Evaluation sectorielle des risques de blanchiment de capitaux et de financement du terrorisme dans le secteur financier belge relevant des compétences de contrôle de la Banque nationale de Belgique

JUILLET 2023

Table des matières

Executive summary

Le 24/10/2023, la Banque nationale de Belgique (BNB) a adopté la nouvelle version de son évaluation sectorielle des risques de blanchiment de capitaux et de financement du terrorisme (ci-après « BC/FT ») dans le secteur financier belge qui relève de ses compétences de contrôle en vertu de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces (ci-après la loi AML)[1].

L'intérêt d'une telle évaluation est multiple :

1. elle alimente l'analyse nationale de risque de blanchiment de capitaux. Elle sera donc communiquée à la CTIF qui est l'organe chargée de coordonner les travaux relatifs à l'analyse nationale des risques. Ces travaux répondent à la Recommandation 1 du Groupe d'action financière (GAFI), selon laquelle les pays doivent identifier, évaluer et comprendre leurs risques BC/FT et adopter une approche basée sur les risques pour atténuer les risques identifiés ;
2. elle formalise et articule les connaissances acquises en la matière par les services de contrôle de la Banque dans l'exercice de leurs responsabilités. Elle permet à la Banque d'affiner son approche fondée sur les risques et de mieux orienter la supervision en allouant adéquatement ses ressources de contrôle. Il est à souligner, conformément aux standards internationaux, que l'exercice de la supervision fondée sur les risques requiert qu'il s'appuie sur une connaissance suffisante des risques de BC/FT associés aux secteurs contrôlés. Il est donc nécessaire que la Banque dispose également d'une évaluation sectorielle des risques ;
3. elle aide les institutions financières à identifier des risques auxquels elles sont exposées et leur permet également d'affiner leur approche fondée sur les risques.

La méthode retenue dépasse la seule évaluation des risques vus de manière « sectorielle » (établissements de crédit, entreprises d'assurance, établissements de paiement et de monnaie électronique, sociétés de bourse) et se focalise également sur dix-neuf services et activités identifiés comme pouvant présenter un risque pour chacune des institutions sous supervision de la Banque.

Elle consiste à évaluer le risque inhérent qui résulte des principales menaces de BC/FT auxquelles les institutions financières sont exposées et les vulnérabilités qui peuvent les impacter. Ensuite les éventuelles mesures d'atténuation des menaces et vulnérabilités sont prises en compte pour déterminer le risque résiduel.

L'analyse est fondée sur de nombreuses sources d'informations mais également sur les constats issus des travaux de supervision effectués par la Banque ces dernières années.

Cette nouvelle version de l'évaluation sectorielle des risques constitue :

1. un **approfondissemen**t de l'évaluation sectorielle des risques de blanchiment de capitaux.
    - Certains risques transversaux nouveaux ont été identifiés alors que d'autres ont fait l'objet d'une analyse plus approfondie. Ainsi, l'évaluation sectorielle des risques BC/FT identifie certaines particularités propres à la situation en Belgique pouvant avoir un impact sur le risque de BC/FT
    - De nouveaux développements sont consacrés notamment
        - à l'accélération du processus de digitalisation impactant les modes de distribution des activités et produits financiers ;
        - aux conséquences que le Brexit a pu avoir sur le secteur financier avec l'établissement en Belgique de plusieurs institutions jouant un rôle important sur le marché et reposant, dans certains cas, sur un business model «innovant» ;

[1] La première version a été adoptée le 8 septembre 2020

- à l'importance grandissante de nouveaux services (Virtual IBAN's) pouvant être des vecteurs de nouvelles typologies et risques de BC/FT ;
- à l'impact de l'activité du port d'Anvers sur les risques BC/FT.

- L'évaluation procède à l'analyse de dix-neuf services financiers contre treize dans l'ancienne version. Les activités d'acquiring, trade finance, change manuel, caution et nantissement, affacturage, clearing et custody font à présent l'objet d'une analyse distincte.
- Différentes sources d'informations publiques ont été utilisées afin de bâtir l'analyse. On peut citer à cet égard des rapports émis par le Groupe d'action financière (GAFI), L'European Banking Authority(EBA), la Cellule de traitement des informations financières (CTIF).

2. une **première évaluation** sectorielle des risques en matière de financement du terrorisme.
   - Il a été choisi d'établir une seule analyse sectorielle couvrant à la fois les risques liés au blanchiment de capitaux et ceux liés au financement du terrorisme vu la proximité des phénomènes et typologies qui sous-tendent leur financement.
   - Différentes sources d'informations publiques ont été utilisées afin de bâtir l'analyse. On peut citer des rapports émis par le FMI, Europol, Eurojust, la CTIF, la Sûreté de l'Etat. La participation par la Banque à différents workshops en matière de lutte contre le financement du terrorisme organisés sous l'égide de la Commission européenne s'est avéré utile.
   - Cinq phénomènes terroristes ont été identifiés comme une menace pour le secteur:
     - Le fondamentalisme islamiste
     - L'extrémisme de droite
     - L'extrémisme de gauche et l'anarchisme
     - Le terrorisme lié à la situation politique d'un pays étranger
     - D'autres formes de terrorisme
   - Il est ensuite procédé, pour chaque service financier, à l'analyse des risques liés au financement du terrorisme auxquels les institutions financières sont exposées en identifiant les risques inhérents et les vulnérabilités

Elle fera l'objet d'une actualisation sur la base d'un cycle de deux ans.

Elle est disponible sur le site internet de la BNB.

Synthèse des risques liés au blanchiment de capitaux

	Risques inhérents	**/5**	**Vulnérabilités**	**/5**	**Risque résiduel**	**/5**
Activités de paiement	Elevés	4	Elevées	4	Elevé	4
Transferts de fonds	Elevés	4,5	Elevées	4	Elevé	4,5
Activités d'acquiring	Modérés	2	Modérées	2	Modéré	2
Initiation de paiement	Faibles	1,5	Modérées	2,5	Modéré	2
Service d'informations sur les comptes	Nuls	0	Nulles	0	Nul	0
Activités de monnaie électronique	Modérés	2,5	Significatives	3	Modéré	2,5
Private banking	Significatifs	3,5	Elevées	4	Elevé	4
Retail banking	Modérés	2,5	Modérées	2,5	Modéré	2,5
Corporate banking	Significatifs	3	Modérées	2	Modéré	2,5
Trade finance	Significatifs	3	Significatives	3	Significatif	3
Service de change manuel	Elevés	4	Significatives	3	Significatif	3,5

Service de caution et de nantissement	Faibles	1,5	Faibles	1,5	Faible	1,5
Activité d'affacturage	Modérés	2	Modérées	2	Modéré	2
Correspondent banking	Elevés	4	Significatives	3	Significatif	3,5
Clearing/Custody/Depositaires	Modérés	2,5	Modérées	2	Modéré	2
Conseil en investissement (private banking)	Significatifs	3,5	Elevées	4	Elevé	4
Conseil en investissement (sans détention)	Modérés	2	Modérées	2	Modéré	2
Assurances vie	Modérés	2	Faibles	1,5	Faible	1,5
Assurances vie (produits d'investissement)	Significatifs	3	Modérées	2,5	Modéré	2,5

Synthèse des risques liés au financement du terrorisme

	Risques inhérents	**/5**	**Vulnérabilités**	**/5**	**Risque résiduel**	**/5**
Activités de paiement	Elevés	4	Elevée	4	Elevé	4
Transferts de fonds	Elevés	4	Elevées	4	Elevé	4
Activités d'acquiring	Faibles	1,5	Faibles	1,5	Faible	1,5
Initiation de paiement	Faibles	1,5	Faibles	1,5	Faible	1,5
Service d'informations sur les comptes	Nuls	0	Nulles	0	Nul	0
Activités de monnaie électronique	Significatifs	3	Significatives	3	Significatif	3
Private banking	Faibles	1,5	Modérées	2	Faible	1,5
Retail banking	Elevés	4	Elevées	4	Elevé	4
Corporate banking	Modérés	2	Modérées	2	Modéré	2
Trade finance	Modérés	2	Modérées	2	Modéré	2
Service de change manuel	Elevés	4	Significatives	3	Significatif	3,5
Service de caution et de nantissement	Faibles	1,5	Faibles	1,5	Faible	1,5
Activité d'affacturage	Faibles	1,5	Faibles	1,5	Faible	1,5
Correspondent banking	Elevés	4	Significatives	3	Significatif	3,5
Clearing/Custody/Depositaires	Modérés	2	Modérées	2	Modéré	2
Conseil en investissement (private banking)	Faibles	1,5	Significatives	3	Modéré	2
Conseil en investissement (sans détention)	Faibles	1,5	Significatives	3	Modéré	2
Assurances vie	Faibles	1,5	Faibles	1,5	Faible	1,5
Assurances vie (produits d'investissement)	Faibles	1,5	Faibles	1,5	Faible	1,5

Liste des abréviations

AISP	Account Information Service Provider
BC/FT	Le blanchiment de capitaux et le financement du terrorisme
BCE	Banque Centrale Européenne
BNB	Banque nationale de Belgique
CTIF	Cellule de traitement des informations financières
EBA	European Banking Authority
EEE	Espace Economique Européen
EU	Union européenne
GAFI	Le Groupe d'action financière
FBI	The Federal Bureau of Investigation
FSMA	Financial Services and Markets Authority
FMI	Fonds Monétaire International
IBAN	International Bank Account Number
LBC/FT	Lutte contre le blanchiment de capitaux et le financement du terrorisme
Loi AML/FT	Loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces
NRA	Analyse nationale des risques
OCAM	L'Organe de Coordination pour l'Analyse de la Menace
PEP	Personne politiquement exposée
PISP	Payment Initiation Service Provider
PSD2	Payment Services Directive
SRA	L'analyse sectorielle des risques
UBO	Ultimate Beneficial Owner

1 OBJET

Le présent document procède à l'évaluation sectorielle des risques de blanchiment de capitaux et de financement du terrorisme dans le secteur financier belge qui relève des compétences de contrôle de la Banque nationale de Belgique (ci-après « la BNB»). Cette évaluation sectorielle des risques vise à orienter l'exercice par la BNB de ses contrôles en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT) conformément à son approche fondée sur les risques et constitue dès lors un complément de la politique de contrôle fondée sur les risques qu'elle a arrêtée. Elle est également destinée à alimenter l'évaluation nationale des risques pour ce qui concerne les risques associés au secteur financier belge, et plus précisément, aux institutions dont la BNB est l'autorité de contrôle en vertu de la loi du 18 septembre 2017 relative à la prévention du blanchiment de capitaux et du financement du terrorisme et à la limitation de l'utilisation des espèces (ci-après la loi AML)[2].

Cette analyse sectorielle des risques sera également utile aux entités sous supervision en vue de la rédaction de leur évaluation globale des risques. L'article 16 de la loi AMLM précise qu'elles doivent tenir compte de toutes les informations pertinentes dont elles disposent. Les conclusions de la présente analyse, également fondées sur des actions de contrôle, leur fourniront un aperçu sectoriel utile.

Le présent document consiste en une mise à jour de la première évaluation sectorielle des risques de blanchiment de capitaux effectuée en 2020 et procède pour la première fois à l'analyse des risques liés au financement du terrorisme.

La méthodologie poursuivie vise d'une part à formaliser une expertise développée au sein des services de la BNB et d'autre part à constituer la base d'un processus d'affinement d'évaluation des risques sectoriels en matière de blanchiment de capitaux (BC) et de financement du terrorisme (FT) qui sera amené à évoluer au fur et à mesure de l'évolution du secteur financier.

Cette analyse s'appuie notamment mais non exclusivement sur[3] :

- l'évaluation supranationale des risques de la Commission européenne COM(2022) 554 final et ses annexes du 27 octobre 2022 (ci-après, le « SNRA »),
- l'analyse nationale des risques de blanchiment de capitaux adoptée le 3 février 2023 par le Comité ministériel de coordination de la lutte contre le blanchiment de capitaux d'origine illicite,
- FATF- Guidance National Money Laundering and Terrorist Financing Risk Assessment, 2013
- FATF Report - Professional money laundering du 26 juillet 2018
- les Orientations de l'ABE du 1er mars 2021 sur les facteurs de risque BC/FT,
- la Joint Opinion of the European Supervisory Authorities JC2019 59 of 4 October 2019 on the risks of money laundering and terrorist financing affecting the European Union's financial sector actualisée par l'Opinion dated 3 March 2021 on the risks of money laundering and terrorist financing affecting the Union's financial sector
- le rapport EBA Risk assessment on ML/TF risks associated with payment institutions du 16 juin 2023.
- les Rapports annuels de la Cellule de Traitement des Informations Financières (CTIF)
- les résultats des actions de contrôle effectuées par la BNB dans le cadre de ses compétences exercées en qualité d'autorité nationale compétente en vertu de la loi AML.
- l'évaluation nationale des risques relative au financement du terrorisme de 2017 (diffusion restreinte)
- le "paper" du FMI- Countering the financing of terrorism. Good practices to enhance effectiveness du 12 mai 2023

---

2 Moniteur belge du 6 octobre 2017 - Chambre des représentants (www.lachambre.be) Documents : 54-2566.

3 Les principaux documents peuvent être consultés sur le site AML/CFT de la Banque nationale de Belgique : Principaux documents de référence | nbb.be

- le rapport Europol – European Union Terrorism Situation and Trend Report 2022
- Eurojust- Rapport annuel 2022 et 2023.
- les rapports annuels de la Sûreté de l'Etat 2020 et 2021
- Egmont paper- Counter terrorism in Belgium: Key challenges and policy options – 2016
- Rusi Europe- Project Craaft – Bit by Bit: Impact of new technologies on terrorism financing risks du 5 avril 2022.

2 MÉTHODOLOGIE

Une évaluation globale du secteur financier qui n'identifierait pas en son sein différentes caractéristiques pour lesquelles des risques et des vulnérabilités particulières seraient présents ne présenterait qu'une faible valeur ajoutée.

La méthodologie suivie vise donc à isoler au sein des différentes catégories d'institutions qui sont soumises à la supervision de la BNB, des activités spécifiques qui se situent au cœur de leurs divers modèles d'entreprise et dont les caractéristiques renvoient à des niveaux de risques inhérents, de vulnérabilité et de risques résiduels particuliers et potentiellement différenciés.

En raison de difficultés liées à l'accès à une information précise agrégée par activité, il n'est pas aisé de tirer des conclusions générales totalement documentées à l'issue de l'exercice. L'expertise acquise par l'exercice du contrôle (sur site et hors site) permet à la BNB de former son « jugement d'expert' », de sorte que l'analyse permet d'aboutir à une série de conclusions suffisamment fondées qui mettent en exergue les risques liés aux activités et les vulnérabilités des institutions dans le cadre du respect des dispositions légales et réglementaires anti-blanchiment.

Une méthodologie visant la mise à jour de l'analyse a été établie.

2.1 IDENTIFICATION DES ACTIVITÉS COUVERTES

Au 31 décembre 2022, le paysage des 209 établissements sous la supervision en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT) de la BNB était le suivant :

- Etablissements de crédit de droit belge : 30
- Succursales d'établissements de crédit d'un pays de l'Espace Economique Européen (EEE) 45
- Succursales d'établissements de crédit hors EEE : 5
- Société de bourse de droit belge : 12
- Succursales d'une société de bourse d'un pays de l'EEE : 10
- Entreprises d'assurance vie de droit belge : 25
- Succursales d'entreprises d'assurance vie d'un pays de l'EEE : 9
- Etablissements de paiement et établissements de monnaie électronique de droit belge : 39
- Succursales et points de contacts centraux d'établissements de paiement et établissements de monnaie électronique d'un pays de l'EEE : 32
- Dépositaires centraux : 2

Pour cet exercice, 19 activités exercées par quatre groupes d'institutions soumises au contrôle de la BNB ont été identifiées et ont permis d'atteindre le degré de granularité souhaitable.

Pour les établissements de paiement, les activités prévues par la PSD2 sont abordées. Une attention particulière est donnée :

- paiement et de transferts de fonds
- monnaie électronique.
- acquiring
- initiation de paiement,
- services d'information sur les comptes

Pour les établissements de crédit, les activités suivantes ont été identifiées :

- banque privée (private banking),
- de services bancaires aux entreprises (corporate banks et trade finance)
- de système de banque d'épargne populaire (savings banks),de l'affacturage et du cautionnement et de nantissement
- de correspondent banking,
- de clearing/settlement,
- custody et dépositaires centraux

Elles peuvent être exercées par des institutions de taille et de nature différente : des grandes banques universelles aux institutions spécialisées uniquement dans l'une ou l'autre activité.

Un point est consacré au secteur du conseil en investissement proposé par les sociétés de bourse.

Pour le secteur de l'assurance, une distinction est opérée entre les produits d'assurance vie à long terme et d'assurance vie en tant que produit d'investissement, d'une part, étant donné les différences entre la nature des produits et des risques y associés, et d'autre part, du fait que ces produits sont occasionnellement proposés par des institutions différentes et affectées de vulnérabilités spécifiques.

Il sera tenu compte de l'exposition des institutions financières aux risques BC/FT liés aux « virtual assets » même si la BNB n'est pas l'autorité compétente. Il n'en demeure pas moins, que les institutions financières peuvent être utilisées par leurs clients aux fins de réaliser des opérations portant sur des actifs virtuels ou détenir de tels actifs pour leurs clients.

Cette liste non limitative pourra être amenée à évoluer lors des mises à jour ultérieures de cette évaluation sectorielle des risques et de la méthodologie y afférente.

2.2 ACTIVITÉS ET RISQUES NON COUVERTS

Cette analyse ne couvre pas les risques relatifs aux opérations que noueraient des clients belges et ou étrangers par le biais des institutions exerçant en Belgique au titre de la libre prestation de service au sein de l'EEE sans l'intervention d'agent/distributeur. Ces institutions n'entrent en effet pas dans le champ de contrôle de la BNB. L'influence qu'elles peuvent exercer quant aux risques de blanchiment de capitaux et de financement du terrorisme affectant les activités financières de clients belges peut ne pas être marginale s'ils ne sont pas adéquatement pris en compte par les autorités des Etats Membres d'origine.

Cette analyse ne couvre pas davantage ni ne mesure les risques des activités exercées illégalement sans agrément et qui échappent par conséquent aux compétences de contrôle de la BNB ou de toute autre autorité de contrôle nationale ou étrangère.[4]

[4] En Belgique la FSMA est compétente pour entamer des poursuites concernant des activités prestées sans agrément

2.3 ANALYSE NATIONALE DES RISQUES DE BLANCHIMENT DE CAPITAUX

L'Analyse nationale des risques de blanchiment de capitaux adoptée le 3 février 2023 permet d'apporter un éclairage sur l'importance et sur certaines caractéristiques des phénomènes de BC/FT en Belgique.

Il en ressort qu'en Belgique, l'importance du blanchiment en Belgique en 2019 peut être chiffré à plus ou moins 12,7 milliards EUR. La position centrale du pays au sein de l'Union européenne et le fait qu'elle abrite un nombre important d'institutions européennes et d'organismes internationaux constitue un facteur de risque.

Selon la Police Fédérale, le nombre de procès-verbaux (PV) pour blanchiment retrouvés dans la banque de données nationale générale (BNG) a augmenté, passant de 856 en 2017 à 1.133 en 2018. Les PV ont été essentiellement établis dans trois arrondissements : Anvers, Bruxelles et Halle-Vilvorde.

La Cellule de traitement des informations financières (CTIF), pour sa part, est alimentée par des déclarations de soupçons reçues des entités assujetties à la loi AML (95%) et d'autres autorités compétentes (5%). Il y a lieu de préciser que la CTIF ne peut pas s'auto-saisir et investiguer des opérations qui ne lui auraient pas été préalablement communiquées par les entités assujetties. Elle ne dispose dès lors pas d'une vue exhaustive du phénomène en Belgique. Entre 2017 et 2022, la CTIF a transmis environ un millier de dossiers par an aux autorités judiciaires.

Les flux financiers dans ces dossiers s'élèvent en moyenne à +/- 1,5 milliard d'euros annuellement. Ce chiffre doit être pris avec précaution dans la mesure où la CTIF travaille sur des indices sérieux qu'il appartient aux autorités judiciaires de confirmer par la suite en prononçant une condamnation.

Au cours des dix dernières années (2009 à 2019), des condamnations ont été prononcées dans 633 dossiers transmis par la CTIF aux autorités judiciaires et des amendes et saisies ont été prononcées pour plus de 300 millions d'euros.

Phénomènes criminels :

L'Analyse nationale des risques de blanchiment de capitaux décrit les principaux phénomènes criminels identifiés en Belgique et dont il y a lieu de tenir compte afin d'essayer d'identifier les produits, services et canaux de distribution qui pourraient être utilisés aux fins de blanchiment de capitaux et de financement du terrorisme. Il peut être cité par ordre d'importance, le trafic illicite de stupéfiants, la fraude fiscale, la fraude sociale, l'escroquerie, les vols ainsi que la traite et le trafic d'êtres humains.

D'autre part, les criminalités sous-jacentes de blanchiment identifiées par la CTIF donnent également une indication des phénomènes criminels les plus importants en Belgique. Cinq phénomènes criminels ressortent des statistiques la CTIF : la fraude fiscale grave, organisée ou non, le trafic illicite de biens et de marchandises, la fraude sociale, la criminalité organisée et l'escroquerie. Ce qui correspond à près de 90% des transmissions de la CTIF en termes de montants communiqués aux autorités judiciaires.

Il y a lieu de souligner que le trafic illicite de stupéfiants est un phénomène important en Belgique (vu les nombreuses saisies de drogue ces dernières années) mais que compte tenu de l'utilisation de techniques de blanchiment permettant l'évitement du système financier (comme la technique de la compensation ou le transport transfrontalier de cash), les transactions issues de cette forme de criminalité sont aujourd'hui moins visibles dans les statistiques de la CTIF.

Risques et vulnérabilités :

L'Analyse nationale des risques relève que le secteur financier est de longue date soumis à des règles strictes et au contrôle prudentiel de la BNB et de la FSMA, y compris en matière de prévention du blanchiment de capitaux. Le niveau de vulnérabilité d'un secteur d'activité dépend fortement de la mise en œuvre de mesures efficaces de prévention du blanchiment de capitaux. Si elles sont correctement mises en œuvre, ces mesures devraient diminuer le niveau de la menace de blanchiment dans ce secteur. Les menaces et les vulnérabilités sont par conséquent des notions étroitement liées.

S'agissant par exemple d'évaluer le niveau de la menace que les institutions financières sont susceptibles de représenter, et indépendamment de leur vulnérabilité aux risques de blanchiment, il y a lieu de relever qu'elles sont soumises à des règles strictes et à un contrôle prudentiel qui inclut des mesures visant à vérifier l'honorabilité professionnelle et l'expertise adéquate de leurs actionnaires, dirigeants et responsables de fonctions essentielles (notamment, les fonctions d'audit interne et de conformité). Cette compétence de contrôle est directement exercée par la Banque centrale européenne à l'égard des plus grands établissements de crédit (les « banques systémiques »), dans le cadre du « mécanisme de surveillance unique », et par la BNB, sous le contrôle de la Banque centrale européenne, à l'égard des établissements de crédits moins importants.

Les mesures de contrôle prudentiel combinées aux mesures de contrôle spécifique de leurs dispositifs de prévention du blanchiment, sont de nature à réduire la menace de blanchiment que les institutions financières représentent. Ces contrôles ne peuvent cependant pas garantir l'absence totale de cette menace.

2.4 FACTEURS DE RISQUES TRANSVERSAUX

Certains facteurs de risques transversaux classiques, tels que l'utilisation de l'argent liquide ou l'importance du risque lié aux modes de distribution sont connus de longue date.

Cependant, au vu du fait que les modifications des activités de blanchiment continuent d'accompagner la transformation des activités financières et de l'environnement règlementaire, préventif et répressif qui l'entoure, des nouveaux facteurs transversaux de risques de blanchiment liés au secteur financier sont désormais apparus :

- les conséquence du Brexit,
- FinTech[5],
- le recours aux nouvelles technologies,
- les actifs virtuels,
- les évolutions et les divergences législatives entre les États membres et les divergences dans les pratiques de supervision BC/FT.

2.4.1 LES CONSEQUENCES DU BREXIT

Le contexte particulier du Brexit a en effet été un événement marquant essentiellement entre 2016 et 2021. De nombreuses demandes d'agrément introduites auprès de la BNB trouvaient leur origine dans la délocalisation partielle ou totale en Belgique des activités jusqu'alors déployées au sein de l'UE depuis le Royaume-Uni. En Belgique, le phénomène a essentiellement touché le secteurs des établissements de paiements et de monnaie électronique. Des acteurs, dont certains parmi les leaders mondiaux du marché ont choisi de localiser leurs activités en Belgique et de les « passeporter » dans l'Espace Economique Européen. L'examen de la qualité de leur système LBC/FT a mis en lumière des lacunes essentiellement consécutives à une externalisation très

[5] FinTech désigne l'innovation financière à base de technologie qui peut déboucher sur de nouveaux modèles d'entreprise, applications, processus ou produits avec un impact matériel associé sur les marchés et institutions financiers et la prestation de services financiers.

intensive et insuffisamment contrôlée des tâches et fonctions relatives à la LBC/FT à d'autres entités du groupe établies en dehors de l'Union Européenne. Il en résulte souvent l'absence de substance des entités agréée en Belgique et une forte dépendance à d'autres entités du groupe.

