F. Aspects de la réglementation et du contrôle prudentiels applicables à l'ensemble des secteurs

En sa qualité d'autorité de contrôle prudentiel, la Banque a compétence sur une série de domaines qui recouvrent plusieurs secteurs et ne sont donc pas abordés dans les parties du présent Rapport annuel dédiées aux banques, aux assurances et aux infrastructures de marchés financiers. Ainsi, au cours des dernières années, la Banque a activement participé aux travaux nationaux et internationaux en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme. Durant l'année sous revue, elle a pour ce faire adapté et renforcé son organisation interne dans le prolongement de la recommandation formulée par le Groupe d'action financière (GAFI). Par ailleurs, des actions de contrôle horizontales ont été entreprises au sujet de l'exécution de sanctions financières à l'encontre des terroristes et des organisations terroristes et au sujet des mesures de prévention des mécanismes fiscaux particuliers et du blanchiment de capitaux issus de la fraude fiscale grave dans le cadre de l'enquête sur les « Panama Papers ».

Durant l'année sous revue, la Banque a créé une nouvelle fonction d'assurance qualité. Elle a pour mission de veiller à ce que le contrôle financier soit conforme aux exigences de qualité fixées par le MSU.

Les avancées technologiques dans le secteur financier ont également conduit à l'apparition de nouveaux acteurs de marché dont le modèle d'entreprise se fonde sur les innovations financières. Ces acteurs FinTech utilisent des applications, des processus ou des produits nouveaux et exercent ainsi une influence réelle sur les marchés et établissements financiers existants et sur la fourniture de services financiers au sens large. Au cours de l'année sous revue, un groupe de travail interne à la Banque a observé leur incidence sur les modèles d'entreprise existants et sur les risques prudentiels.

Les cyber-attaques sont de plus en plus sophistiquées et provoquent toujours davantage de dégâts. La Banque a accordé une attention particulière à la gestion des cyber-risques dans les établissements financiers et les IMF individuels, ainsi que dans l'ensemble du secteur. Les efforts visant à améliorer la cyber-résistance ont encore été intensifiés, en mettant spécifiquement l'accent sur la gestion de ce risque par les acteurs financiers et sur la réalisation de tests permettant d'évaluer le niveau de protection contre les attaques.

1. Lutte contre le blanchiment de capitaux et le financement du terrorisme

1.1 Suivi de l'évaluation mutuelle de la Belgique par le GAFI : poursuite de la réorganisation du contrôle

En vue de répondre adéquatement aux critiques formulées par le GAFI quant au niveau de conformité de la législation et de la réglementation belges aux nouveaux standards du GAFI, et compte tenu de la décision du gouvernement belge, suite aux attentats de Paris du 13 novembre 2015, d'anticiper autant que possible la transposition de la 4e directive européenne relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme[1], la Banque s'est fortement impliquée, en association avec les autres

(1) Directive (UE) 2015/849 du Parlement Européen et du Conseil du 20 mai 2015 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux ou du financement du terrorisme, modifiant le règlement (UE) n° 648/2012 du Parlement européen et du Conseil et abrogeant la directive 2005/60/CE du Parlement européen et du Conseil et la directive 2006/70/CE de la Commission, Journal officiel de l'Union européenne, L 141, du 5 juin 2015.

autorités publiques concernées, dans le groupe de travail chargé d'élaborer, dans le bref délai qui lui était imparti, un avant-projet de loi de transposition qui, tout à la fois, respecte l'ensemble des exigences formulées dans la directive et aligne aussi parfaitement que possible la législation belge avec les 40 recommandations du GAFI.

