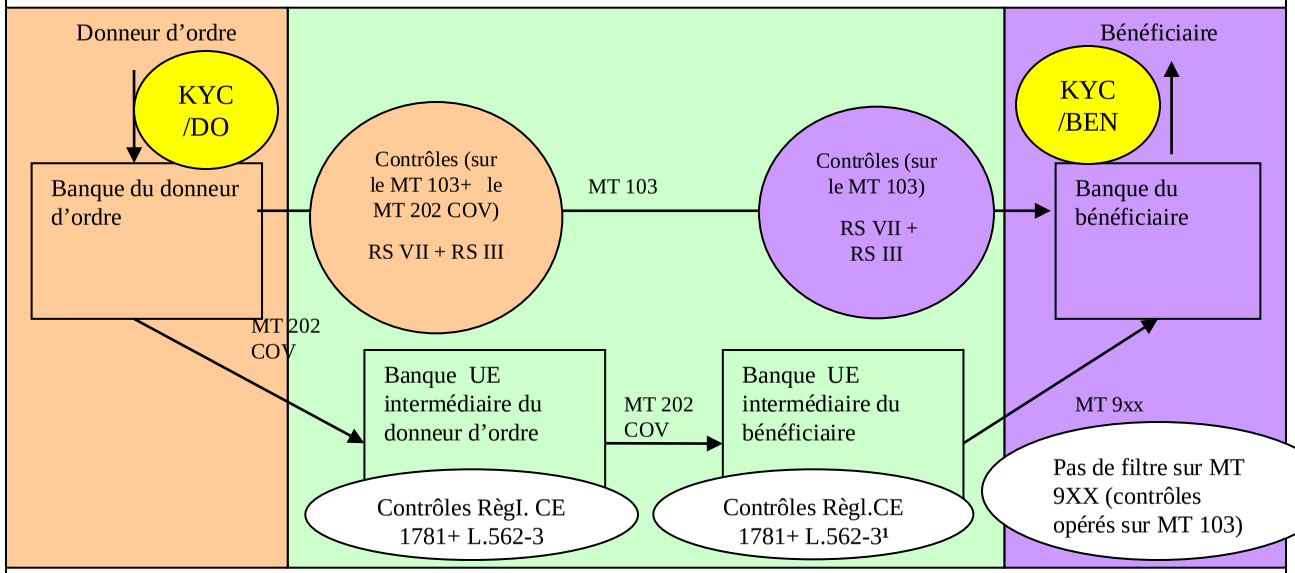



[1] Ou autre réglementation locale d'un Etat membre de l'UE si autre pays que la France.

## MT 103 + MT 202 COV

FLUX ➔

Contrôle sur MT 202 COV➔



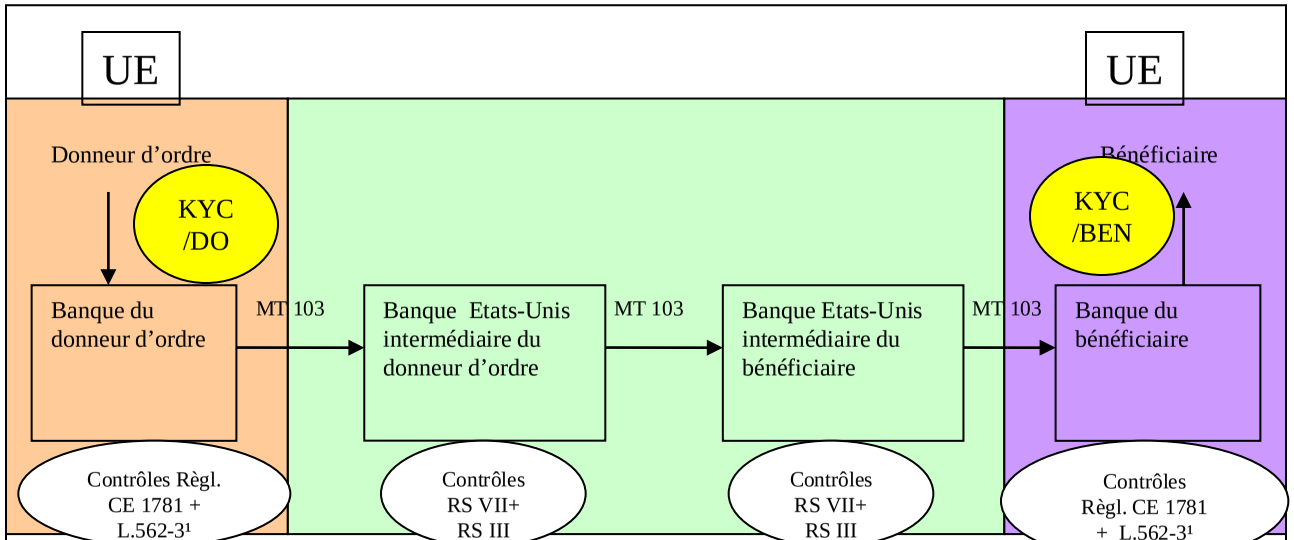

[1] Le contrôle est complet (Règl. CE + L.562-3) en cas d'utilisation d'une même plateforme SWIFT. Le contrôle est restreint à BIC banque du DO (banque UE) en cas de rupture de plateforme de messagerie [ou de plateforme intra groupe.]

# Virement entre deux PSP de l'UE (devise non Euro, par exemple Dollar)

## MT 103 En série

FLUX ➔

Contrôle sur le MT 103➔




¹ Ou autre réglementation locale d'un Etat membre de l'UE si autre pays que la France.

## MT 103 + MT 202 COV

FLUX ➔

Contrôle sur MT 202 COV➔