2.4.2 LA FINTECH

La FinTech connait une croissance significative en Belgique apportant par la même occasion des produits et services innovants. L'émergence de promoteurs de ces nouvelles entités ayant une culture essentiellement voire purement IT, et donc n'appréhendant pas ou pas de manière adéquate et suffisamment approfondie les contraintes LBC/FT liées à la commercialisation de leurs nouveaux produits, peut constituer un risque non négligeable et qui nécessitent également une adaptation des superviseurs tant dans le cadre de leurs contrôles que dans le cadre légal et réglementaire. Le recours par les établissements financiers à des fournisseurs de services externalisés sans évaluer suffisamment dans quelle mesure leurs services répondent aux exigences LBC/FT les expose à un risque important. En outre, le nombre croissant d'applications FinTech en tant que prestataires de services aux clients des établissements de crédit permet une plus grande opacité des transactions et une diminution de leur traçabilité.

La plupart des acteurs marché belge recourent à des solutions technologiques externes et d'autres bases de données, principalement pour identifier ou analyser le profil des clients et leurs activités transactionnelles. Ce marché technologique est relativement limité. Cette concentration potentielle du marché des données soulève des questions concernant :

- la qualité des données ainsi utilisées par un nombre important d'acteurs,
- le manque d'analyse intellectuelle personnalisée,
- l'exacerbation de la réduction des risques (de-risking).

2.4.3 LES ACTIFS VIRTUELS

Les actifs virtuels peuvent être attractifs pour les criminels car ils favorisent la discrétion et l'anonymat par rapport aux autres moyens de paiement. Depuis le 1er mai 2022, les activités de certains prestataires de services liés aux actifs virtuels sont réglementées en Belgique et sont soumises à la supervision de la FSMA, à l'exclusion de toute compétence formelle de la BNB à leur égard. Néanmoins, les institutions financières soumises à la supervision de la BNB peuvent être utilisées par les criminels lors de la phase de l'intégration dans le système financier des fonds issus d'opérations en actifs virtuels. En outre, des clients d'institutions financières peuvent détenir des actifs virtuels ce qui induit des risques particuliers consistant à insérer dans le système financier le produit de la conversion d'actifs numériques en monnaie ayant cours légal[6].

Par ailleurs, les établissements de crédit peuvent avoir des relations d'affaires avec des clients qui sont des « prestataires de services en actifs virtuels ». Notamment, des sociétés qui exploitent des crypto ATM (BTM) et qui collectent énormément de cash seront amenées à insérer le produit de l'activité dans le secteur financier ;

En outre, il se peut que des clients des établissements financiers soient impliqués ou involontairement dans des transactions frauduleuses en crypto monnaies ou qu'ils soient victimes de fraudes :

- des clients font un transfert depuis leurs comptes bancaires vers un compte IBAN appartenant à des escrocs alors qu'ils pensent effectuer un investissement/placement en crypto monnaies (fausses plateformes proposant des placements en crypto monnaies) ;
- des clients sont invités à faire une transaction depuis leur portefeuille en crypto monnaies vers une plateforme d'échange de crypto monnaies (la victime réalise d'abord un achat de

6 Cf. Lignes directrices du Gafi du 21 juin 2019 mise à jour en octobre 2021 sur l'approche fondée sur les risques appliquée aux actifs virtuels et aux prestataires de services liés aux actifs virtuels.

crypto monnaies sur une plateforme d'échange grâce à son compte bancaire et ensuite elle transfère les crypto monnaies sur le portefeuille en crypto monnaies des escrocs) ;
- des clients réceptionnent des fonds provenant de fraudes (ransomware…) ou d'autres activités illicites (vente de stupéfiants) ;
- des clients qui sont actifs dans des opérations de *mining*[7] et qui encaissent sur leur compte en Belgique le produit de ces activités.

Le phénomène est en augmentation constante, il est encore à ce stade difficile d'en chiffrer l'ampleur car toutes les victimes ne déposent pas plainte.

L'émergence de nouveaux défis liés à **l'innovation technologique**, la plus grande intégration des flux financiers dans le marché unique et le caractère « extraterritorial » de l'activité de certaines institutions rendent encore plus utile la recherche d'une plus grande homogénéité des législations nationales ainsi que des pratiques des autorités nationales compétentes en matière de supervision BC/FT.

Il y a également lieu d'indiquer que des établissements financiers peuvent avoir pris des participations dans des avoirs virtuels ce qui peut engendrer un risque prudentiel lequel sort du champ de la présente analyse. Il ressort néanmoins des informations prudentielles qu'à la fin de l'année 2022, l'exposition aux actifs virtuels des institutions financières actives en Belgique est extrêmement limitée. Les établissements de crédit actifs en Belgique sont tenus de notifier leur exposition aux cryptos assets à la BNB. Actuellement seuls deux établissements de crédit ont des projets concrets en ce domaine. Certaines autres banques étant à un stade plus exploratoire.

2.4.4 LES ÉVOLUTIONS ET LES DIVERGENCES LÉGISLATIVES ENTRE LES ÉTATS MEMBERS ET LES DIVERGENCES DANS LES PRATIQUES DE SUPERVISION BC/FT

Certaines évolutions dans la réglementation peuvent créer des situations rendant plus complexes les activités de contrôle. Il peut être fait référence aux développements récents relatifs aux paiements instantanés. En outre, certaines différences dans les législations territorialement applicables peuvent être exploitées aux fins de faciliter les opérations de blanchiment de capitaux.

L'émergence de ces nouveaux risques a été confirmée par le rapport de l'*EBA* [8]" auquel la BNB a notamment contribué.

Au-delà des facteurs de risques transversaux classiques, ces nouveaux facteurs de risque, induits par la modification du secteur au niveau de ses acteurs et des modalités de ses produits, concernent, à des degrés divers, toutes les activités financières et accroissent in fine la possibilité d'effectuer des opérations de blanchiment.

Ainsi, il existe aujourd'hui des conditions nouvelles qui rendent le blanchiment souvent plus difficilement détectable/identifiable qu'auparavant (ex virtual ibans).

2.4.5 LA CRISE SANITAIRE COVID 19

Contrairement aux craintes initiales, le secteur financier belge ne semble pas avoir été impacté par l'apparition de nouvelles typologies propres à la crise Covid. La crainte de voir des faux médicaments, vaccins être diffusés ou que des commandes de faux médicaments soient passées ne semble pas s'être matérialisée significativement en Belgique. La raison est certainement à trouver dans le fait qu'une fois disponibles sur le marché international, les vaccins et éventuels traitements ont été progressivement mis à disposition du plus grand nombre de manière ordonnée et bien

---

7 Un "mineur" est une personne ou une entité qui participe à un réseau décentralisé de monnaie virtuelle en exécutant un logiciel spécial pour résoudre des algorithmes complexes dans un système "proof of work" ou un autre système de preuve utilisé pour valider les transactions dans le système de monnaie virtuelle.

8 EBA Report on ML/FT risks associated with payment institutions (EBA/REP/2023/18) du 16 juin 2023.

souvent gratuitement. Il est par contre indéniable que la crise Covid, les confinements et restrictions imposées ont permis d'accélérer la digitalisation, le développement et le recours et aux nouvelles technologies tant en nombre qu'en volume dans le secteur financier. Le milieu criminel a dès lors pu y trouver des opportunités de phishing ou de fraudes.

2.4.6 MODIFICATION DU SECTEUR FINANCIER ET DES MODÈLES D'AFFAIRES

Les modifications du secteur financier influent sur les modèles d'affaires des institutions financières ainsi que sur la connaissance générale qu'ont les institutions des clients et de leurs caractéristiques (voir également point n°2.4.11).

Dans la mesure où davantage de produits sont proposés aux clients en Belgique, l'accroissement significatif de la concurrence sur des marchés à faible rentabilité peut occasionnellement exacerber les modèles de prises de risques des institutions. La Commission européenne[9] relève précisément comme une des quatre vulnérabilités majeures la mise sous pression des modèles de propension aux risques et le danger que cette pression représente sur l'activité financière en termes de risques de blanchiment.

Parallèlement, la segmentation des activités financières complexifie davantage et peut diminuer la connaissance que les institutions peuvent développer sur les activités et les caractéristiques de leurs clients. En effet, une institution peut être moins à même de détecter une opération atypique d'un client si elle ne dispose d'informations sur son client que dans le cadre d'une activité limitée : ainsi une institution proposant uniquement un type de produit/service financier spécifique dispose naturellement en principe de moins d'informations sur les caractéristiques de ses clients qu'une institution qui peut déployer une connaissance plus détaillée de son client au travers d'une approche commerciale transversale et plus inclusive.

2.4.7 LA MISE EN ŒUVRE DU REGISTRE DES BÉNÉFICIAIRES EFFECTIFS (UBO)

Le rapport 2022 d'Eurojust[10] fondé sur une analyse des dossiers enregistrés auprès d'Eurojust entre 1er janvier 2016 et le 31 décembre 2021, vu l'utilisation de sociétés écrans ou de sociétés boîtes aux lettres destinées à faciliter les opérations de blanchiment de capitaux et de financement du terrorisme, constate que l'identification des UBO's est l'un des principaux défis juridiques et opérationnels auxquels sont les autorités sont concernées.

La mise en œuvre du registre UBO en Belgique dans lequel sont inscrits tous les "Ultimate Beneficial Owners" ou "bénéficiaires effectifs" de toutes les entités juridiques en ce compris les ASBL (*non profit sector*) constitue dès lors une avancée importante. Un niveau élevé de transparence des informations sur les bénéficiaires effectifs est essentiel pour lutter contre la création de structures volontairement opaques. Il convient néanmoins que les établissements financiers développent des outils permettant de garantir que l'identification des bénéficiaires effectifs est effectuée lors de l'application des mesures de vigilance à l'égard des clients.

2.4.8 AGRESSION MILITAIRE RUSSE CONTRE L'UKRAINE

A la suite de l'invasion d'une partie du territoire ukrainien par la Russie en février 2022, l'Union européenne (UE) a sévèrement aggravé les sanctions mises en place contre la Russie depuis 2014. L'UE a également imposé des mesures à l'encontre de la Biélorussie. La Commission européenne mentionne ces mesures dans l'analyse des risques BC/FT du 22 octobre 2022. Une application

---

9 Rapport de la Commission européenne au Parlement européen et au Conseil sur l'évaluation des récents cas présumés de blanchiment de capitaux impliquant des établissements de crédit de l'Union européenne, COM(2019) 373 du 24 juillet 2019

10 https://www.eurojust.europa.eu/publication/eurojust-report-money-laundering.

stricte des règles relatives aux « bénéficiaires effectifs » est essentielle pour pouvoir mettre en œuvre les sanctions.

Néanmoins, les « sanctions financières ciblées » (« SFC ») décrétées par l'UE dans ce contexte n'ont pas de lien avec la lutte contre le blanchiment de capitaux, le financement du terrorisme ou le financement de la prolifération des armes de destruction massive. Elles n'entrent pas dans le champ d'application de la Loi AML[11]. En outre, il n'apparaît pas clairement que l'invasion de l'Ukraine aurait accru le risque de BC/FT en Europe. Au contraire, les SFC décrétées à l'encontre de la Russie et de le la Biélorussie pour des raisons géopolitiques, sans lien avec la LBC/FT, peuvent avoir entravé les flux de fonds d'origine criminelle à destination de l'Europe.

2.4.9 UTILISATION DE L'ARGENT LIQUIDE

L'utilisation de l'argent liquide demeure privilégiée par les criminels dans la mesure où il assure un anonymat des transactions dû à son absence de traçabilité.

C'est pourquoi il existe un risque plus important que les produits financiers impliquant un usage d'argent liquide soient potentiellement davantage liés à l'un des trois processus de blanchiment (placement, empilement, intégration). Il en va de même pour des avoirs comme l'or et les diamants, qui peuvent être conservés en toute sécurité et facilement négociés, transportés et conservés.

Les produits liés à l'utilisation d'argent liquide sont donc considérés comme davantage risqués, a fortiori au vu de la diminution constante et confirmée de l'utilisation de l'argent liquide dans l'économie comme le montrent les trois éléments suivants.

Premièrement, les chiffres des retraits d'argent aux guichets automatiques continuent leur diminution : en 2018, le nombre de ces retraits était de l'ordre de 260 millions pour un montant de 35 milliards d'euros, soit, ramené à la population belge, 23 retraits d'une valeur moyenne de 134 euros par citoyen belge et par an. Le nombre de retrait était de l'ordre de 148 millions pour les chiffres de l'année 2021 pour un montant de 22 milliards. Cette baisse est continue.

Cette tendance est renforcée par la baisse du nombre d'agences bancaires et de distributeurs automatiques de billets accessibles chaque année depuis 2015. Après avoir compté jusqu'à 15 306 appareils en 2010, le pays n'en comptait plus que 10 649 en 2019 et 8 460 en 2020, 5062 en 2021 et environ 5.000 en 2022. Selon les estimations actuellement proposées, il semble qu'à la fin 2025, il y aura 2.369 sites permettant des retraits en Belgique sur lesquels seront répartis 4.061 ATM. Soit respectivement une diminution de 1.296 emplacements et de 1.872 distributeurs par rapport à la situation de fin 2021. La réduction du nombre de guichets automatiques impactera le volume de circulation d'argent cash mais n'aura que peu d'impact sur l'utilisation que les milieux criminels peuvent en faire.

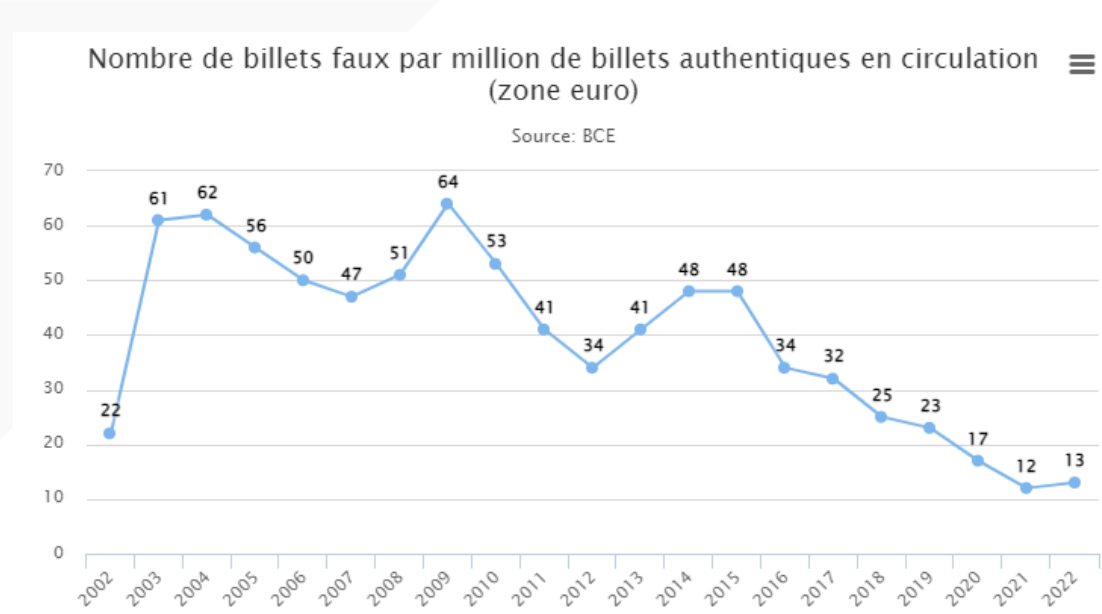
Les fermetures des agences en raison des mesures de confinement liées à la COVID 19 ont fondamentalement modifié le comportement des consommateurs. Cet impact a poussé certaines institutions financières à accélérer leurs plans de transformation numérique et à poursuivre un objectif de diminution du nombre d'agences et de distributeurs automatiques d'argent en Belgique. Le changement le plus évident dans le comportement bancaire des consommateurs a été l'augmentation importante de l'activité bancaire en ligne et sur les applications mobiles mais également l'augmentation du nombre de paiements électroniques dans les commerces au détriment de l'argent liquide. Ces modifications de comportement auront également un impact à plus long terme sur les canaux de distributions des produits par les établissements financiers.

---

11 Elles n'entrent pas dans le champ d'application des articles 4,6° et 8, § 1, 3° de la Loi AML

Notons ensuite au titre de la diminution de ce risque, que depuis 2017, la loi AML limite également les paiements et les dons en espèces à 3.000 EUR par transaction commerciale et exclut tout recours à l'argent liquide pour les transactions immobilières.

Enfin, sur le plan de la contrefaçon de billets, le nombre de faux billets retirés de la circulation en Belgique est en constante diminution depuis 2016, notamment du fait de l'amélioration de des mesures de sécurisation des billets et des efforts de conscientisation de la BNB en la matière. Selon les statistiques de la BNB, 12.016 faux billets pour un montant de 589.605 € ont été retirés de la circulation en 2022, soit 24% de moins que l'année précédente. Une tendance identique est constatée dans la zone euro.



2.4.10 MODES DE DISTRIBUTION DES PRODUITS/DIGITALISATION

Les canaux de distribution des activités et produits financiers ont une influence certaine sur le risque de blanchiment dans la mesure où ils peuvent comprendre des failles alimentant une identification insuffisante des clients et de leurs caractéristiques et une surveillance inadaptée de leurs opérations.

Notamment, lorsqu'un établissement financier a recours à des agents indépendants pour distribuer ses produits, le risque existe qu'en l'absence de lien hiérarchique, certains d'entre eux puissent être tentés d'accorder plus d'attention à la satisfaction des attentes mêmes illicites de leurs clients dont dépend leurs commissions qu'au respect des instructions et procédures internes de l'institution financière qu'ils représentent. Ce risque est encore accru lorsque l'agent n'est pas exclusif et peut dès lors diviser les opérations de ses clients portant sur des montants importants en opérations de plus petits montants et plus discrètes, exécutées en recourant aux différentes institutions financières que cet agent représente, rendant par là même la détection du caractère suspect de ces opération plus complexe. L'institution doit dès lors mettre en œuvre des mécanismes de contrôle fiables et efficaces et y allouer les ressources nécessaires.

Par ailleurs, comme révélé dans l'avis conjoint *des Autorités européennes de surveillance*[12], la digitalisation croissante des activités financières peut également participer à la complexification de l'identification et de la connaissance des caractéristiques du client, que ce soit via le détournement

---

12 Joint Opinion of the European Supervisory Authorities JC2019 59 of 4 October 2019 on the risks of money laundering and terrorist financing affecting the European Union's financial sector actualisée par l' Opinion dated 3 March 2021 on the risks of money laundering and terrorist financing affecting the Union's financial sector.

des mesures de contrôles automatiques (voire via le vol d'identité électronique), ou que ce soit, plus traditionnellement avec l'enchevêtrement de multiples transactions visant à dissimuler le destinataire des fonds blanchis.

La digitalisation représente en effet un risque accru lié au blanchiment de capitaux et de financement du terrorisme dans le cas où les procédures de vigilance à l'égard des clients ne sont pas appropriées pour tenir compte des particularités techniques du canal de distribution digitalisé utilisé ou ne sont pas appliquées correctement à travers les modes de distribution qui sont privilégiés par ces nouveaux acteurs.

2.4.11 IDENTIFICATION DES CLIENTS ET DE SES CARACTÉRISTIQUES

Comme identifié dans l'évaluation supranationale des risques de la Commission européenne du 27 octobre 2022, l'anonymat reste une caractéristique essentielle recherchée par les criminels pour le blanchiment de l'argent provenant d'une activité illégale.

Certaines activités financières proposant des produits composés en partie ou en totalité de manière anonymisée entrainent dès lors *de facto* un accroissement du risque de blanchiment.

L'identification du client demeure la clé de voute du système actuel de lutte anti-blanchiment dans la mesure où elle seule permet d'établir une connaissance suffisante des caractéristiques du client, permettant *in fine* la détection de transactions potentiellement suspectes par rapport à son profil devant être après analyse, le cas échant, transmises à la CTIF.

La digitalisation du processus d'entrée en relation d'affaires avec un client et par conséquence de son identification peut engendrer des risques lorsque la technologie utilisée n'est pas entièrement maîtrisée ou se base sur des technologies présentant des lacunes.

La falsification des documents, qui est un phénomène réel en Belgique[13], ou le recours à des mules financière[14] ou à des hommes de paille pour différentes activités financières représentent donc des risques de détournement des mesures de vigilance mises en place par les institutions et basées sur l'identification du client.

L'identification et la connaissance du client peuvent également être complexifiées lorsque les criminels recourent à des constructions juridiques complexes impliquant de multiples sociétés écrans ou des sociétés « boite aux lettres ».

Notons toutefois, au titre de la diminution de ce risque, la mise en place en Belgique au 31 octobre 2018 du registre des bénéficiaires effectifs qui contribue à réduire les difficultés liées à l'intrication des transactions financières. En outre ce registre n'empêche pas la mise en place dans des pays étrangers présentant un risque élevé de structures opaques à l'entremise desquelles des blanchisseurs peuvent tenter de devenir clients d'institutions financières installées en Belgique tout en s'efforçant de dissimuler leur véritable identité.

2.4.12 CONCENTRATION DE PERSONNES POLITIQUEMENT EXPOSÉES (PEP)

La politique de siège poursuivie par la Belgique, et notamment la présence des sièges de l'OTAN et de l'Union européenne, ont un impact sur la concentration des personnes politiquement exposées

---

13 Près de 3.000 faux papiers d'identité ont été saisis par la police belge en 2019. Voir également en matière de terrorisme l'affaire des faux documents ayant permis à la cellule de Paris et de Bruxelles de financer les attentats.

14 Les mules financières, également appelés « passeurs d'argent » sont des « personnes recrutées –en connaissance de cause ou à leur insu - qui aident les organisations criminelles à blanchir des capitaux illicites. Elles le font en mettant leurs propres comptes à disposition pour recevoir et transférer de fonds frauduleux et ainsi leur donner une apparence de légitimité.

présentes sur le territoire belge. La corruption de personnes politiquement exposée constitue une infraction sous-jacente au blanchiment de capitaux et continue d'être un élément central du modus operandi des groupes criminels organisés, comme indiqué dans la stratégie de l'UE pour lutter contre le crime organisé 2021-2025.

L'exposition du secteur à ce risque a été rappelé par l'actualité de la fin de l'année 2022 au sujet de possibles faits de corruption de membres du Parlement européen et potentiellement clients d'établissements actifs en Belgique.

Dans son Rapport annuel 2021, la CTIF indique que l'analyse des dossiers de blanchiment révèle des dossiers impliquant des personnalités importantes du monde politique, diplomatique (…). Plusieurs dossiers concernent ainsi des personnes politiquement exposées (PPE) en Belgique ou à l'étranger ou un proche d'une PPE.

A côté du cercle relationnel des organisations internationales et des ambassades nationales gravitent également des firmes multinationales, des lobbies, des ONG et de la presse internationale qui contribuent également à augmenter le nombre de personnes politiquement exposées pouvant potentiellement être client et/ou bénéficiaire d'une institution exerçant son activité en Belgique.

Cette concentration potentielle importante de PEP représente un risque accru pour les établissements qui sont soumis à certaines vulnérabilités, comme celles relatives à exercer des activités en Belgique sans disposer d'une connaissance ou des moyens suffisants pour établir l'origine des patrimoines et s'assurer que ceux-ci ne proviennent et/ou ne sont pas destinés à des fins de corruption.

2.4.13 CRIMINALITÉ ET RISQUE DE BLANCHIMENT DE CAPITAUX LIÉS AUX ACTIVITÉS DU PORT D'ANVERS

Ces derniers mois différentes enquêtes criminelles ont mis en lumière l'importance du port d'Anvers qui constituerait une porte d'entrée pour le trafic de stupéfiants dans une large partie de l'Europe. Il semble ressortir des observations des autorités policières et judiciaires ainsi que du rapport annuel 2021 de la CTIF que les opérations de blanchiment de capitaux issus de ces trafics peuvent être identifiés à deux niveaux. Les montants les plus importants dirigés vers les organisateurs des réseaux trafiquants nécessitent la mise en œuvre de moyens plus sophistiqués comme la création et l'utilisation des sociétés écrans via les comptes desquels les fonds transitent, et le recours à de faux documents commerciaux. Les criminels recourent également à certaines techniques de blanchiment permettant l'évitement du système financier comme la technique de la compensation ou le transport transfrontalier de cash. Néanmoins, le secteur financier belge est également soumis à un risque accru d'être utilisé par la criminalité organisée aux fins du blanchiment de capitaux. Les intervenants à un niveau plus bas du réseau ont pour leur part recours à des moyens moins sophistiqués pour transférer les fonds dont ils disposent souvent en cash. Les établissements de crédit (retail, trade finance) mais également les établissements de paiement et de monnaie électronique et notamment ceux offrant de service de paiements dont des comptes libellés en diverses monnaies peuvent être particulièrement exposés à ces risques.