Par ailleurs, comme annoncé dans son rapport annuel 2015, la Banque a entrepris en 2016 l'adaptation de son organisation interne afin d'affermir l'efficacité des contrôles en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (LBC/FT) qu'elle est chargée d'exercer auprès des institutions financières qui relèvent de ses compétences. Un groupe spécialisé a ainsi été constitué pour prendre en charge tant les travaux relatifs à la définition de la politique prudentielle en la matière que le contrôle hors site des institutions financières, tout en maintenant des relations étroites avec les services en charge du contrôle général hors site, d'une part, et avec le service en charge des inspections sur place, d'autre part. Outre le fait que la centralisation des tâches de contrôle hors site dans une équipe de spécialistes accroît par elle-même l'attention attachée par la Banque à l'exercice de cette mission de contrôle, les ressources qui y sont spécifiquement allouées ont d'ores et déjà connu un net accroissement en 2016, tant au sein de l'équipe de contrôle hors site qu'au sein du service chargé des inspections sur place. Des accroissements complémentaires de ressources sont encore prévus pour 2017.

En conséquence de l'ensemble de ces mesures, la Banque a multiplié ses contacts avec les institutions financières dans l'exercice du contrôle hors site, et le nombre d'inspections a sensiblement progressé. Outre que ces actions de contrôle visent en premier lieu à amener les institutions directement concernées à apporter une réponse appropriée aux faiblesses spécifiques décelées dans leur chef, l'intensification des contrôles en matière de LBC/FT, qui se poursuivra en 2017 et se combinera avec la réforme du cadre légal et réglementaire du fait de la transposition de la 4e directive, aura également pour effet de sensibiliser davantage l'ensemble des institutions financières à la nécessité impérative de disposer de mécanismes internes de LBC/FT efficaces.

Un des objectifs poursuivis par la Banque dans ce contexte consiste en particulier à asseoir plus systématiquement l'exercice du contrôle en la matière sur une analyse des risques spécifiques de blanchiment de capitaux et de financement du terrorisme auxquels les institutions financières contrôlées sont exposées. Des mesures allant dans ce sens ont d'ores et déjà été prises, en se fondant notamment sur les réponses fournies par les institutions financières au questionnaire annuel auquel elles sont appelées à répondre[1], sur les rapports annuels de leurs responsables de la lutte contre le blanchiment de capitaux et le financement du terrorisme et sur les informations dont la Banque dispose dans le cadre de l'exercice de ses compétences de contrôle prudentiel. Il importe cependant que cette approche du contrôle, à laquelle la Banque recourra, soit cohérente avec les pratiques qui seront mises en œuvre dans les autres États membres de l'Union européenne. Dès lors, la Banque a pris une part active dans l'élaboration des « orientations », confiée aux Autorités européennes de supervision par la 4e directive précitée. La récente publication de ces orientations[2] permettra à la Banque de poursuivre la construction de son propre modèle d'analyse des risques tout en veillant à la convergence de ses pratiques avec celles des autres autorités nationales en Europe.

1.2 Actions horizontales de contrôle relatives au gel des avoirs des terroristes et aux « *Panama Papers* »

Suite aux attentats terroristes qui ont frappé la France le 13 novembre 2015 et la Belgique le 22 mars 2016, la Banque a décidé de mener une action horizontale de contrôle de l'organisation dont l'ensemble des institutions financières se sont dotées afin de satisfaire à leurs obligations de mise en œuvre des sanctions financières ciblées à l'encontre des terroristes et des organisations terroristes visés par les listes belges et européennes de gel des avoirs et des ressources économiques. Indépendamment des actions individuelles sur lesquelles cette action horizontale a débouché afin de combler les lacunes constatées auprès de certains établissements, la Banque a estimé particulièrement utile de renforcer la sensibilisation de l'ensemble de ces établissements à leurs responsabilités en la matière en leur adressant un courrier dans lequel elle tire les leçons de son action de contrôle, s'efforce de clarifier certains aspects du régime légal applicable qui apparaissaient compris de manière inégale, et exprime ses attentes et ses recommandations en vue d'une meilleure application de ces sanctions financières[3].

En outre, suite à la publication des « *Panama Papers* » dans la presse en avril 2016, la Banque a par ailleurs mené une action horizontale de contrôle concernant la

(1) La nouvelle version du questionnaire périodique relatif à la prévention du blanchiment de capitaux et du financement du terrorisme, auquel les institutions financières devront répondre entre le 1er janvier et le 28 février 2017 sur la base de leur situation au 31 décembre 2016, leur a été adressée par les circulaires NBB_2016_42 et NBB_2016_43 du 26 octobre 2016.