2.4.14 NOUVEAUX DEVELOPPEMENTS PRODUITS

L'émergence de nouveaux produits et modes de distributions, notamment basés sur des technologies nouvelles, et laissant peu de place aux contacts individuels entre l'établissement et le client est un élément d'attraction pour les criminels qui postulent, au début de la mise en service, sur une connaissance et maîtrise plus faible tant dans le chef des établissements financiers que des superviseurs

2.4.15 FRAUDE À LA CARTE BANCAIRE (EN LIGNE), LE PHISHING, SPOOFING

L'année 2020, de par la crise sanitaire mondiale, a connu une augmentation de toutes les formes de fraude en ligne, y compris du phishing. Cette criminalité vise à amener les victimes à transmettre à leur insu leurs codes bancaires personnels aux fraudeurs – généralement en cliquant sur un lien qui mène vers un site web frauduleux – permettant à ces derniers d'effectuer des transactions en leur nom. En 2020, 34 millions d'euros ont ainsi été subtilisés en Belgique. Dans l'intervalle d'un an, ce chiffre a baissé et s'élève à 25 millions d'euros en 2021[15].

La fraude à l'investissement ou fraude de type « boiler room » est en augmentation en Belgique. Il s'agit d'une forme d'escroquerie dans laquelle les fraudeurs proposent d'acheter des actions ou d'autres produits financiers fictifs ou sans valeur. La victime est généralement contactée de manière non sollicitée pour bénéficier d'une offre prometteuse de rendements très élevés. Des comptes bancaires ouverts en Belgique ou se référant à un IBAN « BE » sont utilisés par les criminels. Il peut fréquemment s'agir d'« IBAN virtuels » (voir ci-après). La BNB a été informée de plusieurs situations dans lesquelles des comptes bancaires ont été utilisés par les criminels pour obtenir les fonds payés par les victimes avant de les transférer à l'étranger.

Un certain nombre d'institutions financières ont été confrontées à une augmentation des situations de « mules bancaires », que ce soit dans le secteur des banques de détail ou des money remitters. L'analyse montre dans ces cas que l'activité d'un client se modifie brutalement (*pay in and pay out* souvent depuis ou vers l'étranger). Les autorités judiciaires belges ont démantelé un important réseau actif en la matière au mois de septembre 2021 mais il est évident que bien d'autres criminels restent actifs depuis la Belgique ou l'étranger.

2.4.16 LES INFORMATIONS PROVENANT DU RAPPORT ANNUEL DE LA CTIF

L'examen des rapports annuels de la CTIF portant sur ses activités en 2021 et 2022 permet d'avoir une vue sur l'activité déclarative des institutions financières soumises à la supervision de la BNB.

Nombre de déclarations

	2019	**2020**	**2021**	**2022**
Etablissements de crédit	11.237	17.678	21.624	28.379
Entreprises assurance Vie	308	661	749	1.172
Sociétés de bourse	49	33	39	54
Etablissements de paiement	5.814	6.263	16.016	16.425
Etablissements de monnaie électronique	90	654	774	520

Nombre d'entités assujetties ayant effectué des déclarations

	2019	**2020**	**2021**	**2022**
Etablissements de crédit	60	58	57	55
Entreprises assurance Vie	16	17	22	18
Sociétés de bourse	9	6	6	7
Etablissements de paiement et Etablissements de monnaie électronique	37	32	32	36

Nombre de dossiers transmis au Parquet

	2019	**2020**	**2021**	**2022**

15 https://www.febelfin.be/fr/communique-de-presse/les-chiffres-sur-le-phishing-en-2021

Etablissements de crédit	783	942	990	1.029
Entreprises assurance Vie	-	2	2	6
Sociétés de bourse	2	3	-	1
Etablissements de paiement	102	96	97	80
Etablissements de monnaie électronique	1	4	7	5

Il n'est pas aisé de tirer des conclusions de l'analyse du volume de l'activité déclaratives des institutions regroupées par secteur d'activité.

Ainsi, le nombre total de déclarations effectuées par les établissements appartenant à un secteur est immanquablement impacté par le volume des activités et des transactions effectuées par les clients. Le nombre élevé de déclarations effectuées peut mettre en lumière à la fois le nombre d'opérations suspectes identifiées et dès lors le risque BC/FT encouru mais *a contrario* le nombre élevé de déclarations de soupçons montre également l'attention qui est portée à la détection d'opérations suspectes. Le raisonnement contraire peut être tenu lorsque le nombre de déclarations de soupçons est faible.

Il est noté une augmentation constante du nombre de déclarations d'opérations suspectes dans tous les secteurs (à l'exception des sociétés de bourse). Ce constat s'explique certainement par une plus grande prise de conscience des établissements. Les actions de contrôle menées par la BNB, des établissements de crédit et des établissements de paiement ou de monnaie électronique y ont également contribué. Il en est ainsi lorsque ces actions aboutissent à la réalisation de lookbacks sur des transactions passées qui n'auraient pas fait l'objet de l'attention requise.

Par ailleurs, la très forte augmentation des déclarations d'opérations suspectes effectuées par les établissements de paiement (+ de 300%) semble trouver en partie une explication dans l'établissement en Belgique de certains opérateurs britanniques très importants, à la suite du Brexit, mais aussi par le fait que certains établissements de paiement ont procédé à des déclarations en se fondant sur le dépassement de seuils. Bien qu'il soit explicable par la plus grande difficulté de ces établissements de connaître les caractéristiques de leurs clients et, par conséquent, d'identifier les opérations qui sont « atypiques » au regard de ces caractéristiques, un tel procédé de déclarations « automatiques et objectives » n'est pas satisfaisant.

Le tableau ci-dessous propose une ventilation des natures d'opérations suspectes dans les dossiers transmis en 2022 par la CTIF.

Nature des opérations suspectes	% 2022
Transferts nationaux	33,6%
Transferts internationaux	31,7%
Retraits en espèces (en compte)	12,6%
Versements en espèces (en compte)	10,8%
Money remittance - envoi	2,5%
Money remittance - réception	0,9%
e-money	0,8%
Autres	7,2%
Total	***100%***

2.5 ASPECTS LIÉS AU FINANCEMENT DU TERRORISME

L'impact immédiat et le plus visible du terrorisme est bien entendu les atrocités commises causant le décès ou infligeant de graves blessures et traumatismes aux citoyens souvent visés au hasard par des actions aveugles. Au-delà de ces souffrances, le FMI considère l'impact du terrorisme comme une menace sur la stabilité financière d'une juridiction, du secteur financier et de l'économie au sens large, avec des effets durables sur l'infrastructure, le système financier. Par conséquent, le financement du terrorisme représente un risque pour la stabilité monétaire et financière des pays et devrait être traité comme une question macro-critique pour les économies. Pour les institutions financières en particulier, l'implication dans le financement du terrorisme génère un risque de réputation.

L'analyse des risques liés au financement du terrorisme n'est pas aisée pour une autorité en charge de la supervision des institutions financières. Les aspects liés au financement du terrorisme sont étroitement liés aux services de renseignements et aux analyses effectuées par l'OCAM et qui n'ont pas vocation à être partagées.

La BNB n'est pas impliquée dans les analyses de ces autorités. Il est par ailleurs à relever que, assez logiquement, le secret de l'instruction et la présomption d'innocence qui sont des garanties fondamentales dans un Etat de droit, ne permettent pas la communication systématique et rapide d'informations vers les institutions financières ni même vers les superviseurs.

L'inscription des personnes suspectées d'actes liés au terrorisme ou au financement du terrorisme sur les listes de « sanctions financières ciblées » fournit aux institutions financières un moyen d'action extrêmement utile mais qui ne peut être à lui seul totalement efficace.

Néanmoins, sur la base des échanges dans le cadre de l'Assemblée des partenaires, à la lecture de l'évaluation nationale des risques de terrorisme et de financement du terrorisme de 2017, des rapports annuels de la CTIF, des documents émis par Europol, ainsi que des informations recueillies en provenance de différentes sources scientifiques, il est possible de tirer divers enseignements concernant les activités liées au financement du terrorisme en Belgique.

Cinq « phénomènes terroristes » semblent pouvoir retenir l'attention en matière de financement du terrorisme en Belgique [16]:

- le fondamentalisme islamiste
- l'extrémisme de droite
- l'extrémiste de gauche et l'anarchisme
- le terrorisme lié à la situation politique d'un pays étranger (ethno-nationaliste et séparatiste)
- autre forme

2.5.1 FONDAMENTALISME ISLAMISTE

Les attentats du 11 septembre 2001 aux Etats Unis ont mis en lumière la structure tentaculaire du groupe Al Qaïda lequel a retenu l'attention des services de renseignement.

Durant la période 2015-2018, la Belgique a été particulièrement concernée par le financement du terrorisme fondamentaliste islamiste que ce soit dans le cadre attaques menées sur son territoire ou des attaques organisées à l'étranger depuis son territoire. En outre, un nombre conséquent de citoyens ou résidents belges ont rejoint les rangs des combattants ou sympathisants de Daesh (Etat islamique). La structure et le fonctionnement décentralisé de ce groupe a permis l'envoi de fonds vers un nombre important de personnes ou d'organisations au profit du groupe mais également au

16 European Union Terrorism Situation and Trend Report 2022 - Europol_TE-SAT_2023.pdf (europa.eu)

profit de ses combattants et sympathisants qui pouvaient ensuite les affecter au financement d'activités terroristes (achat d'armes, billets d'avions, moyens de subsistance, …).

Dans son Rapport annuel 2021, la CTIF indique que la tendance à la baisse de ces dernières années du nombre de dossiers transmis en raison d'indices sérieux de financement du terrorisme s'est également poursuivie en 2021. Les montants relatifs aux transmissions sont également limités.

Europol indique qu'une attaque liée au terrorisme islamique a été déjouée en Belgique en 2019 et une autre en 2020. On note que respectivement onze personnes en 2019, 2 personnes en 2020 et dix-huit personnes 2021 ont fait l'objet d'une arrestation judiciaire pour des motifs liés au terrorisme islamiste.

La grande majorité (340) des condamnations et des acquittements prononcée par les juridictions des États membres en 2021 pour toutes les infractions terroristes concernent le terrorisme djihadiste. A noter que la majorité des jugements et arrêts ont été rendus en Belgique et en France (100 et 83, respectivement). Il y a également lieu de prendre en compte le fait que des activités liées au financement du terrorisme peuvent être exercées en Belgique mais sont destinées à financer une action dans un autre pays. La CTIF indique à ce sujet dans le rapport du CTIF (2021) que le contenu d'une partie importante des déclarations de soupçon (22%), essentiellement reçues d'établissements de paiement agréés en Belgique pour des activités exercées dans l'EEE en libre prestation de services est externalisée vers des homologues européens de la CTIF.

La situation des *returnees* ou de leurs familles ainsi que les libérations dans un avenir plus ou proche de personnes condamnées pour terrorisme constituent un point d'attention majeur pour l'avenir.

Malgré ces chiffres relativement faibles, certains éléments ressortent de l'analyse des dossiers. Ils concernent, d'une part, la manière dont l'argent est transféré ou les techniques utilisées pour dissimuler les flux financiers et, d'autre part, une thématique commune à plusieurs dossiers.

La CTIF constate – à l'instar du blanchiment de capitaux – que les "nouveaux" systèmes de paiement en ligne proposés par les "néo-banques"[17], les fournisseurs de services de paiement (PSP) ou les fournisseurs de services d'actifs virtuels (VASP) sont plus fréquemment utilisés pour financer le terrorisme que les services bancaires traditionnels. Le caractère international et la rapidité avec laquelle les comptes sont ouverts et les transactions sont effectuées constituent un élément attractif. C'est particulièrement le cas lorsqu'il s'agit de financement du terrorisme, car les montants en jeu sont moins importants qu'en matière de blanchiment de capitaux. Cependant, l'impact du financement du terrorisme peut se révéler très important, même avec de petits montants comme les enquêtes consécutives aux attentats de Paris ou de Bruxelles l'ont démontré. L'approche fondée sur le risque des néo-banques et des PSP se base généralement sur l'importance des montants et, plus encore que pour le blanchiment de capitaux, elle est mise à rude épreuve lorsqu'il s'agit de traiter le financement du terrorisme compte tenu des faibles montants en jeu par transaction.

2.5.2 EXTRÉMISME DE DROITE

Depuis 2020, il est constaté une augmentation des dossiers liés à cette thématique, une tendance qui s'est poursuivie en 2021. En Belgique et en Europe, l'extrémisme de droite gagne en importance et en visibilité. Il s'agit de personnes et de groupes dont l'idéologie se fonde sur le racisme, le nationalisme et le totalitarisme. Cependant, avec les mouvements Alt-right aux États-Unis, le discours identitaire et les courants ultra-conservateurs en Russie et en Europe de l'Est, l'extrémisme de droite en Belgique et en Europe occidentale devient plus complexe à décrire, à analyser et à combattre qu'il y a 20 ans. Cette difficulté est renforcée par le fait qu'au contraire du terrorisme

[17] Les "néobanques" recourent à la technologie pour offrir des services bancaires de détail, principalement par le biais d'une application pour smartphone et d'une plateforme internet. Elles proposent une gamme de services comprenant des comptes chèques, des comptes de dépôt et des comptes d'entreprise, des cartes de crédit, des conseils financiers et des prêts.

fondamentaliste islamique, il n'existe pas d'organisation d'extrême droite de « référence » qui agirait comme le diffuseur de l'idéologie et qui capteraient l'essentiel des soutiens financiers.

Europol indique qu'une attaque liée au terrorisme d'extrême droite été déjouée en Belgique en 2020 et une autre en 2021. On note que respectivement 1 personne en 2020 et 3 personnes en 2021 ont fait l'objet d'une arrestation judiciaire pour des motifs liés au terrorisme d'extrême droite.

Outre l'application stricte du régime de gel de avoirs, une liste d'acronymes, logos, séries chiffrées pouvant servir de critères d'identification liés à l'idéologie a été établie. Ils peuvent être considérés comme des clignotants pour les établissements financiers s'ils apparaissent dans des dénominations, communications.

Il ne ressort pas des analyses étudiées que le financement du terrorisme d'extrême droite soit actuellement étroitement lié au blanchiment de capitaux. Il semble que les capitaux destinés au financement proviennent généralement des ressources personnelles légitimes des sympathisants de la cause (salaires, épargne, …), d'actions destinées à récolter des fonds, (concerts, …). Les réseaux sociaux constituent un canal pour « l'appel » des fonds. Les extrémistes de droite s'intéressent aussi aux crypto-monnaies. A priori, les activités ne nécessitent pas de voyages ou départ du pays (comme ce fut le cas vers le Syrie dans le cadre du financement de Daesh) étant donné que les éventuelles activités terroristes financées sont effectuées sur le territoire national. Seuls les liens et les transactions financières qu'entretiendrait un individu avec certaines associations ou sympathisants notoires pourraient être un signal d'alerte.

Il ressort par contre des travaux de la CTIF, qu'à plusieurs reprises, il a été constaté dans les dossiers que certaines organisations d'extrême-droite étaient financièrement liées à des homologues étrangers. Il a également été constaté que les organisations qui ont des méthodes de travail modernes et une très bonne compréhension des médias sociaux ont vu leur financement augmenter fortement ces dernières années.

Dans le cas des personnes physiques ayant une idéologie d'extrême droite, les analyses financières ont régulièrement révélé que des achats étaient effectués dans des boutiques en ligne étrangères qui ciblaient exclusivement les personnes ayant cette idéologie.

2.5.3 EXTRÉMISME DE GAUCHE ET ANARCHISME

L'extrémisme de gauche et l'anarchisme se manifestent en Europe par des destructions (incendies) ou des dégradations à des biens représentants une idéologie ou une activité contraire à la leur (installation 5G, agences bancaires, distributeurs de billets) ou à la divulgation des données sensibles concernant des personnes physiques ou morales.

Il ressort du Rapport 2022 d'Europol que six personnes liées au terrorisme d'extrême gauche et l'anarchisme ont été arrêtés en Belgique judiciairement en 2021.

Il ne ressort pas des analyses étudiées que le financement du terrorisme d'extrême gauche soit actuellement étroitement lié au blanchiment de capitaux. Il semble que les capitaux destinés au financement proviennent généralement des ressources personnelles légitimes des sympathisants de la cause (salaires, épargne, …), d'actions destinées à récolter des fonds, (concerts, …).

2.5.4 LE TERRORISME « ETHNO-NATIONALISTE ET SÉPARATISTE »

Le terrorisme « ethno-nationaliste et séparatiste » a constitué une menace importante dans un passé pas si lointain au sein de l'Union européenne, principalement par les activités des groupes tel que ETA (Espagne), IRA (Irlande du Nord). Leurs activités terroristes ont notablement diminué ces dernières années.

La Belgique peut être concernée, par exemple, par le terrorisme lié aux activités du PKK en Turquie d'une part par la présence d'une diaspora turque et d'autre part par la localisation en Belgique du European Kurdish Democratic Societies Congress (KCDK-E) qui constitue la branche politique du mouvement séparatiste kurde.

Deux personnes ont fait l'objet d'une arrestation judiciaire en 2019 en lien avec le terrorisme « ethno-nationaliste et séparatiste ».

2.5.5 AUTRES FORMES

Certains documents officiels[18] relèvent une menace liée à "l'écoterrorisme » qui est défini comme l'utilisation ou la menace d'utilisation de la violence de nature criminelle contre des personnes ou des biens, par un groupe infranational pour des raisons environnementales et politiques. Cette forme de terrorisme a été identifiée aux Etats Unis dès les années 1990. Certains mouvements sont classés sur la liste du terrorisme intérieur du FBI. Les actions visent la commission d'actes consistant en une dérive violente d'actions de contestations ou de désobéissance civile en faveur de la préservation de la planète ou de la sauvegarde des animaux. De telles actions violentes (attentats à la bombe, incendies) ont été constatées aux Etats Unis mais elles n'ont pas été identifiées en Belgique ni en Europe. Néanmoins une certaine radicalisation grandissante de certains discours et actions pourrait laisser croire qu'une menace potentielle pourrait voir le jour.

2.5.6 TENDANCE DE L'ACTIVITÉ LIÉE AU FINANCEMENT DU TERRORISME

La tendance à la baisse de ces dernières années du nombre de dossiers transmis à la CTIF en raison d'indices sérieux de financement du terrorisme s'est poursuivie en 2021. Les montants relatifs aux transmissions sont également limités. La baisse du nombre de dossiers n'implique néanmoins pas que la menace n'existe plus. En 2022, 215 signalements de menace en lien avec le terrorisme ou l'extrémisme ont été dénombrés dans notre pays. Ce chiffre est comparable à celui de l'année précédente. Il ressort également qu'entre le 1er janvier et le 30 avril 2023, trois projets d'attentats auraient été déjoués en Belgique.

Certains éléments communs marquants ressortent de l'analyse des dossiers faite par la CTIF comme décrit ci-avant.

Il a été démontré que les réseaux terroristes actifs en Belgique principalement durant la période 2015-2016 ont eu recours à l'argent liquide en raison de l'anonymat et l'absence d'expertise requise.

Il est à présent constaté – à l'instar du blanchiment de capitaux – que **les "nouveaux" moyens de paiement en ligne** proposés par les prestataires de services de paiement (PSP) sont de plus en plus utilisés pour financer le terrorisme.

Certains risques liés au financement du terrorisme semblent se déplacer d'activités « classiques » telles que les transferts de fonds, ou le recours à l'argent cash pour évoluer vers des produits et services plus nouveaux. Ainsi les activités « E-wallets » ou « **d'ibanisation** » qui se développent actuellement peuvent être attractives en termes de financement du terrorisme. Ces activités liées aux comptes de paiement libellés en diverses devises permettent aux clients d'ouvrir simultanément auprès d'un établissement financier, un ensemble de comptes identifiés par des IBAN's contenant des codes nationaux différents rendant dès lors difficile la traçabilité des opérations et l'identification de l'institution financière détenant les fonds et effectuant les opérations ordonnées par le client.

Le caractère international et la rapidité avec laquelle les comptes sont ouverts et les transactions sont effectuées constituent de nouveaux défis pour les Cellules de traitement des informations financières. C'est particulièrement le cas lorsqu'il s'agit de financement du terrorisme, car les

18 Europol – European Union Terrorism Situation and Trend Report 2022

montants en jeu sont moins importants qu'en matière de blanchiment de capitaux et sont dès lors plus difficilement détectables. Cependant, l'impact du financement du terrorisme peut se révéler très important, même avec de petits montants. L'approche fondée sur le risque de certaines institutions financières repose trop sur l'analyse des montants et volumes de transactions ce qui s'avère insuffisant particulièrement lorsqu'il s'agit de traiter le financement du terrorisme.

La transition vers les systèmes de paiement en ligne est aussi, en partie, la conséquence d'une certaine politique de '**de-risking'** de la part des banques traditionnelles. En conséquence, les comptes des clients à risques (membres de famille de personnes dont les avoirs sont gelés, ou de personnes dont le nom est cité dans une enquête) sont parfois clôturés. Cela rend non seulement le travail des cellules de traitement des informations financières et des services de renseignement plus difficile, mais incite également ces personnes à se tourner vers des institutions offrant des services en ligne, souvent établies à l'étranger. La piste financière dans leur propre pays s'arrête dès lors et il devient difficile de la suivre.

Les **actifs numériques** permettent d'acquérir anonymement des biens ou effectuer des transferts de fonds internationaux. Un client convertit ses fonds en actifs numériques, puis utilise la blockchain pour effectuer une transaction de pair à pair, avant de reconvertir les fonds en monnaie ayant cours légal. Ces fonds peuvent ensuite être retirés en espèces auprès d'un comptoir local ou d'une borne. L'acquisition de biens, armes, produits sur le « darknet » peut être payée en crypto assets.

Cependant, l'utilisation d'actifs numériques requiert des compétences spécifiques et une expertise technique qui freinent leur accès par les groupes criminels et groupements terroristes, même si ces actifs deviennent de plus en plus accessibles. L'importante volatilité des actifs numériques et le relatif manque de liquidité de certains d'entre eux limitent la possibilité de se servir des actifs numériques à des fins de blanchiment de capitaux ou de financement du terrorisme.

Il est néanmoins rappelé que la BNB n'exerce pas de compétence sur la supervision des plateformes utilisées dans la commercialisation des actifs virtuels.

L'utilisation des services bancaires classiques (comptes retails) reste toujours un possible vecteur de financement, du terrorisme par l'utilisation et le transfert de ressources personnelles des terroristes ou sympathisants de la cause.

2.6 PÉRIODE CONSIDÉRÉE

Au vu de la disponibilité des données relatives aux institutions dont la BNB a le contrôle, cette évaluation se base sur la situation telle qu'existante au 31 décembre 2022 et pourra faire l'objet d'une mise à jour sur la base d'un cycle de deux ans.

2.7 SCORING

Dans un premier temps, les « risques inhérents » afférents à chaque activité considérée sont évalués et quantifiés par l'attribution d'un score (de 1 à 5)[19] . Par « risque inhérent », on entend le risque que l'activité soit utilisée à des fins de blanchiment des capitaux en raison de sa nature et de ses caractéristiques objectives, abstraction faite des mesures qui peuvent être prises par les institutions financières pour réduire et gérer ces risques. Le niveau du risque inhérent d'une activité est également influencé par son importance relative dans le secteur financier belge.

Dans un deuxième temps, pour chaque activité, un score (de 1 à 5) concernant les vulnérabilités identifiées dans les institutions pratiquant ces activités est ensuite attribué. La notion de vulnérabilité doit être comprise comme le risque que les institutions financières exerçant l'activité concernée ne disposent pas d'une organisation et d'un contrôle interne adéquats ou de ressources suffisantes

[19] 1 = faible ; 2= modéré ; 3 = significatif, 4 élevé, 5 = critique

pour réduire et gérer les risques inhérents liés à cette activité. Ce score sera basé entre autres sur les différentes connaissances acquises par la BNB, notamment mais non exclusivement, au travers de la supervision 'hors-site »et des différentes inspections réalisées et des constats et recommandations y relatifs.

Les deux scores des activités évaluées sont ensuite reportés dans une matrice formant la base de l'évaluation globale pour l'ensemble du secteur, et qui détermine le « risque résiduel » afférent à chaque activité qui résulte de la combinaison du niveau de risque inhérent et du niveau de vulnérabilité. Ainsi, par exemple, une activité considérée comme présentant un risque inhérent élevé, mais une vulnérabilité basse peut se voir attribuer une notation de risque résiduel (« note globale ») plus basse qu'une activité présentant un risque inhérent moins élevé, mais une plus forte vulnérabilité.

3 ETABLISSEMENTS DE PAIEMENT ET DE MONNAIE ÉLECTRONIQUE

Six types d'activités spécifiques sont identifiées dans la présente section : (i) les activités de paiement traditionnelles, (ii) les activités de transfert de fonds, (iii) l'acquiring, iv) les services d'initiation de paiements, (v) les services d'information sur les comptes et (vi) les activités de monnaie électronique. Les nouveaux services liés aux comptes de paiement libellés en diverses devises seront abordés également.

Comme relevé au point n°2.4.1., le secteur des institutions de paiement et de monnaie électronique continue de connaitre de profondes modifications à la suite de l'arrivée d'une série de nouveaux acteurs sur le marché belge.

Le nombre d'établissement de paiement actifs et de monnaie électronique en Belgique a en effet fortement augmenté ces dernières années. Ce phénomène a été amplifié par le « Brexit » et la nécessité pour un certain nombres d'institutions britanniques de s'établir sur le continent pour y disposer d'un agrément permettant de « passeporter » leurs activités sur l'ensemble du territoire de l'EEE. Entre 2016 et 2021, plus d'une dizaine d'institutions ont été agréées par la BNB dans ce contexte. Pami elle des acteurs majeurs tels que MoneyGram International, WorldRemit Belgium, Ebury, PPS EU, Wise EU…).

L'évolution importante du nombre d'acteurs issus d'autres pays de l'EEE, combinée à la croissance significative d'acteurs proposant des produits en recourant à la libre prestation de services (LPS)[20], c'est-à-dire sans être établis en Belgique par le biais d'une succursale ou d'un réseau d'agent(s) et/ou distributeur(s), modifient profondément les dynamiques du secteur et ont une influence à la fois sur les modèles de propension aux risques et sur le degré de connaissance que peuvent avoir les institutions de paiement d'activités financières fragmentées en une multitude d'acteurs et de produits.

Notons qu'à l'exception d'institutions spécialisées dans une seule activité spécifique, comme celle d'agrégateur d'informations ou d'initiateur d'opérations, la majorité des institutions déclarent et pratiquent plusieurs activités de paiement simultanément ou en combinaison avec d'autres partenaires.

Il apparaît des reportings à la BNB que la majorité des établissements ayant précisé la nature des activités prestées au 31 décembre 2022 prestent, dans la pratique, des services de paiement qui ne sont pas ou peu diversifiés.

[20] La majorité de ces institutions proviennent du Royaume-Uni et des Pays Bas pour les institutions de paiement, et du Royaume-Uni, de Lituanie et de Chypre pour les institutions de monnaie électronique

3.1 SERVICES DE PAIEMENTS

3.1.1 DESCRIPTION DE L'ACTIVITÉ

Qu'entend-on par activité de paiement

Les services de paiement rassemblent différents types d'activités spécifiques que fournissent en globalité ou en partie les établissements de paiement et de monnaie électronique établis en Belgique (y compris les succursales EEE et non EEE) ainsi que les établissements de paiement et les établissements de monnaie électronique agréés dans d'autres États membres de l'Espace économique européen et établis en Belgique par le biais d'un ou plusieurs agent(s) et/ou distributeur(s).

Ces activités comprennent notamment :

1. Toutes les opérations qu'exige la gestion d'un compte de paiement (y compris les services permettant de verser des espèces sur un compte de paiement) ;
2. Les services permettant de retirer des espèces d'un compte de paiement ;
3. L'exécution d'opérations de paiement :
   - L'exécution de prélèvements, y compris de prélèvements autorisés unitairement ;
   - L'exécution d'opérations de paiement par le biais d'une carte de paiement ou d'un dispositif similaire,
   - L'exécution de virements, y compris d'ordres permanents ;
4. L'exécution d'opérations de paiement dans le cadre desquelles les fonds sont couverts par une ligne de crédit accordée à l'utilisateur de services de paiement :
   - L'exécution de prélèvements, y compris de prélèvements autorisés unitairement, ·
   - L'exécution d'opérations de paiement par le biais d'une carte de paiement ou d'un dispositif similaire,
   - L'exécution de virements, y compris d'ordres permanents ;
5. L'émission et/ou l'acquisition d'instruments de paiement ;
6. La transmission des fonds ;
7. Les services d'initiation de paiement ;
8. Les services d'information sur les comptes.

Les activités de transfert de fonds, d'initiation de paiement et d'information sur les comptes présentent des caractéristiques qui leur sont spécifiques du point de vue du risque de blanchiment de capitaux et de financement du terrorisme, ces risques font l'objet d'analyses distinctes

Même si les activités de paiement *stricto sensu* ont toujours été classiquement assumées par le secteur bancaire, la valeur ajoutée de ces services lorsqu'ils sont offerts par les établissements de paiement par rapport aux activités classiques bancaires réside à la fois et non exclusivement dans leur digitalisation, leur délai de transaction plus court, leur réseau d'intégration et de distribution mais également dans leur avantage concurrentiel en terme de marge de taux de change ou de frais de correspondance bancaire ou dans les services connexes non financiers qui sont liés aux produits de ces activités.

Que représente l'activité des établissements de paiement en Belgique

Au 31 décembre 2022, il existait 71 établissements agréés tombant sous le champ de la supervision LBC/FT de la BNB.

Ce chiffre se décompose en 34 établissements de paiement de droit belge agréés, 8 établissements de paiement relevant du droit d'un autre Etat membre de l'EEE et ayant une succursale en Belgique et 24 établissements déployant des activités en Belgique par le biais d'un établissement constitué

uniquement d'un ou plusieurs agents lesquels tombent sous la supervision de la BNB uniquement pour LBC/FT.

Il convient encore d'ajouter, les 5 établissements agréés en tant qu'établissement de monnaie électronique mais qui fournissent également des services de paiement et 1 appartenant à un autre Etat membre de l'EEE.

Outre les services de transmission de fonds (voir 3.2.) et de monnaie électronique (voir 3.6), les activités de paiement se concentrent en Belgique sur la mise à disposition de comptes et de moyens de paiement pour les particuliers et pour les entreprises d'une part et sur les terminaux de paiement et solutions de paiement en ligne à destination des professionnels d'autre part.

Par ailleurs, ces institutions proposent principalement leurs services en ligne, ou via un réseau d'agents/distributeurs, et ne disposent pas nécessairement d'établissements physiques sur le territoire.

Le nombre d'établissements de paiement actifs en Belgique a fortement augmenté ces dernières années. Ce phénomène a été amplifié par le « Brexit » et la nécessité pour un certain nombres d'institutions britanniques à s'établir sur le continent pour y disposer d'un agrément leur permettant d'exercer » leurs activités sur l'ensemble du territoire de l'EEE. Il a parfois été constaté que ces institutions déploient une structure minimaliste en Belgique sans y affecter les moyens de contrôles et humains suffisants et se reposant largement, via des accords d'externalisation de fonctions de LBC/FT, sur l'organisation en place au sein du groupe souvent localisé en dehors du territoire de l'EEE. Les inspections sur place et autres actions de contrôles menées par la BNB auprès de certains de ces établissements ont montré des lacunes dans la mise en œuvre d'un système LBC/FT répondant aux exigences légales et réglementaires belges.

3.1.2 RISQUES INHÉRENTS DE L'ACTIVITÉ

Dans la mesure où un grand nombre de produits différents sont catégorisés en tant qu'activités de paiement, il convient en premier lieu de dissocier les risques selon l'implication de l'institution dans la transaction : en effet un initiateur de paiement ou un agrégateur d'information n'est pas sujet aux mêmes risques que le service impliquant le versement/retrait d'espèces ou la transmission de fonds.

Le risque inhérent élevé associé aux établissements de paiement s'explique généralement par les **facteurs généraux** suivants :[21]

- le volume important et la grande rapidité des transactions dont le monitoring s'effectue principalement *a posteriori* sur la base de l'activité transactionnel du client ;
- le recours intensif à l'argent liquide ;
- la prévalence de transactions occasionnelles plutôt que de relations d'affaires établies et dès lors la plus faible connaissance du profil du client ;
- les corridors géographiques vers des juridictions à haut risque ;
- l'utilisation des nouvelles technologies pour faciliter l'intégration des clients à distance ;
- le canal de distribution utilisé. (via un réseau d'agents et de distributeurs).

Au niveau **des risques liés aux produits**, les activités de paiement permettent des transferts plus rapides et plus importants en termes de volume que pour d'autres produits financiers, les rendant ainsi particulièrement attractifs pour l'envoi massif de fonds provenant d'activités illégales.

Par ailleurs, les activités de paiement demeurent en majorité liées à l'utilisation de l'argent liquide. Ainsi, seules 35% des institutions de paiement offrant des services de paiement en Belgique, et

21 Ces facteurs de risqué généraux sont mentionnés depuis 2017 dans l'analyse supranationale des risques BC/FT de la Commission européenne et des les Opinions de l'EBA sur les facteurs de risqu BC/FT

ayant répondu au questionnaire, ne proposent pas de produits impliquant l'utilisation d'**espèces** (dépôt et/ou retrait).

Le secteur est également particulièrement affecté par **les risques transversaux** liés à la connaissance du client, de ses caractéristiques et de l'objet de la relation d'affaires, la digitalisation ou encore au réseau de distribution lorsque celui-ci implique des agents physiques non assujettis à la loi AML.

De nouveaux services liés aux comptes de paiement libellés en diverses devises (activité d'**ibanisation**) sont offerts par les établissements de paiement. Il s'agit plus particulièrement de l'émission et l'utilisation de numéros de comptes bancaires internationaux virtuels, également appelés IBAN virtuels uniquement destinés à réacheminer les paiements entrants vers un IBAN ordinaire lié à un compte bancaire physique. Ils complexifient l'identification et la localisation du compte sous-jacent. Ces services peuvent rendre plus difficile l'identification des transactions par les cellules de traitement des informations financières et semblent être attractifs pour la criminalité. Certains établissements de droit belge offrent ces comptes et services de paiement à destination des entreprises générant des montants importants. La présence d'établissements de droit belge très actifs dans ces activités renforce le risque pour le marché belge.

Un nouveau phénomène « **marque blanche** » est également identifié dans le secteur. Il consiste en la mise à disposition par des établissements de paiement de leur licence au profit d'agents indépendants qui développent leur propre produit sous la licence de l'institution financière réglementée. Il semble difficile pour les établissements réglementés d'intégrer correctement tous ces produits et les risques correspondants dans leur cadre de LBC/FT et de surveiller et contrôler de manière adéquate les risques découlant de ces activités (analyse globale des risques, surveillance des agents, suivi des transactions, etc.). La présence d'établissements de droit belge très actifs dans ces activités renforce également le risque pour le marché belge.

Au-delà des risques classiques de blanchiment, que connaissent également les activités de dépôt par exemple, le Supranational Risk Assessment (SNRA) identifie particulièrement le cas à haut risque où des services de paiement sont directement utilisés, détournés ou sont contrôlés par des organisations criminelles à des fins de blanchiment sans que les mesures adéquates de vigilance ne soient mises en œuvre dans un délai raisonnable pour intervenir promptement.

Le risque inhérent des activités de paiement est très variable en fonction des caractéristiques des produits et des modalités de distribution. Sans préjudice de l'évaluation individuelle du risque inhérent associé individuellement à chaque établissement, le niveau moyen de ce risque est conséquemment évalué comme élevé (4 sur 5).

3.1.3 VULNÉRABILITÉS DES INSTITUTIONS PRATIQUANT L'ACTIVITÉ

Même si le secteur est composé d'institutions aux profils et activités hétérogènes (TPE ou grande entreprise au sein d'un groupe financier d'ampleur mondiale), les vulnérabilités des institutions identifiées par la BNB, que ce soit au travers de sa supervision off-site ou des inspections réalisées sur place, se concentrent fréquemment, mais non exclusivement, sur :

- le manque de volonté d'établir en Belgique d'une structure autonome des entités du groupe situées hors de l'Union européenne ;
- un manque d'expérience et de formation pertinente et continue des dirigeants et/ou du personnel en matière de AML/CFT ;
- le turn over important du personnel en matière AML/CFT et la difficulté rencontrée par le secteur en Belgique pour recruter du personnel disposant de la connaissance de la matière ;
- une inadéquation d'un cadre préventif (procédures, outils de monitoring automatisés non-satisfaisants) ;

- un manque de connaissance approfondie du cadre légal et réglementaire belge en matière de prévention du BC/FT ainsi que du régime des sanctions et embargos;
- une non-application des dispositions légales par une absence de contrôles relatifs aux PEPs
- une mauvaise organisation des trois lignes de défense en matière d'AML : certaines fonctions externalisées n'étaient pas assez encadrées ou correctement diligentées ; le cadre procédural n'était pas totalement adapté à la réglementation belge ; et sa mise en œuvre n'était pas suffisamment efficiente ;
- le connaissance des clients repose principalement sur l'analyse a posteriori de son activité transactionnelle et le déclenchement des alertes est essentiellement basé sur le dépassement de seuils sans tenir suffisamment compte du comportement transactionnel du client ;
- la faiblesse de l'analyse relative à l'origine des fonds du client ;
- la faiblesse des moyens consacrés à la supervision du réseau de distribution, qu'il soit digital ou qu'il s'agisse de points de vente.

Certains de ces constats ont été confirmés à l'occasion d'inspections sur site réalisées par la BNB.

Comme indiqué supra 2.4.13, le secteur peut être exposé à la criminalité liée aux activités du port d'Anvers.

En outre, l'industrie du diamant est particulièrement importante en Belgique. Elle constitue un secteur d'activité à haut risque BC/FT. Il apparaît qu'à la suite de décisions de de-risking prises par certains établissements de crédit, des entreprises actives dans l'industrie du diamant se sont tournées vers des établissement de paiement offrant à leur clientèle des comptes de paiement parfois libellés en différentes devises ce qui peut compliquer la traçabilité des transactions.

En conséquence, sans préjudice de l'évaluation individuelle de la vulnérabilité de chaque établissement, le niveau moyen des vulnérabilités des institutions de paiement sous contrôle de la BNB sont évaluées comme élevées 4 sur 5), en fonction de leur nature, des caractéristiques de leurs produits et de leurs réseaux de distribution.

3.1.4 SCORE GLOBAL DE L'ACTIVITÉ

Au vu des risques inhérents significatifs liés aux activités de paiements et des vulnérabilités importantes des institutions proposant ces produits, les risques résiduels relatifs au blanchiment *via* des activités de paiement sont, en général, considérés comme élevés (4 sur 5).

3.1.5 CONCERNANT LE FINANCEMENT DU TERRORISME

Risque inhérent :

Plus spécifiquement en matière financement du terrorisme, le secteur des établissements de paiement peut être attractif de par la rapidité des transactions essentiellement internationales en ce compris vers des pays à haut risque.

Il est également constaté (voyez notamment le rapport annuel de la CTIF 2021) que les "nouveaux" services de paiement, particulièrement ceux proposés en ligne par les établissements de paiement pourraient être utilisés pour financer un groupe ou une action terrorisme. Tel est notamment le cas des services permettant l'ouverture de comptes en différentes devises.

Le caractère international et la rapidité avec laquelle les comptes sont ouverts et les transactions sont effectuées peuvent les rendre attractifs pour les criminels. C'est particulièrement le cas lorsqu'il s'agit de financement du terrorisme, car les montants en jeu sont moins importants qu'en matière de blanchiment de capitaux.

Le risque inhérent de financement du terrorisme lié à l'activité peut être considéré comme élevé et quantifié par un score de 4 sur 5.

Vulnérabilité :

L'approche fondée sur le risque appliquée par ces établissements se base généralement sur le volume et le montant des transactions, alors qu'il a été constaté durant la période 2015-2018 que des attaques terroristes ont été financées par diverses opérations de faibles montants.

La réglementation impose aux institutions d'établir un profil du client prenant en compte toutes les caractéristiques du client et qui n'est pas uniquement basé sur l'activité transactionnelle. La pratique montre que c'est n'est pas toujours le cas.

Les vulnérabilités de financement du terrorisme liées à l'activité peuvent être considérées comme élevées et quantifiées par un score de 4 sur 5.

Risque résiduel :

Le risque résiduel de financement du terrorisme lié à l'activité peut être considéré comme élevé et quantifié par un score de 4 sur 5.

3.2 ACTIVITÉS DE TRANSFERT DE FONDS

3.2.1 DESCRIPTION DE L'ACTIVITÉ

L'activité de transfert de fonds consiste en un service de paiement pour lequel les fonds sont reçus de la part d'un payeur, sans création de comptes de paiement au nom du payeur ou du bénéficiaire, à la seule fin de transférer un montant correspondant vers un bénéficiaire ou un autre prestataire de services de paiement agissant pour le compte du bénéficiaire, et/ou pour lequel de tels fonds sont reçus pour le compte du bénéficiaire et mis à la disposition de celui-ci ».[22]

L'élément distinctif des autres activités de paiement est que ce transfert s'opère sans qu'il y ait nécessairement création d'un compte au nom du bénéficiaire et/ou de l'émetteur du transfert.

L'activité de transmission de fonds s'adresse principalement aux particuliers même si certains produits sont spécifiquement proposés aux entreprises et professionnels dans la mesure où ils offrent parfois certains avantages par rapport à une correspondance bancaire plus classique.

De par leur vaste réseau d'agents et de points de vente de proximité en Belgique à l'étranger, les activités de transfert de fonds permettent de toucher un public mondial dans des pays ou des zones où les institutions financières sont peu ou pas présentes. L'activité présente un intérêt sociétal certain dans la mesure où l'immense majorité des transferts effectués par les membres de la diaspora ont pour objet une assistance familiale.

Compte tenu de leur facilité d'accès, de la rapidité du transfert et des tarifs attractifs, les institutions de transfert de fonds entendent capter une clientèle qui ne se tournerait pas naturellement vers une banque classique pour obtenir ce type de services.

Il y a lieu de relever la présence d'établissements de droit belge d'importance sur le marché mondial offrant des services de transferts de fonds essentiellement en argent liquide (Moneygram International) et également uniquement par le canal digital (WorldRemit).

---

22 Article 4, n°22 de la Directive 2015/2366

Parmi les institutions de paiement soumises au contrôle de la BNB, 15 institutions ont déclaré avoir une activité de transfert de fonds au 31 décembre 2022. [23]

Les transferts de fonds initiés depuis la Belgique représentent annuellement un montant supérieur à 1 milliard d'euros dont près de la moitié effectués en argent liquide. Près de la moitié du volume de transferts de fonds était à destination d'un pays considéré comme à haut risque.

Les principaux corridors de transferts de fonds en Belgique sont à destination du Maroc et de la République démocratique du Congo. Pour les paiements entrants, il s'agit du Congo, et du Cameroun. Ces volumes se justifient par la présence d'une large diaspora présente en Belgique. Les autres principaux pays à risque d'où proviennent ou sont envoyés les fonds sont l'Afghanistan, la Cote d'Ivoire, la Tunisie, et la Turquie.

Une grande majorité d'institutions en Belgique acceptent l'argent liquide comme moyen d'effectuer des transferts et la plupart opèrent à la fois en ligne mais également via un réseau d'un nombre important d'agents non exclusifs composés majoritairement de commerces de détail.

3.2.2 RISQUES INHÉRENTS DE L'ACTIVITÉ

Les activités de transferts de fonds demeurent en majorité liées à l'utilisation de l'argent liquide.

Néanmoins, même si l'utilisation d'argent liquide reste majoritaire, les acteurs traditionnels les plus importants actifs en Belgique développent et encouragent (réduction des f*ees*) l'utilisation d'applications digitales permettant les transferts de fonds.

Certaines institutions recourent uniquement à ce canal de distribution digital. Bien que l'absence d'argent liquide diminue le risque inhérent, l'absence de contacts lors de l'entrée en relation d'affaires et des faiblesses dans les méthodes d'onboarding à distance créant ainsi la possibilité pour un même client de créer plusieurs profils (doublons) peuvent augmenter le risque.

Les activités de transfert de fonds sont par nature moins enclines à assurer une connaissance efficace des activités des clients non seulement pour détecter le dépassement du caractère occasionnel des transactions qui caractérise le modèle d'affaires, mais davantage encore par la caractéristique fondamentale liée à l'absence de comptes. : Les modalités d'identification , de vérification de l'identité et des caractéristiques du client sont d'autant plus importantes lorsque le transfert est effectué en provenance ou en destination d'un pays à risque.

Au niveau du risque produit, les services de transmission de fonds demeurent intrinsèquement liés à l'utilisation de l'argent liquide, s'adressant par nature à des profils peu ou pas bancarisés. Le risque produit est donc important s'agissant de la transmission de fonds.

Au niveau du risque géographique, il apparait que les services de transferts de fonds s'adressent principalement à des personnes en relation avec des pays considérés comme à haut risque en matière de blanchiment. L'activité de transfert de fonds se trouve ainsi souvent liée à un risque géographique important et un transfert de fonds dans un pays dans lequel coexistent des systèmes informels de transmission de fonds constitue en effet un risque additionnel et donc un attrait complémentaire pour des processus de blanchiment.

---

[23] Notons bien que les établissements de crédit détiennent également la possibilité d'effectuer des transferts de fonds mais qu'en pratique, cette activité est pour ces institutions dans la majeure partie liée à la création d'un compte, ce qui ne rencontre pas la définition d'un transfert de fonds tel que nous le concevons dans cette analyse.

Par ailleurs, les activités de transferts de fonds s'adressant également à des clientèles issues de secteurs de l'économie illégale ou connues pour leurs risques de blanchiment, rendent le risque lié au client plus important.

Les établissements de paiement sont exposés au risque fraude et notamment via l'utilisation de « mules financières » utilisées par la criminalité comme un maillon de la phase de la dispersion des capitaux issus de la fraude. Le recours à des mules permettant le transfert de fonds issus de fraudes a été identifié en Belgique dans le cadre de diverses fraudes (romance, phishing, …).

Il y a également lieu de relever la disparité des risques encourus entre les différentes institutions au sein de ce même secteur en raison de la disparité des produits et services offerts.

Au vu de ces considérations le risque inhérent lié à l'activité de transfert de fonds par les institutions de paiement est considéré comme élevé. (4,5 sur 5).

3.2.3 VULNÉRABILITÉS DES INSTITUTIONS PRATIQUANT CETTE ACTIVITÉ

Il y a, à nouveau, lieu d'indiquer que le secteur est composé d'institutions aux profils et activités hétérogènes (TPE ou grande entreprise au sein d'un groupe financier d'ampleur mondiale).

Les actions de contrôle ont permis de constater que certaines institutions déploient une structure minimaliste en Belgique se reposant largement sur l'organisation en place en sein du groupe fréquemment situé en dehors du territoire de l'EEE.

Les inspections sur place et autres actions de contrôles menées par la BNB auprès de certains de ces établissements ont parfois montré des lacunes graves dans la mise en œuvre d'un système LBC/FT répondant aux exigences légales et réglementaires

Au niveau du risque de distribution, les services de transmission de fonds s'appuient principalement sur des réseaux de distribution de proximité, composés majoritairement de commerces de détails qui n'offrent pas les garanties nécessaires à la bonne application des prescrits légaux de la règlementation AML. Ces agents offrent bien souvent les services de plusieurs établissements. Toutes les institutions soumises au contrôle de la BNB qui pratiquent l'activité sont des PME (- 250 ETP) mais certaines d'entre elles s'appuient sur un réseau de plus de 2.500 agents/distributeurs qui sont en majorité non exclusifs et peuvent donc proposer plusieurs produits concurrents. Ces agents ne sont, dans leur immense majorité, pas soumis à une supervision ni à une quelconque déontologie ou règles professionnelles organisées. Il ressort en outre d'informations recueillies par la BNB, que le crime organisé tente de s'insérer dans le secteur par le biais d'agents agissant de concert avec le crime organisé soit volontairement soit à la suite de contraintes (chantage, …). Le crime organisé pourrait utiliser leur position, leurs accès à l'information et aux systèmes pour effectuer des transactions liées au blanchiment de capitaux.