(2) « *Joint Guidelines on the characteristics of a risk-based approach to anti-money laundering and terrorist financing supervision, and the steps to be taken when conducting supervision on a risk-sensitive basis – The Risk-Based Supervision Guidelines* », ESAs 2016 72, 16 novembre 2016.

(3) La lettre horizontale du 6 décembre 2016 concernant l'application du régime financier de sanction (financement anti-terrorisme) peut être consultée sur le site www.nbb.be.

mise en œuvre tant des mesures de prévention des mécanismes particuliers de nature fiscale que des mesures de prévention du blanchiment de capitaux issus de la fraude fiscale grave (voir encadré 14).

Encadré 14 – L'action horizontale relative à la publication des « *Panama Papers* » et l'audition du Gouverneur devant la Commission spéciale au sein de la Chambre des représentants

Dans les jours suivants la publication dans la presse, en avril 2016, d'une liste de montages *off-shore* constitués à l'intervention d'un bureau d'avocats panaméens dans un but de fraude ou d'évasion fiscales (la publication des « *Panama Papers* »), et compte tenu de la possibilité que certaines institutions financières belges aient pu prendre part à quelque titre que ce soit à l'élaboration ou à l'utilisation de tels mécanismes fiscaux particuliers, la Banque a mené une action horizontale visant à s'assurer du respect par les institutions qui relèvent de ses compétences, d'une part, de leurs obligations en matière d'interdiction et de prévention des mécanismes particuliers ayant pour but ou pour effet de favoriser la fraude fiscale de leurs clients, et d'autre part, de l'application effective des mécanismes requis pour la prévention du blanchiment de capitaux issus, en particulier, de la fraude fiscale grave. Dans un premier temps, la Banque a requis de toutes ces institutions financières qu'elles répondent dans un bref délai à un certain nombre de questions visant à recenser celles d'entre elles qui auraient pu avoir aidé leurs clients à monter des sociétés écrans dans des paradis fiscaux, et à savoir si leurs systèmes de contrôle internes avaient mis en lumière des opérations suspectes liées à ces mécanismes fiscaux particuliers. À la suite de l'analyse des réponses, des entretiens ont été organisés avec les représentants de certaines institutions financières. Bien que cette action n'ait pas conduit la Banque à prendre des mesures importantes, les informations recueillies dans le cadre de cette action horizontale seront également prises en compte dans l'évaluation des risques sur laquelle repose l'exercice du contrôle prudentiel en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme (cf. *supra*).

Lors de son audition devant la Commission spéciale « fraude fiscale internationale/*Panama Papers* » au sein de la Chambre des représentants, le Gouverneur de la Banque a souligné la nécessité d'une plus grande harmonisation, notamment européenne, sur le plan des deux tâches spécifiques touchant aux *Panama Papers*, à savoir la lutte contre les mécanismes fiscaux particuliers ainsi que la définition des infractions sous-jacentes au blanchiment de capitaux, comme, par exemple, la fraude fiscale. Par leur nature (lien avec des dispositions fiscales en ce qui concerne la prévention de mécanismes particuliers et avec des dispositions pénales s'agissant du dispositif de lutte contre le blanchiment de capitaux), ces deux tâches ont toutefois un caractère territorial : les dispositions concernant les mécanismes particuliers sont spécifiques à notre pays et ne reposent sur aucun socle européen commun, tandis que, pour la lutte contre le blanchiment, la définition des délits sous-jacents n'est pas encore harmonisée. A défaut d'harmonisation européenne, au regard du caractère territorial de ces dispositions, la Banque en sa qualité d'autorité de contrôle ne dispose d'aucune compétence lui permettant d'agir contre ce type de montage auprès d'une filiale étrangère d'une institution financière belge. Un pas important sera franchi lors de la transposition par les États membres de la 4e directive précitée qui aura pour effet de reconnaître, dans tous les États membres, la fraude fiscale grave comme un délit sous-jacent au blanchiment de capitaux. En outre, les groupes de sociétés, en ce compris transfrontaliers, devront définir une approche globale en matière de lutte contre le blanchiment de capitaux applicable à l'ensemble des entités du groupe.