La surveillance et les récentes inspections auprès des institutions de paiement impliquées dans la transmission de fonds ont permis de relever les vulnérabilités suivantes :

- le manque de volonté d'établir en Belgique d'une structure autonome des entités du groupe situées hors de l'Union européenne ;
- un manque d'expérience et de formation pertinente et continue des dirigeants et/ou du personnel en matière de AML/CFT ;
- le *turn over* important du personnel en matière AML/CFT et la difficulté rencontrée par le secteur en Belgique pour recruter du personnel ;
- une mauvaise organisation des trois lignes de défense en matière d'AML : certaines fonctions externalisées n'étaient pas assez encadrées ou correctement diligentées ;
- une inadéquation d'un cadre préventif (procédures, outils de monitoring automatisés non-satisfaisants) ;

- une analyse globale des risques incomplète ne prenant pas en compte les risques présentés par de nouveaux produits ou des risques géographiques précis ;
- un manque de connaissance approfondie du cadre légal et réglementaire belge en matière de prévention du BC/FT ainsi que du régime des sanctions et embargos ;
- la faiblesse dans les méthodes d'entrée en relations d'affaires à distance ;
- la connaissance du client repose principalement sur l'analyse ex post de son activité transactionnelle ;
- le déclenchement des alertes essentiellement basé sur le dépassement de seuils sans tenir suffisamment compte du comportement transactionnel du client ;
- le manque d'analyse quant à l'origine des fonds du client ;
- une inadéquation des moyens consacrés à la supervision du réseau de distribution : qu'il soit digital ou qu'il s'agisse de points de vente physiques ;
- une supervision du réseau d'agents insuffisante : soit par manque de moyens humains et/ou matériels dédiés à la formation et au contrôle soit par une inadaptation des mesures de monitoring par l'institution ;
- le fait que de nombreux agents sont non exclusifs affaiblit également la capacité des établissements de paiement de contrôler la globalité des activités de transferts de fonds exercées par ces agents et permet à ceux-ci de diviser des opérations de transferts portant sur des montants importants en opérations de montants plus faibles opérées par les différents transmetteurs de fonds qu'ils représentent ;
- une surveillance pas suffisamment approfondie des transactions réalisées par les agents en nom propre.

Certains constats ont été confirmés à l'occasion d'inspections on-site réalisées par la BNB.

La surveillance continue et les inspections ponctuelles ont notamment permis une amélioration dans les modes de déclarations à la CTIF et des systèmes de contrôle relatifs à la prévention du risque de blanchiment. Néanmoins, la très forte augmentation des déclarations d'opérations suspectes effectuées par les établissements de paiement (+ de 300%) semble trouver en partie une explication par le fait que certains établissements de paiement ont procédé à des déclarations en se fondant sur le dépassement de seuils de montant des transactions. Un tel procédé n'est pas satisfaisant.

En conclusion les vulnérabilités des institutions pratiquant le transfert de fonds aux risques de blanchiment sont considérées comme élevées (4 sur 5).

3.2.4 SCORE GLOBAL DE L'ACTIVITÉ

En fonction du risque inhérent élevé (4,5 sur 5) pour les activités de transfert de fonds, et de l'identification de vulnérabilités élevées (4 sur 5), le risque résiduel est considéré comme élevé (4,5 sur 5

3.2.5 CONCERNANT LE FINANCEMENT DU TERRORISME

Risque inhérent :

Plus spécifiquement concernant le financement du terrorisme en Belgique, il a été établi que certaines attaques terroristes menées en ou largement organisées et préparées depuis la Belgique entre 2015 et 2018 ont été financées par diverses transactions de transferts de fonds portant généralement sur de faibles montants et par divers intervenants, présentant parfois un lien de parenté rendant dès lors plus difficile l'identification des transactions.

Selon Europol, les acteurs djihadistes recourent aux services de transfert de d'argent soit directement soit par l'intermédiaire des « mules » financières. Les mules constituent un maillon

important de ces réseaux, car elles agissent comme intermédiaires et collecteurs d'espèces au nom du destinataire final. Il a également été constaté que des intermédiaires retirent de l'argent de services de transferts dans des lieux situés en dehors de l'UE et à proximité de zones de conflit, où l'argent est ensuite acheminé et remis aux destinataires.

Les produits et services sont attractifs notamment de par la rapidité des transactions internationales et la possibilité de fractionner les transferts que ce soit au sein d'une même marque commerciale ou auprès de plusieurs.

Le risque inhérent de financement du terrorisme lié à l'activité peut être considéré comme élevé et quantifié par un score de 4 sur 5.

Vulnérabilité :

Bien que les principaux acteurs du secteur aient développé, après les premiers attentats de 2015, des scenarios de monitoring destinés à identifier/limiter les transferts de fonds vers la zone frontalière de la Turquie avec la Syrie, il est apparu que certains agents n'ont pas agi avec la vigilance suffisante en se satisfaisant d'une justification de l'opération fondée sur l'achat de médicaments ou d'un lien familial non établi.

A ce jour, les actions de contrôle auprès des établissements de paiement n'ont pas mis en évidence de manquement lié au respect des sanctions, gels des avoirs et embargos.

Les vulnérabilités de financement du terrorisme liées à l'activité peuvent être considérées comme élevées et quantifiées par un score de 4 sur 5.

Risque résiduel :

Le risque résiduel de financement du terrorisme lié à l'activité peut être considéré comme élevé et quantifié par un score de 4 sur 5.

3.3 ACTIVITÉ D'AQUIRING

3.3.1 DESCRIPTION DE L'ACTIVITÉ

Les activités d'acquisition ou acquiring désignent les diverses activités associées à la réalisation d'opérations au sein de réseaux de paiement et permettant d'autoriser des transactions dans les points de vente ou sur des sites marchands. Le rôle de l'acquirer vise à faciliter ou procéder à la compensation et au règlement des transactions.

L'activité en Belgique

Actuellement, 4 établissements présentent une offre spécialisée dans ce service parmi les établissements belges de paiement offrant des services d'initiation de paiements. Le marché belge est néanmoins caractérisé par la présence d'acteurs importants sur le marché international offrant les services liés aux activités exercées par des points de vente ou par des sites marchands. Il est à noter que certains établissements de crédit exercent également l'activité.

3.3.2 RISQUES INHERENTS DE L'ACTIVITÉ

L'activité d'acquiring présente certains risques de blanchiment de capitaux.

Concernant le risque lié aux produits, il est relevé qu'ils permettent la réalisation de transactions financières pouvant être transfrontalières et portant sur des montants pouvant être importants.

L'acquisition par des tiers commerçants a été identifiée comme une tendance émergente engendrant un nouveau risque de blanchiment de capitaux lié aux établissements de paiement. L'acquéreur marchand qui est l'entité fournissant des services de paiements aux commerçants sous-traite certaines parties du processus d'acquisition à un tiers acquéreur (TPA). Le tiers acquéreur expose l'acquéreur au risque de traiter indirectement des fonds illicites s'il devait s'avérer que le cadre mis en place n'est pas satisfaisant.

L'absence de connaissance adéquate ou de mise à jour de cette connaissance des activités réelle du client exploitant un point de vente muni d'un terminal de paiement ou un site marchand constitue un risque. Il se pourrait qu'elle ne soit pas conforme à celle déclarée lors de l'entrée en relations d'affaires ou que cette activité soit modifiée par la suite.

Certains secteurs d'activités des clients sont identifiés comme présentant un risque élevé comme par exemple, les secteurs « réservés aux adultes », le gaming, gambling, tabac ou certains produits pharmaceutiques.

L'envoi ou réception de fonds associés à des contreparties établies dans des « pays tiers à haut risque » est possible.

Certains travaux internationaux font état du développement d'une activité consistant en la location « privée » d'ATM permettant des retraits d'argent liquide. Une telle activité qui n'est actuellement pas autorisée en Belgique présenterait des risques en ce sens qu'elle permettrait au locataire de l'ATM de recharger l'appareil avec des fonds provenant d'activités illégale.

Néanmoins, la matérialisation de ces risques est considérée comme étant modérée. Au vu de ces considérations le risque inhérent lié à l'activité d'acquiring est considéré comme modéré (2 sur 5).

3.3.3 VULNÉRABILITÉS

Les établissements dans ce segment doivent s'assurer que l'activité du client (c'est-à-dire le commerçant ou le site transactionnel) est toujours celle prise en compte au moment de l'entrée en relation d'affaires. Ils doivent également s'assurer que le volume de transactions est en adéquation avec le profil et l'activité attendue du client.

Les entreprises doivent également pouvoir vérifier régulièrement l'identité des UBO du client. Les entités sont sujettes au risque de ne pas détecter suffisamment rapidement des modifications d'UBO qui contrôlent ces activités.

Nonobstant l'intervention de l'acquirer dans la chaine des opérations de paiement, l'institution financière auprès de laquelle les comptes de paiement mouvementés sont ouverts exerce également une vigilance sur les clients dont ils peuvent avoir une meilleure connaissance et sur leurs transactions ce qui vient mitiger le risque

En conclusion les vulnérabilités des institutions pratiquant l'activité d'acquiring aux risques de blanchiment sont considérées comme modérées (2 sur 5).

3.3.4 SCORE GLOBAL DE L'ACTIVITÉ

En fonction du risque inhérent modéré (2 sur 5) pour les activités d'acquiring, et de l'identification de vulnérabilités modérées (2 sur 5), le risque résiduel est considéré comme modéré (2 sur 5).

3.3.5 CONCERNANT LE FINANCEMENT DU TERRORISME

Risque inhérent :

Plus spécifiquement concernant le financement du terrorisme, il n'apparaît pas que l'activité d'acquiring présente un risque particulier. L'utilisation des services d'acquiring aux fins du financement d'une activité terroriste demande des connaissances et nécessite un ensemble de démarches et la mise en place d'une structure, ce qui ne semble pas concorder avec les menaces actuellement liées au financement du terrorisme en Belgique.

Le risque inhérent de financement du terrorisme lié à l'activité peut être considéré comme faible et quantifié par un score de 1,5 sur 5.

Vulnérabilité :

Les vulnérabilités de financement du terrorisme liées à l'activité peuvent être considérées comme faibles et quantifiées par un score de 1,5 sur 5.

Risque résiduel :

Le risque résiduel de financement du terrorisme lié à l'activité peut être considéré comme faible et quantifié par un score de 1,5 sur 5.

3.4 ACTIVITÉS D'INITIATION DE PAIEMENT

3.4.1 DESCRIPTION DE L'ACTIVITÉ

L'activité d'initiation de paiement consiste à donner ordre, au nom d'une autre personne, à l'institution financière auprès de laquelle cette autre personne dispose d'un compte de paiement, d'exécuter des paiements à partir de ce compte dont l'initiateur de paiement n'est pas lui-même titulaire.

Ce service peut être offert dans le cadre d'une relation d'affaires nouée par le « prestataires de services d'initiation de paiement » (PSIP ou PISP en anglais) avec un commerçant (exerçant le plus souvent une activité de commerce sur internet), dans le but de faciliter les paiements par les clients de ce commerçant du prix de leurs achats, et de lui offrir ainsi la garantie que ces paiements seront effectivement exécutés. Dans ce cas, il n'existe aucune relation d'affaires avec les clients du commerçant, et celui-ci est le seul bénéficiaire potentiel des paiement initiés par le PISP.

Ce service peut cependant aussi être offert par le PSIP à une personne qui est titulaire du ou des comptes au départ desquels les paiements seront initiés, et viser à faciliter les paiements à effectuer par cette personne au départ de ce ou ces comptes. Dans ce cas, les paiements sont effectués au bénéfice d'une gamme extrêmement large de bénéficiaires avec lesquels le PSIP n'entretient pas de relation d'affaires. Le service permet l'initiation de paiements dont les motivations ne sont pas nécessairement liées aux activités professionnelles des bénéficiaires et ne sont pas connues du PSIP.

Ce service peut être offert par l'ensemble des prestataires de services de paiement (établissements de crédit, établissements de paiement, établissements de monnaie électronique), auquel cas ce service complète la gamme des services qu'ils offrent à leurs clients. Il peut cependant aussi être offert par des établissements de paiement spécialisés exerçant cette seule activité.

L'activité en Belgique

Actuellement, parmi les 9 établissements belges de paiement offrant des services d'initiation de paiement, seuls 4 établissements présentent une offre spécialisée dans ce service, en combinaison avec le service d'information sur les comptes (cf. chapitre 3.5 infra), mais sans offrir simultanément l'ouverture de comptes de paiement, de services de crédit ou de services d'émission d'instruments de paiement. Seuls ces derniers sont considérés et qualifiés de PSIP dans le présent chapitre.

3.4.2 RISQUES INHERENTS DE L'ACTIVITÉ

Les établissements de paiement qui ne fournissent que le service d'initiation de paiement, présentent des risques faibles dans la mesure où ce service est limité à l'exécution d'une opération de paiement pour le compte d'un client. Ces prestataires ne détiennent à aucun moment de fonds de la clientèle.

L'activité de PSIP n'est cependant pas dénuée de tout risque de blanchiment de capitaux.

On peut relever des risques liés au produit dans la mesure où ils permettent des transferts de fonds, provenant de différents comptes de paiement et envoyés à une même personne et dont la somme représente un volume important sans avoir nécessairement de justification économique.

Il est possible d'initier des paiements au profit d'une très large gamme de bénéficiaires et sans pouvoir en connaître la motivation lorsque le service est offert aux titulaires des comptes de paiement concernés.

L'envoi ou la réception de fonds associés à des contreparties établies dans des « pays tiers à haut risque constitue un risque géographique.

Il est toutefois relevé :

- que le PSIP n'entre à aucun instant en possession des fonds appartenant au titulaire des comptes de paiement mouvementés ;
- que l'intervention du PSIP ne fait nullement obstacle à l'exercice des devoirs de vigilance (notamment le monitoring des opérations) de l'institution financière auprès de laquelle le compte de paiement mouvementé est ouvert.

Au vu de ces considérations le risque inhérent lié à l'activité d'initiation de paiement est considéré comme faible (1,5 sur 5).

3.4.3 VULNÉRABILITÉ DES INSTITUTIONS PRATIQUANT CETTE ACTIVITÉ

Une certaine vulnérabilité des PSIP au blanchiment de capitaux doit être reconnue du fait notamment de ce que :

- contrairement à l'institution financière auprès de laquelle le compte mouvementé est ouvert, le PSIP ne dispose pas d'informations complètes couvrant l'ensemble des opérations effectuées sur le compte de paiement mouvementé, mais uniquement celles de ces opérations qu'il a lui-même initiées ;
- les activités de PSIP sont fréquemment développées par de petites entreprises focalisées essentiellement sur le développement de solutions technologiques nouvelles et qui ne disposent pas nécessairement d'une connaissance approfondie du cadre légal et réglementaire belge en matière de prévention du blanchiment.

Inversement, lorsque le service d'initiation de paiement est offert dans le contexte d'une relation d'affaires conclue avec le commerçant, le PSIP est en mesure de s'assurer de la cohérence des paiements initiés avec le profil du commerçant et de ses activités commerciales.

En conclusion les vulnérabilités des institutions pratiquant l'activité d'initiation de paiement aux risques de blanchiment sont considérées comme modérées (2,5 sur 5).

3.4.4 SCORE GLOBAL DE L'ACTIVITÉ

Nonobstant un niveau faible du risque inhérent (1,5 sur 5) associé aux activités d'initiation de paiement, le niveau modéré de vulnérabilités (2,5 sur 5) permet de considérer que le risque résiduel est modéré (2 sur 5).

3.4.5 CONCERNANT LE FINANCEMENT DU TERRORISME

Plus spécifiquement concernant le financement du terrorisme, il peut être constaté au regard des développements ci-dessus, que l'activité n'engendre pas de risque particulier dans la mesure où les institutions concernées ne détiennent pas de fonds des clients. Néanmoins par leurs activités, elles pourraient avoir une vue plus complète sur l'activité d'un individu aux départs de plusieurs comptes.

Le risque résiduel de financement du terrorisme lié à l'activité peut être considéré comme faible et quantifié par un score de 1,5 sur 5.

3.5 SERVICES D'INFORMATION SUR LES COMPTES

3.5.1 DESCRIPTION DE L'ACTIVITÉ

L'activité de services d'information sur les comptes consistent en des services permettant au client de regrouper sur une seule interface les informations relatives aux soldes et opérations réalisées auprès de plusieurs établissements.

Les agrégateurs de compte (« Account Information Service Providers » ou « AISP ») peuvent offrir ce service comme activité principale ou comme activité auxiliaire.

L'activité en Belgique

Outre les quatre établissements belges de paiement offrant les services d'agrégation de comptes en combinaison avec la seule activité d'initiation de paiements, seules trois sociétés sont agréées en Belgique pour offrir exclusivement le service d'agrégation de comptes.

3.5.2 RISQUES INHERENTS DE L'ACTIVITÉ

L'activité d'agrégation de compte n'inclut aucune intervention quelconque dans l'exécution des opérations du client, ni n'amène, a fortiori, l'agrégateur à entrer en possession des fonds appartenant au client. Le service d'agrégation des informations sur les comptes ne porte aucun préjudice à la capacité des institutions financières à remplir leurs obligations de vigilance à l'égard des opérations effectuées sur les comptes concernés. Dès lors, aucun risque lié au blanchiment de capitaux n'est identifié.

3.5.3 VULNÉRABILITÉ DES INSTITUTIONS PRATIQUANT CETTE ACTIVITÉ

Dès lors qu'aucun risque inhérent ne peut être identifié, l'évaluation de la vulnérabilité de ces opérateurs est non pertinente.

3.5.4 SCORE GLOBAL DE L'ACTIVITÉ

Au vu de l'absence de risque et de vulnérabilités, le score global de l'activité d'information sur les comptes est nul.

3.5.5 CONCERNANT LE FINANCEMENT DU TERRORISME

Plus spécifiquement concernant le financement du terrorisme, il peut être constaté au regard des développements ci-dessus, que l'activité n'engendre pas de risque particulier.

3.6 LA MONNAIE ÉLECTRONIQUE

3.6.1 DESCRIPTION DE L'ACTIVITÉ

La monnaie électronique[24], est une valeur monétaire qui est stockée sous une forme électronique, y compris magnétique, représentant une créance sur l'émetteur, qui est émise contre la remise de fonds aux fins d'opérations de paiement au sens du 22° du présent article et qui est acceptée par une personne physique ou morale autre que l'émetteur de monnaie électronique.

Plusieurs distinctions peuvent être opérées au niveau des modalités des produits proposés dans le cadre de cette activité : des cartes et portefeuilles électroniques servant à effectuer des paiements dans un réseau d'acceptation limité comme une ou plusieurs enseignes commerciales, aux cartes de crédit prépayées.

Toutefois, les activités de monnaie électronique impliquent, selon des seuils d'usage différents, un chargement par l'utilisateur (ou un tiers) de la monnaie électronique par le biais d'un dépôt d'espèces sur un support électronique (matériel ou logiciel) et des applications de paiements incluant, généralement, le retrait d'argent liquide.

L'activité en Belgique

Le nombre d'établissements de paiement et de monnaie électronique sous supervision AML/CFT de la BNB diminue. Au 31 décembre 2022, le champ de contrôle de la BNB pour les établissements de monnaie électronique était composé de cinq institutions de droit belge pour la monnaie électronique, un établissement de monnaie électronique relevant du droit d'un autre Etat membre de l'EEE ayant une succursale enregistrée en Belgique, et six établissements de monnaie électronique relevant du droit d'un autre Etat membre de l'EEE qui prestent en Belgique sous le régime de la libre prestation de services avec un agent et/ou un distributeur.

Le montant de monnaie électronique émis en Belgique par les institutions soumises au contrôle de la BNB au titre de l'activité était d'environ 350 millions d'euros, et seule une institution offrait la possibilité d'utiliser un crédit/rechargement par un tiers.

Ces institutions, en plus de proposer l'émission de monnaie électronique, offrent également des services de paiement, et sont ainsi soumises aux mêmes risques dont il est question au point n°3.1, dont le retrait et le versement d'espèces. De plus, les produits proposés sont également de plus en plus digitalisés et s'adressent aussi bien aux particuliers qu'aux entreprises.

---

[24] Article 2,77° de Loi du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique, à l'accès à l'activité de prestataire de services de paiement, et à l'activité d'émission de monnaie électronique, et à l'accès aux systèmes de paiement

L'activité sur le marché belge est caractérisée par le fait que certains établissements de monnaie électronique ont développé un *business model* dans lequel les agents/distributeurs sont en général des sociétés qui développent une activité autonome nécessitant l'utilisation de solutions de paiement et de monnaie électronique. Ne possédant pas l'agrément requis pour émettre de la monnaie électronique et offrir des services de paiement, ces agents/distributeurs sollicitent l'établissement de monnaie électronique agréé afin d'intégrer les solutions de paiement et de monnaie électronique dans le cadre de leur activité.

Dans la mesure où les clients de l'établissement de monnaie électronique rentrent principalement en relation d'affaires avec lui en vue de bénéficier des services offerts par l'agent/distributeur, les risques associés auxdits clients varient nécessairement en fonction de l'activité exercée par ailleurs par l'agent/distributeur concerné. La structure de ce business model implique donc qu'une attention particulière soit accordée par l'établissement de monnaie électronique aux risques liés à l'ensemble des activités développées, par chaque agent/distributeur et dans le cadre desquelles la monnaie électronique est distribuée et les services de paiement offerts.

3.6.2 RISQUES INHÉRENTS DE L'ACTIVITÉ

L'activité liée à la monnaie électronique est particulièrement soumise au risque d'identification des caractéristiques des clients, que ce soit par le biais de produits anonymisés ou via le recours à des hommes de paille. La digitalisation a également amplifié ce processus dans la mesure où le recours à des mules bancaires virtuelles permet dorénavant d'envisager plus simplement des opérations massives de blanchiment via des moyens électroniques selon le schéma suivant : le recours à de nombreux sites marchands (réels ou fictifs) permet d'écouler une monnaie électronique chargée depuis de l'argent liquide provenant d'opérations illégales.

Les produits de l'activité de monnaie électronique demeurent en effet soumis au risque transversal lié à l'argent liquide, soit qu'il soit possible de créditer de la monnaie électronique par de l'argent liquide, soit que le produit permette le retrait d'argent liquide sur un vaste réseau de terminaux partout dans le monde. Les criminels désireux de blanchir un argent liquide vont en effet continuer à préférer des produits recourant à l'argent liquide et privilégieront d'ailleurs les produits pouvant être achetés/rechargés par argent liquide de même que ceux permettant le retrait en Belgique ou ailleurs dans le monde. De plus, par rapport à l'argent liquide, la monnaie électronique présente la caractéristique complémentaire d'être dématérialisée, donc plus facilement transportable et/ou transmissible à un tiers.

Notons toutefois qu'en sus des seuils d'utilisation anonyme, limités légalement à 150 euros la relative traçabilité de la monnaie électronique, depuis son émission jusqu'à sa distribution en passant par son usage, constitue un facteur potentiel de diminution relative de risques contrairement à d'autres activités de paiement impliquant le recours à de l'espèce liquide intraçable par définition.

Outre la possibilité de retrait d'argent liquide, et en dehors de la problématique relativement limitée des produits anonymes, le risque principal de l'activité de monnaie électronique est donc qu'elle soit utilisée comme un simple medium d'un processus de blanchiment plus vaste.

Le risque inhérent des activités de monnaie électronique est donc jugé faible par nature quand il n'implique pas d'argent liquide, mais potentiellement plus significatif dans la mesure où cette activité est souvent distribuée parallèlement à d'autres services de paiement plus sujets à risques en fonction de leur nature et de leur mode de distribution (2,5 sur 5).

3.6.3 VULNÉRABILITÉS DES INSTITUTIONS PRATIQUANT CETTE ACTIVITÉ

Comme relevé dans l'Analyse supranationale des risques BC/FT de nombreux cas de blanchiment via des cartes prépayées ont été relevés par les forces de police, et le recours à des agents/distributeurs est parfois privilégié aux hommes de paille jugés plus couteux. Il demeure que ce phénomène de mules est de nouveau rendu possible par la digitalisation et les moyens électroniques.

Dans la mesure où les activités de monnaie électronique sont généralement distribuées via un réseau d'agents physiques dont certains sont non assujettis en tant que tels à la loi AML, la supervision du réseau d'agents devient fondamentale. Elle doit être mise en œuvre dès l'onboarding des agents et porter ensuite sur le monitoring des activités. La formation des agents doit également être un point d'attention.

Les autres acteurs présents en Belgique ont toutefois développé des systèmes de contrôle, depuis l'acquisition jusqu'à l'usage, qui font l'objet d'une évaluation constituée d'une supervision permanente ainsi que d'inspections thématiques ponctuelles visant à s'assurer notamment de l'adéquation des mesures de gestion des risques aux défis du blanchiment. Cette double supervision n'a pas amené à relever d'anomalies majeures dans le fonctionnement des institutions de paiement, s'agissant des activités de paiement

La surveillance continue et les récentes inspections auprès des institutions de paiement impliquées dans l'émission de monnaie électroniques ont permis de relever les vulnérabilités suivantes :

- le manque de volonté d'établir en Belgique d'une structure autonome des entités du groupe situées hors de l'UE ;
- un manque d'expérience et de formation pertinente et continue des dirigeants et/ou du personnel en matière de AML/CFT ;
- le *turn over* important du personnel en matière AML/CFT et la difficulté rencontrée par le secteur en Belgique pour recruter du personnel ;
- une mauvaise organisation des trois lignes de défense en matière de prévention du BC/FT: Certaines fonctions externalisées n'étaient pas assez encadrées ou correctement diligentées ;
- une inadéquation d'un cadre préventif (procédures, outils de monitoring automatisés non-satisfaisants) ;
- une analyse globale des risques incomplète ne prenant pas en compte les risques présentés par de nouveaux produits ou des risques géographiques précis ;
- le manque de maîtrise par l'entité supervisée de certains produits développés par ses agents ;
- la connaissance du client repose principalement sur l'analyse a posteriori de son activité transactionnelle ;
- un manque de connaissance approfondie du cadre légal et réglementaire belge en matière de prévention du BC/FT ainsi que du régime des sanctions et embargos ;
- le déclenchement des alertes essentiellement basé sur le dépassement de seuils sans tenir suffisamment compte du comportement transactionnel du client ;
- le manque d'analyse quant à l'origine des fonds du client ;
- une supervision du réseau d'agents insuffisante, soit par manque de moyens humains et/ou matériels dédiés à la formation et au contrôle soit par une inadaptation des mesures de monitoring par l'institution.

Les vulnérabilités relevées ci-dessus ne concernant pas l'ensemble des institutions pratiquant l'émission de monnaie électronique mais certaines présentant un business model particulier fondé sur le recours à des agents/distributeurs. Dès lors, globalement, les vulnérabilités peuvent être considérées comme significatives (3 sur 5).

3.6.4 SCORE GLOBAL DE L'ACTIVITÉ

Comme relevé dans les orientations de l'EBA du 1er mars 2021 sur les facteurs de risque BC/FT, *« le niveau de risque de BC/FT associé à la monnaie électronique dépend in fine principalement des caractéristiques des différents produits de monnaie électronique et de la mesure dans laquelle les émetteurs de monnaie électronique ont recours à d'autres personnes agissant pour leur compte pour distribuer et rembourser de la monnaie électronique* ».

Au vu des considérations du marché belge en la matière, le risque résiduel des activités de monnaie électronique va de modéré à significatif, en fonction principalement des caractéristiques et modalités propres des produits proposés et des caractéristiques des institutions et de leurs modes de distribution. Le risque résiduel est modéré 2,5 sur 5).

3.6.5 CONCERNANT LE FINANCEMENT DU TERRORISME

Risques inhérents :

Plus spécifiquement en matière financement du terrorisme, le secteur des établissements de monnaie électronique peut être attractif de par la rapidité des transactions essentiellement internationales en ce compris vers des pays à haut risque et la difficulté pour les institutions d'établir un profil du client autrement basé que sur l'activité transactionnelle. Le caractère international et la rapidité avec laquelle les comptes sont ouverts et les transactions sont effectuées peuvent les rendre attractifs pour les criminels. C'est particulièrement le cas lorsqu'il s'agit de financement du terrorisme, car les montants en jeu sont moins importants qu'en matière de blanchiment de capitaux.

Le risque inhérent de financement du terrorisme lié à l'activité peut être considéré comme significatif et quantifié par un score de 3 sur 5.

Vulnérabilités :

L'approche fondée sur le risque appliquée par ces établissements se base généralement sur le volume et le montant des transactions, alors qu'il a été constaté durant la période 2015-2018 que certaines attaques terroristes ont été financées par diverses opérations de faibles montants.

Les vulnérabilités de financement du terrorisme liées à l'activité peuvent être considérées comme significatives et quantifiées par un score de 3 sur 5.

Risque résiduel :

Le risque de financement du terrorisme lié à l'activité peut être considéré comme significatif et quantifié par un score de 3 sur 5.

4 ETABLISSEMENTS DE CRÉDIT

On relève 30 établissements de crédit de droit belge, 45 établissements de crédit relevant du droit d'un autre Etat membre de l'Espace économique européen ayant une succursale enregistrée en Belgique et 5 succursales des établissements de crédit relevant du droit d'un Etat non-membre de l'Espace économique européen.

Le marché belge est caractérisé par la présence d'un certain nombre de banques « universelles » offrant un ensemble extrêmement large de produits et de services tant à destination de la clientèle privée qu'à destination des entreprises. D'autres établissements de crédit offrent uniquement des services plus restreints et spécialisés à destination d'une clientèle ciblée.

Pour les établissements de crédit disposant de l'agrément, neuf types d'activités sont à prévoir.

4.1 ACTIVITÉS DE PRIVATE BANKING

4.1.1 DESCRIPTION DE L'ACTIVITÉ

Il s'agit des prestations délivrées par un organisme financier, et caractérisées

- d'une part, par la détention des avoirs et la gestion d'un patrimoine ou de ressources économiques d'un client portant sur des montants supérieurs à un certain seuil défini à un niveau généralement élevé. Il est utile de relever la distinction d'une part, entre la gestion discrétionnaire pour laquelle la banque reçoit mandat de décider des opérations de gestion du portefeuille en fonction d'un objectif et d'une politique d'investissement et, d'autre part, la "gestion conseil" par laquelle le client conserve le pouvoir de décider des opérations de gestion du portefeuille ;
- d'autre part, par une offre de services, de produits et de conseils spécifiques adaptée au profil spécifique de chaque client.

La gestion de fortune peut offrir les services et produits suivants (liste non exhaustive) :

- des services bancaires (ouverture de compte, crédits dont le crédit lombard) ;
- des services d'investissement (conseils en investissements, gestion de portefeuille) ;
- des produits d'assurance-vie ;
- l'ingénierie patrimoniale, les conseils en cession d'entreprise,…

L'activité en Belgique

Cette activité est proposée en Belgique tant par des divisions spécialisées des grandes banques universelles (BNPPF, ING, KBC, Belfius, …) ou par des établissements de crédit de droit belge spécialisés dans le domaine (Banque Degroof Petercam, Delen Private Bank…) ou encore par des succursales belges d'établissements relevant du droit d'un autre Etat membre de l'EEE (ABN Amro, Deutsche Bank, Puilaetco, Edmond de Rothschild, …). A noter que cette activité peut également être exercée par des sociétés de bourse (Capitalatwork, Leleux, …), et que les éléments repris dans le présent chapitre leur sont dès lors également applicables.

Il s'agit d'une activité très importante en Belgique, estimée en 2022 à 454 MM d'euros d'actifs gérés.

4.1.2 RISQUES INHÉRENTS DE L'ACTIVITÉ

Il s'agit d'une activité particulièrement sensible, du fait du risque lié à la gestion de patrimoines importants dont il est parfois difficile de connaître l'origine, de la discrétion requise par certains titulaires de grandes fortunes, ou encore des rapatriements de fonds liés à la transparence fiscale qui a été rendue obligatoire ces dernières années au sein de l'Union Européenne par la voie de Directives.

En outre, les montants en jeu sont généralement importants et peuvent permettre la dissimulation de fonds d'origine illicite parmi des fonds d'origine licite, ce qui peut complexifier l'émergence de soupçons.

L'activité se caractérise également par la recherche pour le client de conseils en optimisation fiscale parfois agressifs et qui pourraient viser la mise en place de mécanismes particuliers de type

« Cum/Cum et Cum/Ex[25] » entraînant en outre des risques de réputation pour les institutions financières.

Citons également parmi les risques inhérents liés aux produits :

- la fréquence et l'importance des mouvements transfrontaliers ;
- des structures patrimoniales complexes présentes dans des pays avec un régime fiscal avantageux;
- le manque de transparence de l'origine des fonds et le difficulté dans certains cas d'identifier les bénéficiaires économiques ultimes.

Une fois l'origine des fonds clarifiée, le risque inhérent diminue de manière drastique, les opérations de gestion étant initiées par l'institution financière elle-même, en exécution de son mandat, raison pour laquelle l'essentiel des efforts de vigilance doit être fourni lors des entrées de fonds, et concernent prioritairement la justification de leur origine et la cohérence de celle-ci avec les caractéristiques du client, en ce compris l'étendue et l'origine de son patrimoine.

Citons également parmi les risques inhérents liés aux clients et aux produits :

- caractéristiques liées aux clients :
  - les clients disposant de revenus et/ou d'un patrimoine issus de secteurs économiques à risque élevé (l'armement, la construction, les jeux d'argent, les industries extractives, le secteur diamantaire) ;
  - les clients ayant fait l'objet d'allégations crédibles d'infractions ;
  - les clients exigeant un niveau de confidentialité ou de discrétion inhabituel, notamment au niveau de l'origine des fonds (cf. supra) ;
  - les clients dont le niveau de transactions ne correspond pas à leur profil (notamment l'étendue de leur patrimoine) ;
  - les clients très fortunés et influents ;
  - les clients non-résidents et les PPE.
- la demande de montants importants en espèces ou en métaux précieux ;
- les arrangements financiers impliquant des pays ou des territoires associés à un risque plus élevé de BC/FT ;
- l'utilisation de structures commerciales complexes, comme les trusts ou les fiducies. Cela semble assez peu pratiqué en Belgique ;
- les activités commerciales exercées dans plusieurs pays ;
- les arrangements transfrontaliers, pouvant inclure des pays ou territoires non coopératifs ;
- les produits favorisant l'anonymat.

Compte tenu de qui précède, le score en matière de risques inhérents peut être fixé à 3,5 sur 5 (significatif).

---

25 Le Cum/Cum (arbitrage de dividendes) consiste pour un investisseur étranger à revendre ses actions à une banque d'un certain pays qui touche, elle, les dividendes avant imposition. La banque bénéficie ensuite du remboursement par le fisc de l'impôt sur les dividendes et rétribue, moyennant une commission, les dividendes touchés à l'investisseur. Le Cum/Ex consiste à déclarer des dividendes sur des sociétés dont les actions sont échangées à haute fréquence entre plusieurs établissements bancaires mondiaux qui vont tous se déclarer propriétaires dans leur pays et bénéficiaires des dividendes associés

4.1.3 VULNÉRABILITÉS DES INSTITUTIONS PRATIQUANT CETTE ACTIVITÉ

Néanmoins, les vulnérabilités détectées sont les suivantes :

- la recherche d'objectifs commerciaux et une culture inadéquate de contrôle en matière AML/CFT, qui peut être liée aux liens particuliers tissés entre les chargés de relation et leur clientèle ;
- les exigences de connaissances techniques et réglementaires pointues en matière LBC/FT et en fiscalité.
- la mise en œuvre de ressources insuffisantes pour ce faire, car le contrôle en matière AML/CFT a souvent la réputation de coûter de l'argent et non d'en rapporter, et d'entrer en conflit avec les impératifs commerciaux ;
- les problèmes liés aux échanges d'information intra groupe lorsqu'une même personne est cliente de plusieurs entités du même groupe (ce qui semble parfois poser problème pour certains pays tiers) ;
- la difficulté pour identifier les bénéficiaires économiques ultimes ;
- la difficulté de s'assurer de l'origine des fonds notamment au moment d'opérations liées au rapatriement de fonds organisés par la législation belge (DLU). ;
- le monitoring des transactions inadéquat.

Des mesures peuvent être mises en place afin de limiter ces risques, comme :

- le renforcement des mesures de vigilance lorsque le client ou son bénéficiaire effectif est un PPE ou est situé dans un pays à risque ;
- la mise en place d'une politique de LBC/FT au niveau du groupe ;
- le renforcement des mesures de vigilance pour les rapatriements de fonds depuis l'étranger ;
- les exigences issues de la Directive européenne sur les marchés d'instruments financiers (MiFid) et particulièrement les exigences liées à l'identification du client.

Compte tenu de ce qui précède, la vulnérabilité peut être estimée élevée (4 sur 5).

4.1.4 SCORE GLOBAL DE L'ACTIVITÉ

Le Score global de risque résiduel de blanchiment de capitaux de l'activité est de 4 (risque élevé).

4.1.5 CONCERNANT LE FINANCEMENT DU TERRORISME

Risques inhérents :

Spécifiquement concernant le financement du terrorisme, il ne semble pas qu'un lien soit établi entre l'activité de « private banking » et le financement du terrorisme. L'entrée en relations d'affaires est soumise à des conditions assez strictes notamment en termes de montants des investissements demandés la rendant dès lors peu attractive pour les personnes impliquées dans le financement du terrorisme. En outre, l'activité ne se prête pas aux transferts rapides des sommes investies au profit d'autres personnes impliquées.

Le risque inhérent de financement du terrorisme lié à l'activité peut être considéré comme faible et quantifié par un score de 1,5 sur 5.

Vulnérabilités :

Il n'y a pas de vulnérabilités spécifiques renvoyant au financement du terrorisme autres que celles identifiées ci-dessus.

Les vulnérabilités de financement du terrorisme liées à l'activité peuvent être considérées comme modérées et quantifiées par un score de 2 sur 5.

Risque résiduel :

Le risque lié à l'activité peut être considéré comme faible et quantifié par un score de 1,5 sur 5.

4.2 ACTIVITÉ DE RETAIL BANKING

4.2.1 DESCRIPTION DE L'ACTIVITÉ

Les banques de détail proposent un large éventail de services comme des comptes à vue et d'épargne, des services de paiement (virements, prélèvements, cartes bancaires, …), des crédits (crédits à la consommation, crédits hypothécaires, …) et ce à destination de clients particuliers ou de petites et moyennes entreprises.

L'activité en Belgique

Les banques de détail sont très présentes en Belgique, qu'il s'agisse de banques de droit belge ou de succursales belges de banques étrangères (essentiellement EEE). Cela va des grandes banques universelles à des banques de petite taille en passant par des établissements de taille intermédiaire (Argenta, Crelan).

La concurrence est dès lors très forte, et se caractérise :

- par des marges sous pression, dans un contexte de taux d'intérêt restés bas durant de nombreuses années ;
- par une digitalisation croissante et une réduction drastique du nombre d'agences bancaires.

4.2.2 RISQUES INHÉRENTS DE L'ACTIVITÉ

L'activité retail se caractérise par le très grand nombre de clients concernés et par l'exécution pour ces clients d'un très grand nombre d'opérations (notamment de paiement) portant sur des montants très variables parmi lesquelles il peut être malaisé de repérer les opérations susceptibles d'être liées au blanchiment de capitaux. L'activité se caractérise également par une grande diversité de profils des clients en ce compris des clients présentant des risques particuliers liés à leur profession. En revanche, d'une part, ces opérations sont exécutées dans le cadre de relations d'affaires souvent durables permettant, en principe, à la banque de disposer d'une connaissance relativement détaillée des clients, en ce compris l'origine des fonds, devant permettre plus aisément la détection d'opérations atypiques. D'autre part, les facteurs risques de blanchiment associés aux opérations retail sont relativement bien connus de longue date, ce qui est également de nature à réduire le risque inhérent associé à cette activité.

Dans ce contexte, les banques de détail sont notamment soumises au risque d'utilisation du cash (cf. les dépôts/retraits en espèces), et dans une moindre mesure des produits favorisant l'anonymat (mais ce risque est désormais plutôt réduit en Belgique, sauf dans quelques cas de figure comme par exemple, le remboursement de prêts par des tiers non préalablement identifiés). Le risque lié à la digitalisation et à ses conséquences pratiques (comme l'identification à distance) est par ailleurs en croissance rapide.

Constituent ainsi des facteurs du risque inhérent associé à cette activité :

- l'activité professionnelle du client ;
- l'accessibilité et le caractère très répandu de l'offre de comptes bancaires ;

- la nature des produits et services proposés dont le retrait d'argent liquide ;
- les modalités pour créditer des comptes (question de la traçabilité des dépôts d'espèces) ;
- l'exposition au risque transfrontalier ;
- l'utilisation de technologies nouvelles pour des produits pas toujours bien maîtrisés ;
- l'ouverture d'un compte bancaire sur la base de faux documents ;
- fraude via l'utilisation de « mules financières » utilisées par la criminalité comme un maillon de la phase de la dispersion des capitaux issus de la fraude.

Le risque inhérent peut être classé comme modéré et un score de 2,5 sur 5 lui est attribué.

4.2.3 VULNÉRABILITÉS DES INSTITUTIONS PRATIQUANT CETTE ACTIVITÉ

Les principales vulnérabilités auxquelles les banques de détail semblent être soumises sont les suivantes :

- la mise en place de ressources insuffisantes, notamment sur le plan informatique et sur le plan des effectifs, pour contrôler un flux d'informations (KYC) et de transactions qui peut s'avérer extrêmement important ;
- la difficulté d'obtenir une vue exacte du profil du client ayant recours à divers produits et services ;
- la difficulté de connaître les UBO quand il s'agit de clients personnes morales et d'intégrer cette information dans le système de monitoring des opérations ;
- le recours à des systèmes informatisés suffisamment robustes et le cas échéant interconnectés de manière à ce que l'informations circulent correctement entre les deux premières lignes de défense et qu'ils ne permettent pas de déroger aux mesures adoptés (limitation des produits…) ;
- le volume important des transactions qui doivent être surveillées ;
- le recours à des systèmes de monitoring automatisé basés sur des modèles, fondements et qui ne sont pas totalement maîtrisés (black box) ou dont les mises à jour ne sont pas suffisantes pour tenir compte de l'évolution des risques ou des nouvelles tendances ;
- des procédures et systèmes informatisés suffisamment performants que pour conserver adéquatement les informations relatives aux clients et qu'elles puissent être disponibles ;
- le nombre potentiellement élevé d'opérations atypiques ;
- la mise en place de mécanismes limitant le nombre d'alertes à traiter par l'AMLCO ;
- le recours à du personnel pour la Compliance présentant un profil « Junior » ou ne possédant pas d'expérience dans la matière AML/CFT.

La vulnérabilité peut être considérée comme modérée et quantifiée par un score de 2,5 sur 5.

4.2.4 SCORE GLOBAL DE L'ACTIVITÉ

Le score global de risque résiduel de blanchiment de capitaux peut être fixé à 2,5 sur 5 (risque modéré).

4.2.5 CONCERNANT LE FINANCEMENT DU TERRORISME

Risque inhérent :

Plus spécifiquement concernant le financement du terrorisme, l'accessibilité des comptes bancaires et de paiement à l'immense majorité des citoyens exposent les institutions à des risques de financement du terrorisme. En effet, des fonds peuvent transiter sur un compte avant de servir à financer un groupe ou une action terroriste, par exemple pour financer le départ de combattants vers

des zones de conflits, financer des actions terroristes sur le territoire national, ou vers des zones limitrophes de zones de conflit.

Il n'est pas aisé pour les institutions financières de mettre en œuvre dans les systèmes de monitoring des scenarios adéquats et suffisamment granulaires pour identifier des opérations atypiques pouvant être liées au financement du terrorisme parmi la masse des transactions quotidiennes. En outre, afin d'éviter d'attirer l'attention et de tomber dans le champ de scenarios de monitoring, les sommes transférées restent généralement inférieures à 1000 EUR. Comme l'indique Europol, le «smurfing»[26] reste une pratique courante.

L'application sans faille des obligations liées au régime des sanctions est impérative. Des actions de contrôle menées ont mis en évidence des disfonctionnement temporaires des systèmes permettant le screening des clients et des contreparties par rapport aux listes de sanctions.

Il ressort également des tendances actuelles qu'un certain nombre d'actions terroristes sont financées par les revenus des personnes impliquées qui les affectent, notamment via leur compte bancaire, aux activités terroristes. L'utilisation des services bancaires classiques (comptes retail) reste donc toujours un possible vecteur de financement, par l'utilisation et le transfert de ressources personnelles des terroristes ou sympathisants de la cause.

Le crédit à la consommation non affecté au financement d'une dépense particulière peut être utilisé aux fins de de financement du terrorisme lorsqu'il est de montant faible et que les sommes peuvent être retirées en espèces

Le risque inhérent de financement du terrorisme lié à l'activité peut être considéré comme élevé et quantifié par un score de 4 sur 5.

Vulnérabilités :

Outre les vulnérabilités mentionnées ci-dessus, il apparaît que la faiblesse des montants des transactions à identifier parmi un volume global extrêmement important de transactions compliquent le monitoring et l'identification des transactions suspectes. L'onboarding à distance de plus en plus répandu permettent, dans certains cas, l'usurpation d'identité.

Les vulnérabilités de financement du terrorisme liées à l'activité peuvent être considérées comme élevées et quantifiées par un score de 4 sur 5.

Risque résiduel :

Le risque de financement du terrorisme lié à l'activité peut être considéré comme élevé et quantifié par un score de 4 sur 5.

4.3 ACTIVITÉ DE CORPORATE BANKING

4.3.1 DESCRIPTION DE L'ACTIVITÉ

L'activité de Corporate banking consiste en des services bancaires aux entreprises comme les services :

- de financement (sous forme de prêts, crédits de trésorerie/découverts, crédits d'investissement hors crédit-bail, affacturage et crédits immobiliers, escomptes, refinancement de factures, cessions de créances professionnelles);
- de paiement;

[26] Transaction split.

- de garde;
- d'épargne (compte épargne, compte à terme) et placement.

L'activité en Belgique

Le service de Corporate Banking est principalement fourni par deux types d'institutions en Belgique: les grandes banques universelles et une vingtaine de filiales ou succursales des institutions étrangères dont certaines localisées dans des pays présentant un risque plus élevé, qui ont été créées afin de supporter les activités de leurs entreprises domestiques à l'étranger (en Belgique ou en Europe).

Le recours à la sous-traitance est possible pour les fonctions annexes comme l'IT ou la comptabilité. Pour des établissements de petite taille comme les filiales et succursales, ne permettant pas d'internaliser les fonctions d'audit interne et de Compliance, la sous-traitance peut s'étendre à ces fonctions. En toute hypothèse, la sous-traitance ne peut pas s'étendre aux éléments essentiels des activités dont l'exercice requiert un agrément.

4.3.2 RISQUES INHÉRENTS DE L'ACTIVITÉ

Les services bancaires aux entreprises connaissent les risques inhérents suivants :

- En ce qui concerne les crédits aux entreprises :
  - interposition d'une personne morale en tant que débiteur : elle peut permettre d'occulter l'origine illicite des fonds servant au remboursement du crédit et elle ouvre la possibilité que les opérations soient "pilotées" par les bénéficiaires effectifs du client ;
  - risque de fraude documentaire donnant une vision inexacte de la situation comptable de l'entreprise et pouvant ainsi favoriser la commission d'infractions (organisation frauduleuse d'insolvabilité, abus de biens sociaux) ;
  - octroi de crédits à des entreprises dont la situation est fortement compromise ou en procédure collective ou à des sociétés « dormantes » réactivées à des fins criminelles ;
  - refinancement de fausses créances qui n'ont pas pour origine la livraison de biens ou de services : l'établissement achète une créance qui ne correspond à aucune livraison effective de biens ou de prestation de service et règle le créancier, qui reçoit des fonds d'un organisme financier. Celui-ci est ensuite payé par le débiteur sur la base d'une fausse créance, au moyen de fonds d'origine douteuse, qui sont ainsi blanchis ;
  - sous-facturation ou surfacturation permettant à l'acheteur et au vendeur, de récupérer un montant supérieur à la valeur des biens ou services fournis : la valeur supplémentaire est transmise par l'acheteur au vendeur en cas de sous-facturation ou par le vendeur à l'acheteur en cas de surfacturation (« trade based money laundering »). Sont notamment sensibles le secteur de la construction et des travaux publics et de l'import/export lié ou non à des marchés publics dans des pays émergents, pour lesquels il existe un risque de délit sous-jacent, lié à la corruption ou à la prise illégale d'intérêts ;
  - la possibilité d'utiliser des fonds d'origine douteuse pour rembourser le prêt, en particulier lorsque le client opère dans des secteurs avec un risque de blanchiment de capitaux important caractérisé par une forte utilisation des espèces ;
  - un recours excessif à l'endettement peut être un moyen d'organiser frauduleusement son insolvabilité. Une entreprise peut se porter caution pour le prêt accordé à une autre entreprise ou à une personne physique (chef d'entreprise), ce qui peut être constitutif d'un abus de biens sociaux.

- En ce qui concerne le leasing:
  - le recours au leasing peut permettre à des criminels d'acquérir des actifs mobiliers matériels d'une valeur significativement élevée (voitures de luxe par exemple) en évitant

d'avoir à acheter le bien et ainsi de justifier de l'origine des fonds correspondant au prix d'acquisition du bien.

Compte tenu de qui précède, le score en matière de risques inhérents peut être fixé à 3 sur 5 (significatif).

4.3.3 VULNÉRABILITÉS DES INSTITUTIONS PRATIQUANT CETTE ACTIVITÉ

Le marché belge se caractérise par la présence de succursales importantes d'établissements situés dans ou hors de l'EEE. Il a dans certains cas été constaté une grande dépendance aux outils développés par le groupe dont, dans certains cas, la maison mère est située dans un pays considéré comme à haut risque de BC/FT et qui ne prennent pas nécessairement en considération les spécificités de l'activité déployée en Belgique. Ces outils doivent en outre être suffisamment performants.