Dans son rapport remis à la Commission spéciale, la Banque a plaidé pour un renforcement de la collaboration au niveau international entre les différentes autorités compétentes en matière de lutte contre le blanchiment de capitaux et le financement du terrorisme : pour la mise en place d'un système de donneurs d'alerte au sein des entités assujetties : pour un renforcement des fonctions de *compliance* ou encore pour l'assujettissement à la loi du 11 janvier 1993 relative à la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme des entreprises de conseil en matière de structure du capital, de stratégie industrielle et de conseils et services dans le domaine de la fusion et du rachat d'entreprises.

1.3 Devoirs de vigilance à l'égard des demandeurs d'asile

Devant l'afflux de demandeurs d'asiles que connaît l'Europe, l'ABE a publié le 12 avril 2016 un avis[1] par lequel elle fournit des orientations aux établissements financiers sur la manière dont ils peuvent se conformer à leurs obligations légales en matière de LBC/FT, sans devoir refuser à des demandeurs d'asile l'accès au système financier. Ces orientations se fondent sur la considération qu'il est important que ces demandeurs d'asile puissent avoir accès au système financier pendant leur séjour en Europe, non seulement parce qu'un tel accès constitue une condition indispensable à leur intégration dans la vie sociale pendant leur séjour en Europe, mais également afin d'éviter qu'à défaut, des prestataires irréguliers de services financiers qui s'efforcent de se soustraire à tout contrôle, notamment en matière de LBC/FT, ne puissent y trouver des opportunités de développer des activités illicites en proposant leurs services à ces personnes en situation précaire, de sorte que les risques de blanchiment de capitaux et de financement du terrorisme auxquels l'Europe est confrontée s'en trouveraient encore accrus.

La Banque a relayé cet avis de l'ABE auprès de l'ensemble des institutions financières par une circulaire[2] qui précise les modalités d'application en Belgique des principes promus par l'ABE, par référence aux dispositions légales et réglementaires belges telles que commentées dans la circulaire CBFA_2010_09 du 6 avril 2010 relative aux devoirs de vigilance à l'égard de la clientèle, la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, et la prévention du financement de la prolifération des armes de destruction massive (version coordonnée)[3].

2. Assurance qualité (*Quality assurance*)

La Banque s'est dotée au cours de l'année 2016 d'une nouvelle fonction d'assurance qualité qui vient en complément de son arsenal existant d'outils de maîtrise de la qualité de ses activités de supervision financière. Cette fonction, qui se positionne dans la deuxième ligne au sein du modèle de trois lignes de défense de la Banque[4], a pour objectif de donner l'assurance que la supervision financière de la Banque répond aux exigences de qualité en la matière, qui s'envisagent selon les quatre dimensions suivantes : « homogénéité et consistance », « respect des délais », « contenu » et « conformité » avec le dispositif réglementaire et les « bonnes pratiques » (*best practices*) qui font la promotion d'une supervision efficace, efficiente et rigoureuse.

Le périmètre d'intervention de cette nouvelle fonction comprend l'ensemble des activités de supervision financière de la Banque, qu'elle agisse en tant qu'autorité de résolution ou en tant qu'autorité en charge des aspects de réglementation et de contrôle (macro- et micro-)prudentiel et ce, qu'elle exerce ses responsabilités sur le secteur des banques, des assurances ou des infrastructures de marchés financiers. En particulier dans le contexte du MSU, la nouvelle fonction d'assurance qualité de la Banque collabore activement avec ses homologues à la BCE et dans d'autres autorités nationales, afin de couvrir de la manière la plus adéquate ce périmètre spécifique. En ligne avec les modalités de coopération mises en place au sein du MSU, il est ainsi prévu que les fonctions d'assurance qualité des autorités nationales soient directement responsables pour ce qui est de garantir la qualité des travaux réalisés par leur autorité respective sur le périmètre des établissements de crédit de moindre importance, et qu'elles assistent leur homologue à la BCE dans ses travaux en la matière sur le périmètre des établissements importants.