Il a été relevé un *turn over* du personnel impliqués dans LBC/FT dans certaines de ces institutions.

Il est parfois relevé une difficulté dans certains cas d'identifier les bénéficiaires économiques ultimes et d'intégrer cette information de manière utile dans les mécanismes de détection et d'analyse des opérations atypiques.

L'utilisation des nouvelles technologies et la relation commerciale développée à distance (*non face to face*) constituent une vulnérabilité.

Actions prises par les institutions :

- les institutions financières actives dans ce secteur sont en général bien informées des risques liés au blanchiment de capitaux ;
- de moins en moins de banques s'intéressent au segment des entreprises actives dans les secteurs sensibles comme le secteur diamantaire. Les dernières années, les entreprises actives dans le secteur diamantaire ont dû chercher un fournisseur de service dédié, du fait d'un certain de-risking ;
- en général, les institutions financières n'offrent plus des services aux entreprises qui sont organisées comme trust.

La vulnérabilité est considérée comme modérée et est quantifiée par un score de 2 sur 5.

4.3.4 SCORE GLOBAL DE L'ACTIVITÉ

Le secteur de corporate banking est considéré comme présentant un risque résiduel de blanchiment de capitaux modéré (score de 2,5 sur 5).

4.3.5 CONCERNANT LE FINANCEMENT DU TERRORISME

Risque inhérent :

Plus spécifiquement le risque inhérent lié au financement du terrorisme, est assez faible au regard de la sophistication des montages à mettre en œuvre. En outre, l'activité porte généralement sur des montants importants ce qui ne correspond pas au mode de financement actuel des organisations terroristes. Actuellement, il n'a pas été constaté que des organisations terroristes auraient eu recours à ce mode de financement

Le risque inhérent de financement du terrorisme lié à l'activité peut être considéré comme modéré et quantifié par un score de 2 sur 5.

Vulnérabilité :

Il n'y a pas de vulnérabilités spécifiques renvoyant au financement du terrorisme autres que celles identifiées ci-dessus.

Les vulnérabilités de financement du terrorisme liées à l'activité peuvent être considérées comme modérées et quantifiées par un score de 2 sur 5.

Risque résiduel :

Le risque lié à l'activité peut être considéré comme moyen et quantifié par un score de 2 sur 5.

4.4 ACTIVITÉ DE TRADE FINANCE

4.4.1 DESCRIPTION DE L'ACTIVITÉ

Les crédits commerciaux (trade finance) désignent le rôle d'intermédiaire joué par les établissements de crédit dans l'organisation des paiements afin de faciliter les mouvements de marchandises et la fourniture de services tant à l'intérieur du pays qu'à l'international. Ils visent à renforcer la confiance de l'importateur qui pourrait craindre que les marchandises achetées ne parviennent pas à destination et rassurer l'exportateur quant au paiement des marchandises expédiées.

L'activité de Trade Finance consiste en des services bancaires aux entreprises comme les services :

- des opérations à compte ouvert,
- les lettres de crédit,
- la remise documentaire.

L'activité en Belgique

Les grandes banques « universelles » de droit belge sont généralement actives dans le secteur. On relève une vingtaine de filiales ou succursales des institutions non EEE dont certaines localisées dans des pays présentant un risque plus élevé, qui ont été créées en Belgique afin de supporter les activités de leurs entreprises domestiques en Belgique ou au sein de l'EEE.

4.4.2 RISQUES INHÉRENTS DE L'ACTIVITÉ

Les risques inhérents identifiés en lien avec cette activité sont les suivants :

- certaines opérations peuvent concerner géographiquement des pays présentant un haut risque de blanchiment de capitaux ou de financement du terrorisme ou des pays au sein duquel un grand nombre d'infraction sous-jacente sont constatées (contre façon, trafic de drogue) ;
- les opérations de Trade Finance peuvent être utilisées pour rapatrier des fonds accumulés à l'étranger sous une apparence licite ou exporter des biens d'origine douteuse. La sous-facturation ou la surfacturation peut permettre de transférer des fonds d'origine douteuse d'un pays à un autre, d'augmenter artificiellement le montant de la TVA récupérable ou encore réduire le montant dû au titre des taxes douanières. Les opérations de financement du commerce international peuvent également servir à financer des infractions à des embargos sur des biens ou des pays destinataires de ces biens ;

- la multi facturation (émission de plusieurs factures pour une même transaction) permet d'apporter une justification économique à des transferts de fonds d'origine douteuse.

Compte tenu de qui précède, le score en matière de risques inhérents peut être fixé à 3 sur 5 (significatif).

4.4.3 VULNÉRABILITÉS DES INSTITUTIONS PRATIQUANT CETTE ACTIVITÉ

Les établissements n'ont pas toujours un accès complet aux informations relatives à l'opération commerciale et aux parties à celle-ci. Il est parfois difficile pour eux de connaître avec précision l'activité réelle exercée par les parties (ou l'une d'elle) et de juger l'adéquation de la transaction avec les activités des entreprises concernées. Il y a également lieu de prendre en compte la difficulté pour les établissements de crédit de disposer d'une expertise suffisante permettant de juger du caractère adéquat des documents fournis.

La vulnérabilité est considérée comme significative et est quantifiée par un score de 3 sur 5.

4.4.4 SCORE GLOBAL DE L'ACTIVITÉ

Le secteur de Trade finance est considéré comme présentant un risque significatif de blanchiment de capitaux (score de 3).

4.4.5 CONCERNANT LE FINANCEMENT DU TERRORISME

Risque inhérent :

Plus spécifiquement concernant le financement du terrorisme, le risque est assez faible au regard de la sophistication des structures et montages à mettre en œuvre ainsi que la connaissance requise. En outre, l'activité porte généralement sur des montants importants ce qui ne correspond pas au mode de financement actuel des organisations terroristes. Actuellement, il n'a pas été constaté que des organisations terroristes auraient eu recours à ce mode de financement.

Le risque inhérent de financement du terrorisme lié à l'activité peut être considéré comme modéré et quantifié par un score de 2 sur 5.

Vulnérabilité :

Il n'y a pas de vulnérabilités spécifiques renvoyant au financement du terrorisme autres que celles identifiées ci-dessus.

Les vulnérabilités de financement du terrorisme liées à l'activité peuvent être considérées comme modérées et quantifiées par un score de 2 sur 5.

Risque résiduel :

Le risque de financement du terrorisme lié à l'activité peut être considéré comme modéré et quantifié par un score de 2 sur 5.

4.5 ACTIVITÉ DE SERVICE DE CHANGE MANUEL

4.5.1 DESCRIPTION DE L'ACTIVITÉ

L'activité de change manuel consiste dans le fait d'accepter l'échange immédiat de billets ou monnaies libellés en devises différentes ainsi que l'échange des espèces délivrées à un client, moyennant le règlement par un autre moyen de paiement libellé dans une devise différente.

L'activité en Belgique

Bien que l'activité ait connu une baisse sensible à la suite de la mise en circulation de l'Euro en 2002, elle est encore effectuée par un grand nombre des banques de détail et par des sociétés de bourse ainsi que des établissements de paiement. L'activité de change peut être importante dans les grandes villes du pays, dans les villes touristiques ainsi qu'aux abords des ports d'Anvers et de Zeebrugge. Certaines institutions financières ont conclu des contrats avec des sociétés maritimes afin de permettre le paiement des équipages étrangers en euro.

4.5.2 RISQUES INHÉRENTS DE L'ACTIVITÉ

La menace de blanchiment de capitaux est spécifiquement élevée avec des personnes souhaitant changer des devises dont l'origine est plus difficile à établir.

Les principaux risques inhérents à l'activité sont principalement liés à :

- l'utilisation fréquentes de l'argent liquide ;
- la nature de la clientèle souvent constituée des communautés itinérantes, par exemple des immigrants, des demandeurs d'asile, des travailleurs frontaliers, des touristes ;
- de nombreuses opérations sont occasionnelles ce qui rend difficile de bâtir une connaissance effective du client. ;
- Les clients peuvent chercher à convertir des fonds dans une autre devise pour en faciliter la conversion, le transfert ;
- au fractionnement des opérations de change dans différents établissements financiers pour éviter d'attirer l'attention, le cas échéant sous des patronymes différents, ou en recourant à des « mules » afin d'éviter les seuils d'identification appliqués par les établissements. Le cas échéant, ce fractionnement des opérations peut être effectués auprès d'institutions différentes ;
- la clientèle en relation avec des pays à risques.

Compte tenu de qui précède, le score en matière de risques inhérents peut être fixé à 4 sur 5 (élevé).

4.5.3 VULNÉRABILITÉS DES INSTITUTIONS PRATIQUANT CETTE ACTIVITÉ

Les vulnérabilités auxquelles sont exposés les établissements financiers offrant ce service sont les suivantes :

- le manque d'expérience et de formation pertinente et continue des dirigeants et/ou du personnel en matière de AML/CFT ;
- le manque de connaissances de certains préposés en contact direct avec la clientèle peut limiter l'effectivité des opérations d'identification et de vérification de l'identité du client et complique la collecte d'informations concernant l'origine des fonds ;
- le *turn over* important du personnel en matière AML/CFT et la difficulté rencontrée par le secteur en Belgique pour recruter du personnel ;
- l'origine des fonds peut être difficile à établir.

La matérialité de ces vulnérabilités pourra être variable en fonction du type et de la structure plus ou moins développées de l'établissement. Globalement les vulnérabilités peuvent être considérées comme étant significatives (score 3 sur 5).

4.5.4 SCORE GLOBAL DE L'ACTIVITÉ

Le score global de l'activité de change manuel est considéré comme présentant un risque significatif (score de 3,5 sur 5).

4.5.5 CONCERNANT LE FINANCEMENT DU TERRORISME

Risque inhérent :

Plus spécifiquement en matière de financement du terrorisme, l'activité du change peut être attractive dans la mesure où elle repose sur l'utilisation des espèces, facilite la conversion et le transfert des devises et ne requiert pas de connaissances particulières. Le fractionnement des opérations de change dans différents établissements financiers en vue d'éviter d'attirer l'attention, le cas échéant sous des patronymes différents, ou en recourant à des « mules » afin d'éviter les seuils d'identification appliqués par les établissements est un risque de l'activité.

Le risque inhérent de financement du terrorisme lié à l'activité peut être considéré comme élevé et quantifié par un score de 4 sur 5.

Vulnérabilité :

Il n'y a pas de vulnérabilités spécifiques renvoyant au financement du terrorisme autres que celles identifiées ci-dessus.

Les vulnérabilités de financement du terrorisme liées à l'activité peuvent être considérées comme significatives et quantifiées par un score de 3 sur 5.

Risque résiduel :

Le risque de financement du terrorisme lié à l'activité peut être considéré comme significative et quantifié par un score de 3,5 sur 5.

4.6 ACTIVITÉ DE SERVICE DE CAUTION ET DE NANTISSEMENT

4.6.1 DESCRIPTION DE L'ACTIVITÉ

Le cautionnement et le nantissement sont deux contrats accessoires à une obligation principale dont une personne physique ou morale peut être débitrice envers un établissement de crédit. La personne se portant caution d'une obligation s'engage envers le créancier à satisfaire à cette obligation, si le débiteur n'y satisfait pas lui-même. Le nantissement est l'affectation en garantie d'une obligation, d'un ou de plusieurs biens meubles corporels ou incorporels, présents ou futurs, tels que des œuvres d'art, des parts de sociétés, des titres financiers, ou des contrats d'assurance-vie ou de capitalisation. Le nantissement d'un compte est possible lorsqu'il porte sur un compte titres.

4.6.2 RISQUES INHÉRENTS DE L'ACTIVITÉ

Le nantissement peut être utilisé dans le cadre de montage de fraude fiscale. Par exemple, un contrat d'assurance-vie est nanti pour garantir un emprunt immobilier, l'emprunteur ne rembourse pas le prêt et utilise le contrat nanti pour le rembourser (montage dit du crédit lombard).

Le cautionnement offre aussi la possibilité de payer la dette garantie avec des fonds provenant d'un tiers, rendant plus difficile la recherche de l'origine des fonds.

Compte tenu de qui précède, le score en matière de risques inhérents peut être fixé à 1,5 sur 5 (faible).

4.6.3 VULNÉRABILITÉS DES INSTITUTIONS PRATIQUANT CETTE ACTIVITÉ

La caution n'est pas « le client » de l'institution financière qui dispose donc d'une connaissance plus faible de la caution et de ses caractéristiques que celle du client.

L'origine des fonds peut également être plus difficile à établir.

La vulnérabilité est considérée comme faible et est quantifiée par un score de 1,5 sur 5.

4.6.4 SCORE GLOBAL DE L'ACTIVITÉ

L'activité de cautionnement et nantissement est considérée comme présentant un risque faible de blanchiment des capitaux (score de 1,5 sur 5).

4.6.5 CONCERNANT LE FINANCEMENT DU TERRORISME

Plus spécifiquement concernant le financement du terrorisme, il peut être constaté au regard des développements ci-dessus, que l'activité n'engendre pas de risques particuliers liés au financement du terrorisme dans la mesure où les techniques à mettre en œuvre son peu compatibles avec la rapidité de mise à disposition des fonds aux fins d'une éventuelle entreprise terroriste. Le risque de financement du terrorisme peut être qualifié de faible et quantifié par un score de 1,5 sur 5.

4.7 ACTIVITÉ D'AFFACTURAGE

4.7.1 DESCRIPTION DE L'ACTIVITÉ

Il s'agit d'un service principalement offert par les établissements de crédit consistant en une méthode de financement et de recouvrement de créances utilisée par les entreprises visant à anticiper le règlement de leurs fournisseurs pour bénéficier de trésorerie avant la date de règlement contractuelle. La technique de l'affacturage recouvre trois types de prestations qui peuvent toutes être souscrites, séparément ou non, par l'entreprise :

- le recouvrement du poste client avec la gestion de ce compte (enregistrement des factures, la relance des débiteurs en cas de retard de paiement…) ;
- le financement de la trésorerie par l'avance du montant de créances dès leur cession par le client ;
- l'assurance-crédit avec la garantie de paiement de la créance.

L'activité en Belgique

La majorité des banques exerçant des activités dans le secteur « corporate » offre des services liés à la mise en place et la gestion des opérations de « factoring ».

4.7.2 RISQUES INHÉRENTS DE L'ACTIVITÉ

L'affacturage peut être utilisé pour le financement de fausses créances qui n'ont pas pour origine la livraison de biens ou de services. Dans ce cas, l'établissement achète une créance qui ne correspond à aucune livraison effective de biens ou prestations de services et paie le créancier, qui reçoit des fonds d'un organisme financier. Celui-ci est ensuite payé par le débiteur sur la base d'une fausse créance au moyen de fonds d'origine douteuse qui sont ainsi blanchis.

Il peut exister un risque de surfacturation permettant à l'acheteur et au vendeur, de récupérer un montant supérieur à celui des biens ou services fournis. Le vendeur pourra rétrocéder à l'acheteur le montant surfacturé.

Compte tenu de qui précède, le score en matière de risques inhérents de blanchiment de capitaux peut être fixé à 2 sur 5 (modéré).

4.7.3 Vulnérabilités des institutions pratiquant cette activité

Les établissements de crédit sont confrontés à la difficulté d'analyser l'adéquation de la transaction avec les activités des entreprises concernées.

La vulnérabilité est considérée comme modérée et est quantifiée par un score de 2 sur 5.

4.7.4 SCORE GLOBAL DE L'ACTIVITÉ

L'activité d'affacturage est considérée comme présentant un risque modéré de blanchiment des capitaux (score de 2 sur 5).

4.7.5 CONCERNANT LE FINANCEMENT DU TERRORISME

Plus spécifiquement concernant le financement du terrorisme, il peut être constaté au regard des développements ci-dessus, que l'activité n'engendre pas de risques particuliers liés au financement du terrorisme dans la mesure où les techniques à mettre en œuvre son peu compatibles avec la rapidité de mise à disposition des fonds aux fins d'une éventuelle entreprise terroriste. Le risque de financement du terrorisme peut être qualifié de faible et quantifié par un score de 1,5 sur 5.

4.8 CORRESPONDENT BANKING

4.8.1 DESCRIPTION DE L'ACTIVITÉ

La correspondance bancaire est la fourniture de services bancaires par une banque en tant que correspondant à une autre banque en tant que cliente, y compris la mise à disposition d'un compte courant et la fourniture de services qui y sont liés, tels que la gestion de trésorerie, les transferts internationaux de fonds, les services de change, les relations entre et parmi les établissements de

crédit et les établissements financiers. L'établissement correspondant exécute des opérations pour compte de tiers.

L'activité en Belgique

Le correspondent banking est concentré en Belgique auprès de quelques-uns des principaux établissements de crédit.

4.8.2 RISQUES INHERENTS DE L'ACTIVITÉ

Les risques inhérents pour le correspondent banking sont les suivants :

- la fourniture de services bancaires à des banques fictives (shell banks)[27] ou à des banques ne faisant pas l'objet d'un contrôle adéquat permet un accès indirect au système bancaire à des établissements non régulés ou insuffisamment régulés. De telles institutions établies dans des zones off-shore sont ainsi particulièrement exposées à des risques de BC/FT ;
- dès lors que la banque correspondante fournit à la banque cliente des services consistant dans l'exécution d'opérations initiées par les clients de cette dernière, le risque inhérent de blanchiment de capitaux associé à l'activité de correspondance bancaire est très fortement influencé par la qualité et l'efficacité des mécanismes de prévention du blanchiment mis en œuvre par la banque cliente ainsi que par les secteurs d'activités de ses clients ;
- les risques inhérents afférents à cette activité sont également fortement influencés par les risques géographiques lorsque les banques clientes sont établies dans des pays ou territoires dont la législation anti-blanchiment et/ou le contrôle de sa mise en application effective présente des faiblesses importantes ;
- les risques sont encore accrus lorsque la banque cliente a recours à la relation de correspondance bancaire, non seulement pour servir ses propres clients, mais également pour offrir à son tour des services identiques ou analogues de correspondance à diverses autres banques établies dans le même pays, voire d'autres pays (« netting ») : les risques de blanchiment de capitaux encourus par la banque correspondante sont dans ce cas fortement influencés par la qualité des mécanismes de prévention du blanchiment de capitaux mis en œuvre par ces autres banques clientes de sa propre cliente, et le cas échéant par le risque géographique qui leur est associé.
- les services offerts peuvent comporter l'ouverture d'un compte de passage (« payable-through account ») permettant au client de l''établissement client d'exécuter des transactions directement sur le compte de l'établissement client.

Les risques inhérents de blanchiment de capitaux relatifs à ces activités sont évalués comme élevés et sont quantifiés par un score de 4 sur 5.

4.8.3 VULNÉRABILITÉS DES INSTITUTIONS PRATIQUANT CETTE ACTIVITÉ

Il est difficile pour les institutions financières fournissant ces services, de disposer d'informations pertinentes fiables relatives aux activités et à la qualité des mécanismes de prévention du blanchiment de capitaux mis en œuvre par les institutions clientes. On relève également la difficulté d'allouer des ressources humaines suffisantes, disposant des connaissances et de l'expérience adéquates, pour procéder à l'évaluation individuelle des risques associés à chaque institution cliente et à l'analyse de ses opérations. De plus, les banques correspondantes doivent disposer d'outils spécifiquement formatés pour procéder de manière adéquate au monitoring des opérations des banques clientes, tenant compte du profil de chacune d'entre elles.

---

[27] Telles que définies par l'article 4.37 loi AML.

Une autre vulnérabilité consiste en la possible utilisation du compte par d'autres banques clientes qui ont une relation directe avec l'établissement client mais pas avec la banque correspondante (nesting account ou comptes imbriqués ou encore dans le cas de compensation d'aval (downstream clearing), de telle sorte que l'établissement correspondant fournit indirectement des services à d'autres banques qui ne sont pas parmi ses établissements clients.

Inversement, il est relevé que seules des institutions financières de premier ordre ou spécialisées, disposant de ressources importantes et de la capacité de recruter du personnel spécialisé fournissent ce type de services financiers.

L'intermédiation dans les chaines d'exécution des transferts de fonds peut rendre plus complexe la détection des bénéficiaires ou donneurs d'ordres figurant sur des listes de sanctions internationales.

Les activités de correspondance bancaire avec des établissements établis dans des pays tiers (hors EEE) présentent en elles-mêmes des vulnérabilités intrinsèques plus importantes, l'établissement client étant dans ce cas soumis à des exigences LCB-FT (réglementaires et/ou de supervision) différentes des exigences européennes.

La vulnérabilité au risque de blanchiment de capitaux des institutions pratiquant cette activité est considérée comme modérée (score de 2,5 sur 5) pour les activités de correspondance bancaire transfrontalières au sein de l'EEE et comme significative pour les activités de correspondance bancaire transfrontalières hors de l'EEE et quantifiée par un score de 3.

4.8.4 SCORE GLOBAL DE L'ACTIVITÉ

Le risque résiduel de blanchiment de capitaux est évalué significatif et quantifié par un score de 3,5 sur 5.

4.8.5 CONCERNANT LE FINANCEMENT DU TERRORISME

Risque inhérent :

Plus spécifiquement en matière de financement du terrorisme, la correspondance bancaire transfrontalière peut permettre à des personnes ou entités dont les fonds sont gelés d'accéder indirectement au système bancaire en passant par des banques établies dans des pays tiers (par exemple si la banque correspondante offre des services bancaires à des banques qui elles-mêmes ont des implantations dans des territoires présentant des risques de FT).

Le risque pour les banques concerne donc le transfert involontaire de fonds liés au terrorisme lorsqu'elles fournissent des services de banque correspondante à d'autres institutions financières étrangères. Cela peut conduire la banque à traiter à son insu des transactions provenant de banques étrangères pour le compte d'organisations ou d'individus complices. A titre d'exemple, il pourrait s'agir de transferts de fonds plus importants effectués pour le compte du Hezbollah ou de ses soutiens financiers, ou de fonds acheminés par l'Iran pour soutenir des mandataires terroristes, des groupes militants régionaux ou d'autres activités malveillantes.

L'application sans failles des règles et mesures liées au respect des sanctions, gels des avoirs et embargos ainsi que l'identification des UBO's est importante.

Le risque inhérent de financement du terrorisme lié à l'activité peut être considéré comme élevé et quantifié par un score de 4 sur 5.

Vulnérabilité :

Outre les vulnérabilités mentionnées ci-dessus, il peut être indiqué que les montants des opérations de financement du terrorisme en Belgique sont généralement faibles, et peuvent ne pas être identifiés dans le cadre du monitoring des opérations de correspondance bancaire portant sur des montants très nettement plus élevés.

Les vulnérabilités de financement du terrorisme liées à l'activité peuvent être considérées comme significatives et quantifiées par un score de 3 sur 5.

Risque résiduel :

La risque de financement du terrorisme peut être qualifié de significative et quantifiée par un score de 3,5 sur 5

4.9 CLEARING SETTLEMENT/CUSTODY/DEPOSITAIRES CENTRAUX

4.9.1 DESCRIPTION DE L'ACTIVITÉ

L'activité de clearing et de settlement vise l'exécution le dénouement des opérations de ventes/achats de titres, où qu'elles aient lieu par transfert des titres de ceux-ci de compte à compte en contrepartie du paiement du prix, libérant les parties à la transaction de leurs obligations respectives. Cette activité est aussi destinée aux grandes entreprises et à des institutions ne se trouvant pas dans le cadre d'un statut de contrôle.

L'activité de dépositaire central de titres (DCT) a un double rôle :

- -en qualité de « notaire », dans la mesure où le dépositaire central de titres répertorie les titres au moment de leur émission. A cet effet, il fait le lien entre les sociétés émettrices de titres financiers qui y déposent leurs titres et les intermédiaires financiers qui conservent ces titres pour le compte des investisseurs (ou pour leur propre compte) ;
- -en tant que gestionnaire du système de règlement-livraison de titres, permettant ainsi la circulation des titres entre les participants. Il permet alors aux intermédiaires financiers de réaliser les opérations de livraison des titres financiers contre paiement à la suite des négociations ou des cessions réalisées sur ces titres.

L'activité en Belgique

L'activité custody et dépositaire central est particulièrement significative, avec la présence de deux acteurs centraux et essentiels dans le paysage financier.

En marge de l'activité de settlement, ces institutions financières offrent d'autres services auxiliaires liés aux activités sur titres tels que:

- Securities lending and borrowing: crédits intraday toujours collatéralisés afin de permettre le *settlement on time* des transactions ;
- Asset servicing, custody ;
- Investment funds related services ;
- Collateral management ;
- Fund Settlement services ;
- Money transfer services: services de "comptes en banque" très limités, les participants peuvent verser le résultats des ventes de titres sur leur propres comptes dans des (autres) banques commerciales.

4.9.2 RISQUES INHÉRENTS DE L'ACTIVITÉ

Les risques inhérents associés aux activités de clearing settlement, custody et dépositaires centraux sont assez similaires aux risques associés aux activités de correspondance bancaire lorsque le client est lui-même une banque ou une institution financière assujettie aux obligations de prévention du BC (cf. ci-dessus).

Bien que les participants au dépositaire central de titres soumettent également leurs clients à leurs propres systèmes de LBC/FT, les transactions pour compte propre et avec des tiers, en raison de la complexité qu'elles peuvent impliquer, constituent néanmoins un facteur de risque. À cet égard, bien que tous les flux soient traçables, le fait qu'ils puissent être compensés avec d'autres transactions peut rendre difficile l'identification d'éventuels comportements suspects. En conséquence, compte tenu de la masse d'instructions entre les participants, de leur éventuelle compensation et de la variété des instructions possibles, le dépositaire central de titres n'a pas une image détaillée des stratégies sous-jacentes des transactions passant par son système.

Les institutions peuvent être confrontées à des mécanismes particuliers mis en place visant à éluder l'impôt. Il en va ainsi, par exemple, des systèmes d'arbitrage de dividendes « Cum/Ex » ou « Cum/Cum » qui consistent à éluder ou à récupérer indûment le précompte mobilier lié à un instrument financier. Des transactions autour de la date du dividende permettent d'induire en erreur les services fiscaux des pays impliqués[28].

Les montants des transactions sont particulièrement élevés, ce qui constitue un facteur de risque accru.

Les risques inhérents relatifs à ces activités sont évalués comme modérés et sont quantifiés par un score de 2,5 sur 5.

4.9.3 VULNÉRABILITÉS DES INSTITUTIONS PRATIQUANT CETTE ACTIVITÉ

Les entités pratiquant l'activité sur le territoire belge sont spécialisées et disposent d'une expertise certaine.

Une mesure de mitigation réside dans le fait que les participants au dépôt central des titres et les institutions qui les soutiennent sont eux-mêmes des entités supervisées, soumises à la LBC/FT et qu'elles n'ont pas de clients « personnes physiques ».

En outre, les participants sont soumis à une due diligence qui consiste à vérifier le respect des critères d'admission (y compris la soumission à un système de LBC/FT) en fonction de critères de risque principalement géographiques. Le processus d'onboarding des participants implique des procédures de vérification de leur qualité (enregistrement, agrément, actionnaires, dirigeants), mais aussi, selon leurs statuts, la vérification de leur soumission à la réglementation anti-blanchiment.

La vulnérabilité des institutions pratiquant cette activité est considérée comme modérée et quantifiée par un score de 2 sur 5.

4.9.4 SCORE GLOBAL DE L'ACTIVITÉ

Le risque résiduel de blanchiment de capitaux est qualifié de modéré et quantifié par un score de 2 sur 5.

---

[28] Cf. les développements à cet égard sous le point relatif à l'activité « private banking »

4.9.5 CONCERNANT LE FINANCEMENT DU TERRORISME

Risque inhérent :

Plus particulièrement concernant le financement du terrorisme, l'activité est relativement peu exposée directement à la menace du financement du terrorisme. Elle est en effet très intégrée dans l'écosystème financier et ne proposant que des procédures d'échange électronique nécessitant l'utilisation de systèmes de communication standardisés et difficiles d'accès (Swift). Elle est inaccessible aux particuliers et difficilement accessible aux personnes morales n'ayant pas d'activité significative de règlement de titres à long terme. Le niveau élevé d'investissement requis pour accéder aux systèmes de règlement rend l'utilisation directe du dépositaire central de titres inappropriée aux fins du financement du terrorisme. L'application sans failles des règles et mesures liées au respect des sanctions, gels des avoirs et embargos ainsi que l'identification des UBO's reste cependant importante.

Actuellement, il n'a pas été constaté que des organisations terroristes auraient eu recours à ce mode de financement.

Le risque inhérent de financement du terrorisme lié à l'activité peut être considéré comme modéré et quantifié par un score de 2 sur 5.

Vulnérabilité :

Il n'y a pas de vulnérabilités spécifiques renvoyant au financement du terrorisme autre que celles identifiées ci-dessus.

Les vulnérabilités de financement du terrorisme liées à l'activité peuvent être considérées comme modérées et quantifiées par un score de 2 sur 5.

Risque résiduel :

La menace de risque de financement du terrorisme peut être qualifiée de modéré et quantifiée par un score de 2 sur 5 .

5 CONSEIL EN INVESTISSEMENT (SOCIÉTÉS DE BOURSE)

5.1 DESCRIPTION DE L'ACTIVITÉ

Les deux principales activités des sociétés de bourse portent d'une part sur le private banking (pour cet aspect, il est renvoyé à ce qui est dit supra au point 4.1. pour les établissements de crédit se livrant à cette activité), et d'autre part sur la réception/transmission d'ordres. Dans ce cadre, les sociétés de bourse sont autorisées à ouvrir des comptes titres et des comptes de liquidités à leurs clients, des règles spécifiques étant fixées pour l'utilisation de ces comptes. Rappelons ici que l'agrément octroyé aux sociétés de bourse est un agrément à tiroirs, et que d'autres activités peuvent également être exercées par les sociétés de bourse, comme la négociation pour compte propre ou la prise ferme. Ces activités ne sont pas abordées dans la présente note.

L'activité en Belgique

La tendance dans ce secteur est à la consolidation et à la réduction du nombre d'institutions de droit belge sous statut de contrôle. Cette tendance s'explique notamment par la masse critique d'activités nécessaire pour devenir rentable, par la digitalisation, par une clientèle vieillissante et par la difficulté de répondre à l'inflation réglementaire.

Le secteur comptait à fin 2022, 12 sociétés de droit belge, à répartir entre 7 sociétés familiales et 5 sociétés faisant partie d'un groupe. Il faut également noter que parmi les 5 sociétés faisant partie d'un groupe, deux sociétés de bourse exercent exclusivement une activité spécifique de gestion des fonds. Le montant des avoirs sous gestion pour ces 12 sociétés de bourse de droit belge s'élevait fin 2020 à 8,88 MM d'euros.

Il faut y rajouter 10 succursales de sociétés de bourse relevant du droit d'un autre Etat membre de l'EEE.

5.2 RISQUES INHÉRENTS DE L'ACTIVITÉ

Les risques inhérents associés aux activités de réception et exécution d'ordres sont les suivants :

- le montant inhabituellement élevé des transactions ;
- les raisons sous-tendant l'investissement ne comportent pas de finalité économique évidente, comme par exemple :
  - le client demande le rachat ou le remboursement d'un placement à long terme dans un délai court, sans justification claire et alors que cela entraîne pour lui une perte financière ;
  - le client transfère des fonds dont le montant dépasse celui requis pour l'investissement et demande le remboursement du trop-payé ;
  - le client est réticent à fournir des informations dans le cadre des mesures de vigilance légitimes ;
- la nature du client (véhicule d'investissement non réglementé, PEP, …) ;
- les activités du client (par exemple si les fonds proviennent de secteurs d'activité associés à un risque de criminalité financière élevé) ;
- le risque géographique (investisseur ou dépositaire installé dans un pays ou territoire à risque, ou fonds provenant d'un tel pays ou territoire) ;
- la connaissance insuffisante de l'origine des fonds.

La nature du produit peut présenter un niveau de vulnérabilité différent (coté/non coté, simple/complexe, produits échangés sur le marché de gré à gré moins régulé, …).

Sur base de ce qui précède, le niveau de risques inhérents peut être considéré comme étant de « modéré » (niveau 2 sur 5) pour la réception/transmission d'ordres, et « significatif » pour le private banking (niveau 3,5 sur 5).

5.3 VULNÉRABILITÉS DES INSTITUTIONS PRATIQUANT CETTE ACTIVITÉ

Les vulnérabilités suivantes peuvent être soulignées :

- l'absence d'un monitoring adéquat. Ainsi, les sociétés de bourse ne peuvent ouvrir des comptes de liquidité à des particuliers que pour autant qu'il s'agisse de comptes destinés à recevoir soit des fonds en attente d'investissement, soit les fonds résultant de la vente d'instruments financiers. De tels comptes ne sont par conséquent pas destinés à pouvoir effectuer des paiements ordinaires. Un danger peut par conséquent consister dans le fait que de tels comptes pourraient servir à réaliser des opérations suspectes ou inhabituelles, sans qu'un monitoring adéquat ne permette de détecter de tels mouvements suspects ;
- le développement des FinTech/RegTech débouche sur des risques nouveaux comme l'identification *non face to face*, le développement de l'outsourcing pour les contrôles dans le cadre des devoirs de vigilance , ou la *reliance on third party service providers*.

- il ressort de l'expérience des services dans ce secteur qu'un certain nombre de sociétés de bourse sous-estiment le risque de blanchiment lié à leur activité, et ne disposent dès lors ni des moyens humains et/ou techniques pour y faire face, ni de l'expertise nécessaire, et ne consacrent pas les moyens nécessaires à la formation de leur personnel.

Le score en termes de vulnérabilité peut être estimé comme modéré (2 sur 5) pour l'activité de réception/transmission d'ordres, et élevé pour l'aspect private banking (4 sur 5).

5.4 SCORE GLOBAL DE L'ACTIVITE

Le risque résiduel de blanchiment de capitaux est qualifié de modéré et quantifié par un score de 2 sur 5 pour l'activité de réception/transmission d'ordres.

Le risque résiduel de blanchiment de capitaux est qualifié « élevé » et quantifié par un score de 4 sur 5 pour l'activité private banking.

5.5 CONCERNANT LE FINANCEMENT DU TERRORISME

Risque inhérent :

Plus spécifiquement concernant le financement du terrorisme, il ne semble pas qu'un lien soit établi entre l'activité des sociétés de bourse et le financement du terrorisme. L'entrée en relation d'affaires est soumise à des conditions assez strictes mais au contraire de l'activité de « private banking », les montants des investissements demandés sont plus faibles. L'activité ne se prête pas à l'anonymat des transactions ni aux transferts directs et rapides des sommes investies au profit d'autres personnes impliquées.

Le risque inhérent de financement du terrorisme lié à l'activité peut être considéré comme faible et quantifié par un score de 1,5 sur 5.

Vulnérabilités :

Il n'y a pas de vulnérabilités spécifiques renvoyant au financement du terrorisme autres que celles identifiées ci-dessus.

Les vulnérabilités de financement du terrorisme liées à l'activité peuvent être considérées comme significatives et quantifiées par un score de 3 sur 5.

Risque résiduel :

La menace de risque de financement du terrorisme peut être qualifiée de modérée et quantifiée par un score de 2 sur 5.

6 INSTITUTIONS D'ASSURANCE VIE

6.1 DESCRIPTION DE L'ACTIVITÉ

Les produits d'assurance-vie recouvrent les produits visant à protéger le bénéficiaire contre le risque de survenance d'un évènement futur relatif à la durée de la vie humaine.

L'activité d'assurance vie consiste en la vente des produits assurance-vie au niveau individuel (comme notamment les assurances épargne et assurances investissement) et groupe (assurances retraite).

En matière d'assurance vie, les différents produits sont classés en branches (de 21 à 29) en fonction de leurs caractéristiques et du degré de risque y afférents.

21. Assurances sur la vie non liées à des fonds d'investissement à l'exception des assurances de nuptialité et de natalité.
22. Assurances de nuptialité et de natalité non liées à des fonds d'investissement.
23. Assurances sur la vie, assurances de nuptialité et de natalité liées à des fonds d'investissement.
24. L'assurance pratiquée en Irlande et au Royaume-Uni, dénommée "permanent health insurance" (assurance maladie, à long terme, non résiliable).
25. Les opérations tontinières.
26. Les opérations de capitalisation.
27. Gestion de fonds collectifs de retraite.
28. Les opérations telles que visées par le Code français des assurances au livre IV, titre 4, chapitre Ier.
29. Les opérations dépendant de la durée de la vie humaine, définies ou prévues par la législation des assurances sociales, lorsqu'elles sont pratiquées ou gérées en conformité avec la législation d'un Etat membre par des entreprises d'assurances et à leur propre risque.

Au-delà du type de risque, la catégorisation des produits en branches permet de distinguer également les aspects liés aux avantages fiscaux éventuels, aux taxes sur les primes et aux précompte mobilier.

L'activité en Belgique

En 2022, le secteur belge de l'assurance-vie comptait 34 institutions (contre 40 en 2020) agréées ou autorisées. Ces organismes se répartissent entre 25 organismes d'assurance agréés ou autorisés de droit belge (contre 29 en 2020) et 9 succursales EEE (11 en 2020). Plus de 50% des institutions actives en assurance vie font partie d'un groupe de bancassurance.

Les quinze principaux groupes d'assurances représentent ensemble 97% du total des encaissements en 2022.

Les assurances vies individuelles à taux garanti (branche 21) et les assurances groupe demeurent les produits les plus répandus mais les branches 26 et 23 enregistrent ces dernières années une croissance en termes d'encaissements de primes.

6.2 RISQUES INHÉRENTS DE L'ACTIVITÉ

Le développement des FinTech/RegTech risque de faire naître des risques complémentaires liés à l'identification à distance, ou au recours à l'outsourcing pour l'AML.

Les facteurs de risques suivants peuvent être soulignés :

- le bénéficiaire du contrat n'est pas nécessairement le preneur. Il s'ensuit que la compagnie d'assurance peut disposer de moins d'information le concernant ;
- la flexibilité des paiements (en provenance de tiers non identifiés, primes d'un montant élevé ou illimité, …) ;
- la négociabilité du produit ;

- l'anonymat du produit ;
- la nature du client (PPE, actif dans un secteur requérant beaucoup d'espèces ou exposé à un risque de corruption, …) ;
- le comportement du client (client transfère le contrat à un tiers sans lien apparent, il encourt des frais élevés en demandant la résiliation anticipée d'un produit, paiements en espèces, …).

Le paiement des primes en argent liquide n'est plus autorisé par les compagnies d'assurance actives en Belgique ce qui limite quelque peu le risque de blanchiment de capitaux.

Les produits d'assurance-vie à long terme

La plupart des produits d'assurance-vie classiques (donc hors produits d'investissement) sont conçus pour le long terme, et beaucoup d'entre eux ne sont pas assez flexibles que pour constituer un véhicule de prédilection des blanchisseurs de capitaux. Par ailleurs, les frais relatifs aux rachats anticipés et à la résiliation de contrats rendent le processus de blanchiment couteux si réalisé sur du court terme. En outre l'opération de rachat anticipé ou de résiliation sont des événements aisément identifiables par les entreprises d'assurance. Le risque que les fonds utilisés pour souscrire une assurance-vie proviennent d'une activité criminelle ne peut cependant être exclu, en particulier dans le cas de contrats à primes uniques de montants importants.

Les risques liés à l'activité dépendent *in fine* du type d'assurance vie

Ainsi, les assurances retraite largement répandues en Belgique sont considérées comme présentant un risque de blanchiment significativement moins élevé, lorsque les primes sont de faible montant et que le modèle se base sur une contribution définie et limitée. Par ailleurs, les assurances groupes sont considérées comme moins risquées quand le paiement des primes est également limité en volume et s'opère par prélèvement sur la rémunération et exclusivement réservé à l'employeur et à l'employé. Les modalités de constitution du capital, les conditions de paiement ou de rachat de l'assurance groupe (au départ à la retraite, avance en vue de l'achat d'un bien immobilier) font que ce type d'assurance n'est pas attractif en termes de blanchiment de capitaux et de financement du terrorisme.

Les produits d'assurance comme instrument de placement

A contrario, les assurances vie constituant des contrats de capitalisation (branche 26) présentent un risque inhérent plus important, dans la mesure où ils peuvent permettre le placement à court terme d'argent provenant d'une activité criminelle ou originaire de la fraude fiscale (rapatriement de fonds/ donations non déclarées).

Le risque relatif aux assurances de type branche 23, liées à des fonds d'investissement, peut également s'avérer plus élevé. Il s'agit en effet d'un produit de type placement qui s'écarte du produit d'assurance-vie classique du type branche 21, et qui présente un profil fiscal favorable par rapport à des placements bancaires plus classiques. Il offre également la possibilité de retraits exonérés de tout impôt sur la police. On relève que les assurances branche 23 ont connu ces dernières années un développement très important, souvent au détriment de la branche 21 dont les taux garantis avaient fortement diminué du fait de la baisse généralisée des taux. Les produits de branche 23 permettent d'investir indirectement sur les marchés financiers.

Peuvent également constituer des risques inhérents :

- l'origine des fonds si ceux-ci proviennent par exemple de rapatriements depuis l'étranger ;
- des produits d'épargne branche 23 peuvent, du fait de leur flexibilité, faire l'objet de montages complexes rendant opaque l'identité du bénéficiaire ;
- possibilité de retraits des fonds investis en branche 23 sans impact fiscal.

En conséquence, le risque inhérent de l'activité d'assurance vie en Belgique est jugé modéré pour les assurances-vie classiques (2 sur 5) et significatif pour les assurances-vie comme outil de placement (3 sur 5).

6.3 VULNÉRABILITÉS DES INSTITUTIONS PRATIQUANT CETTE ACTIVITÉ

De manière générale, il est apparu que les entreprises d'assurance, a priori moins susceptibles que d'autres institutions financières d'être confrontées à un risque de blanchiment de capitaux, avaient quelque peu négligé cette problématique, tant en ce qui concerne les moyens humains et matériels qui y étaient consacrés, qu'en ce qui concerne l'expertise en leur sein (notamment en n'assurant pas des formations adaptées).

Un contrat d'assurance présente essentiellement deux moments importants en termes de prévention du blanchiment de capitaux : la conclusion du contrat, le paiement de la prestation. C'est à ces deux moments clés que les informations essentielles sur le client et le(s) bénéficiaire(s) sont recueillies. Au contraire d'une relation commerciale avec un établissement de crédit, il est plus difficile pour la compagnie d'assurance de bâtir une véritable connaissance du client. Un nouveau Code sectoriel développé par l'association professionnelle ASSURALIA en 2019 mis à jour en 2021 semble avoir permis d'augmenter la compréhension au sein du secteur et d'atteindre un meilleur niveau de conformité en matière LBC/FT. Notamment les compagnies d'assurance actives en Belgique ont dans leur majorité modifié leur approche qui était basée sur les différents contrats souscrits pour adopter à présent une approche fondée sur le client ce qui permet d'avoir une vue holistique du portefeuille du client.

Il y a lieu d'indiquer que les produits d'assurance vie nécessitent des actions de monitoring qui requièrent toute l'attention de la compagnie au moment de l'entrée en relation et au moment du pay-out en ce compris le rachat ou la mise en garantie. Entre ces moments, le suivi est généralement plus aisé (pour autant qu'il n'y ait pas de changement (identité de la personne qui alimente le contrat, prime plus élevée...)

Le recours à des tiers pour la commercialisation des produits d'assurance, et pour l'identification des clients et des relations d'affaires ainsi que la conservation des données AML y relatives est susceptible de constituer une vulnérabilité pour les entreprises d'assurance si les procédures ne sont pas adéquates et si des contrôles adéquats ne sont pas réalisés.

Il y a néanmoins lieu de noter que les intermédiaires en assurances (agents liés, agent-non liés, courtiers) sont soumis en Belgique à la supervision de la FSMA en matière LBC/FT

Les assurances-vie classiques

La distribution des produits d'assurance vie classiques est moins répandue que celle des autres services financiers, ce qui pourrait en diminuer l'attrait pour les criminels.

S'agissant d'ailleurs des risques de blanchiment pour l'intermédiation financière, nous renvoyons vers les travaux de la FSMA[29] et notamment ses constatations à l'issue de plusieurs inspections auprès d'intermédiaires d'assurance.

Les institutions proposant des activités d'assurance-vie sont par ailleurs relativement moins exposées à d'éventuelles transactions clandestines/non enregistrées du fait que la connaissance du client qu'elles peuvent générer est davantage qualitative dans la mesure où un grand nombre d'informations sur le client doivent être récoltées.

29 https://www.fsma.be/sites/default/files/legacy/content/FR/Blanchiment/2020-05-26_rapporttpc.pdf

Au vu de ce qui précède, les vulnérabilités des institutions d'assurance sont considérées comme présentant un caractère faible (1,5 sur 5) pour les assurances-vie classiques.

Les assurances-vie comme produit de placement

Les assurances-vie en tant que produits de placement sont soumises à des vulnérabilités générales comme reprises ci-dessus. La présence de ressources insuffisantes et d'un manque d'expertise en matière AML peut être particulièrement dommageable pour un produit assez flexible comme les assurances de la branche 23.

Même si le risque reste relativement limité, la vulnérabilité en la matière peut être qualifiée de modérée (2,5 sur 5).

6.4 SCORE GLOBAL DE L'ACTIVITÉ

Le risque résiduel de blanchiment de capitaux est qualifié de faible et quantifié par un score de 1,5 sur 5 l'activité d'assurance vie classique

Le risque résiduel de blanchiment de capitaux est qualifié de modéré et quantifié par un score de 2,5 sur 5 pour les assurances vie comme produits de placement.

6.5 CONCERNANT LE FINANCEMENT DU TERRORISME

Plus spécifiquement concernant le financement du terrorisme, il peut être constaté au regard des développements ci-dessus, que l'activité n'engendre pas de risque particulier dans la mesure où les techniques à mettre en œuvre son peu compatibles avec la rapidité de mise à disposition des fonds aux fins d'une éventuelle entreprise terroriste. Le risque peut être qualifié de faible et quantifié par un score de 1,5 sur 5.

7 SYNTHÈSE DES SCORES :

Synthèse des risques liés au blanchiment de capitaux

	Risques inhérents	**/5**	**Vulnérabilités**	**/5**	**Risque résiduel**	**/5**
Activités de paiement	Elevés	4	Elevées	4	Elevé	4
Transferts de fonds	Elevés	4,5	Elevées	4	Elevé	4,5
Activités d'acquiring	Modérés	2	Modérées	2	Modéré	2
Initiation de paiement	Faibles	1,5	Modérées	2,5	Modéré	2
Service d'informations sur les comptes	Nuls	0	Nulles	0	Nul	0
Activités de monnaie électronique	Modérés	2,5	Significatives	3	Modéré	2,5
Private banking	Significatifs	3,5	Elevées	4	Elevé	4
Retail banking	Modérés	2,5	Modérées	2,5	Modéré	2,5
Corporate banking	Significatifs	3	Modérées	2	Modéré	2,5
Trade finance	Significatifs	3	Significatives	3	Significatif	3
Service de change manuel	Elevés	4	Significatives	3	Significatif	3,5
Service de caution et de nantissement	Faibles	1,5	Faibles	1,5	Faible	1,5
Activité d'affacturage	Modérés	2	Modérées	2	Modéré	2
Correspondent banking	Elevés	4	Significatives	3	Significatif	3,5
Clearing/Custody/Depositaires	Modérés	2,5	Modérées	2	Modéré	2
Conseil en investissement (private banking)	Significatifs	3,5	Elevées	4	Elevé	4
Conseil en investissement (sans détention)	Modérés	2	Modérées	2	Modéré	2
Assurances vie	Modérés	2	Faibles	1,5	Faible	1,5
Assurances vie (produits d'investissement)	Significatifs	3	Modérées	2,5	Modéré	2,5

Synthèse des risques liés au financement du terrorisme

	Risques inhérents	**/5**	**Vulnérabilités**	**/5**	**Risque résiduel**	**/5**
Activités de paiement	Elevés	4	Elevée	4	Elevé	4
Transferts de fonds	Elevés	4	Elevées	4	Elevé	4
Activités d'acquiring	Faibles	1,5	Faibles	1,5	Faible	1,5
Initiation de paiement	Faibles	1,5	Faibles	1,5	Faible	1,5
Service d'informations sur les comptes	Nuls	0	Nulles	0	Nul	0
Activités de monnaie électronique	Significatifs	3	Significatives	3	Significatif	3
Private banking	Faibles	1,5	Modérées	2	Faible	1,5
Retail banking	Elevés	4	Elevées	4	Elevé	4
Corporate banking	Modérés	2	Modérées	2	Modéré	2
Trade finance	Modérés	2	Modérées	2	Modéré	2
Service de change manuel	Elevés	4	Significatives	3	Significatif	3,5
Service de caution et de nantissement	Faibles	1,5	Faibles	1,5	Faible	1,5
Activité d'affacturage	Faibles	1,5	Faibles	1,5	Faible	1,5
Correspondent banking	Elevés	4	Significatives	3	Significatif	3,5

Clearing/Custody/Depositaires	Modérés	2	Modérées	2	Modéré	2
Conseil en investissement (private banking)	Faibles	1,5	Significatives	3	Modéré	2
Conseil en investissement (sans détention)	Faibles	1,5	Significatives	3	Modéré	2
Assurances vie	Faibles	1,5	Faibles	1,5	Faible	1,5
Assurances vie (produits d'investissement)	Faibles	1,5	Faibles	1,5	Faible	1,5