La démarche de cette nouvelle fonction correspond à la démarche de supervision financière de la Banque, qui s'inscrit dans une approche fondée sur les risques, tout en veillant en particulier à ce que la Banque réponde aux attentes de la BCE en termes d'assurance qualité dans le cadre du MSU.

Dans ce contexte, les premiers travaux d'assurance qualité sont actuellement réalisés dans le domaine de la supervision des banques, et en priorité sur le périmètre des établissements de crédit de moindre importance. Ce type de démarche, de type « projet », fait partie des outils à la disposition de la fonction d'assurance qualité qui comprennent également la mise en place et le suivi d'outils de monitoring permanents de la qualité de la supervision financière en général, ou la réalisation de missions *ad hoc*. Le projet d'assurance qualité actuellement en cours a pour objectif de répertorier, de compléter (si nécessaire) et

(1) « *Opinion of the European Banking Authority on the application of customer due diligence measures to customers who are asylum seekers from higher-risk third countries or territories* », EBA-Op-2016-07.

(2) Circulaire NBB_2016_32 du 12 juillet 2016 relative à l'avis de l'Autorité bancaire européenne (ABE) « *on the application of customer due diligence measures to customers who are asylum seekers from higher-risk third countries* » (EBA-Op-2016-07).

(3) Circulaire CBFA_2010_09 du 6 avril 2010 modifiée par la circulaire CBFA_2011_09 du 1 mars 2011 relative aux devoirs de vigilance à l'égard de la clientèle, la prévention de l'utilisation du système financier aux fins du blanchiment de capitaux et du financement du terrorisme, et la prévention du financement de la prolifération des armes de destruction massive (version coordonnée).

(4) La gouvernance de la Banque prévoit un modèle de maîtrise de ses risques qui s'appuie sur trois lignes de défense. Il appartient ainsi au Comité de direction et au management opérationnel, en tant que première ligne de maîtrise des risques, d'endosser et de gérer ceux-ci au travers de la mise en œuvre d'un système de contrôle interne approprié et efficace. La deuxième ligne de maîtrise des risques définit le cadre de gestion des risques de la Banque, aide à sa mise en œuvre au sein de la première ligne et veille à ce que la mise en œuvre par celle-ci soit adéquate et effective. Dans le cadre de ce modèle, l'Audit interne agit en tant que troisième ligne, indépendante, qui applique une approche systématique et méthodique visant à évaluer les processus de contrôle interne, de gestion des risques, et de gouvernance, et à formuler des recommandations pour les améliorer.

d'améliorer (si nécessaire) les processus, procédures et contrôles appliqués au sein de la première ligne de défense en charge de la supervision des établissements de moindre importance et, dès lors, de veiller à ce que le cadre mis en place garantisse une supervision de qualité, conforme aux quatre dimensions énoncées ci-avant.

3. FinTech

Ces dernières années, sous l'impulsion des technologies émergentes toujours plus abordables, le secteur financier a été confronté à une multitude d'innovations. L'entrée sur le marché d'un grand nombre de nouveaux acteurs dont le modèle d'entreprise est basé sur ces innovations est corroborée par une croissance considérable des montants de capitaux à risque investis dans ces nouveaux arrivants et leur technologie financière. L'évolution des préférences des consommateurs vient encore amplifier ce phénomène. Cette tendance est également connue sous le nom de « révolution *FinTech* », *FinTech* étant un terme générique qui désigne toutes les innovations financières menant à de nouvelles applications, de nouveaux processus ou de nouveaux produits qui ont une incidence importante sur les marchés financiers et les établissements existant et sur la fourniture de services financiers au sens large.

Les innovations *FinTech* s'adressent en général à des segments de marché où les attentes des clients ne sont pas entièrement satisfaites alors qu'une marge intéressante est réalisée. Dans différents segments du secteur financier apparaissent de nouveaux acteurs *FinTech* porteurs d'un modèle d'entreprise innovant, tels que le *crowdfunding*, les prêts *peer-to-peer*, les modes alternatifs de transferts et de paiements internationaux, le conseil robotisé, les nouvelles plateformes de commerce électronique, etc. Ces changements auront indéniablement des retombées positives, telles qu'une expérience client améliorée, des frais de transactions moins élevés et un élargissement de la fourniture de services à des segments de clientèle qui n'étaient jusqu'alors pas ou insuffisamment servis. Simultanément, une nouvelle forme d'offre de services de soutien est en train de voir le jour, laquelle consiste pour les acteurs *FinTech* à s'adresser à des intervenants existants et à proposer certains processus opérationnels plus efficaces, plus sûrs ou meilleurs, tels que les solutions de *cloud computing*, la possibilité d'identifier des clients par voie électronique, les logiciels d'analyse de données qui permettent d'étudier le comportement des clients ainsi que les solutions de « registres distribués » (*distributed ledger*), grâce auxquelles il est possible de travailler sans intermédiaire et de conclure des transactions de manière plus sûre et plus efficace.

L'incidence potentiellement disruptive de ces évolutions *FinTech* sur les établissements financiers existants a fait l'objet de nombreux débats au cours des dernières années et a mené, entre autres, les autorités de contrôle, les autorités de réglementation et les établissements financiers à faire quantité de projections. Un premier scénario, qui est aussi le plus extrême, prévoit que les établissements financiers actuels disparaissent complètement et que de nouveaux acteurs numériques prennent leur place. Dans un deuxième scénario, les services sont fournis par l'intermédiaire d'acteurs *FinTech* qui proposent en direct des produits financiers (alternatifs), ce qui entraînerait une désintermédiation des établissements financiers. Songeons à ce sujet aux initiatives prises dans le secteur financier par des géants de la technologie tels que Google, Facebook, Apple, Amazon, Samsung, Alibaba,… Dans ce scénario, les établissements financiers existants procurent à ces nouveaux acteurs des services tels que la mise à disposition de leur infrastructure, le dévelopement de produits, la prise en charge de la conformité au cadre réglementaire, etc. Dans un troisième scénario, les établissements financiers parviennent – grâce éventuellement à une reprise ou à une intégration de nouveaux acteurs ou en collaborant avec ceux-ci – à élaborer eux-mêmes des modèles d'entreprise répondant aux attentes des clients. Ils parviennent ainsi à maintenir la relation client. Au stade actuel, il est impossible de prévoir à quelle vitesse un scénario donné va se réaliser et quelles en seront les conséquences. Dans la pratique, l'on assistera vraisemblablement à une conjonction de ces différents scénarios et le résultat variera probablement selon le segment de marché.

L'évolution *FinTech* est aussi susceptible de comporter de nouveaux risques, notamment pour la rentabilité des établissements financiers existants, qui risquent de perdre certaines activités rentables au profit des nouveaux arrivants, et ce alors que leur rentabilité est déjà mise sous pression dans les circonstances actuelles. Face à ces évolutions, les établissements financiers sont tenus d'adopter une politique de vigilance de manière à pouvoir intégrer rapidement les innovations utiles dans leur modèle d'entreprise et adapter leur stratégie à ces innovations. Ces changements font également naître de nouveaux risques opérationnels, liés à une dépendance accrue vis-à-vis des systèmes informatiques ainsi qu'à l'accroissement attendu de l'externalisation d'activités à de nouveaux acteurs qui ne connaissent pas le cadre réglementaire. Il convient d'accorder une attention particulière à la protection des données et de la vie privée, ainsi qu'à la fiabilité et l'extensibilité de ces nouvelles technologies et applications. En l'occurrence, il s'agit de trouver un juste équilibre entre le confort de l'utilisateur, d'une part, et la limitation des risques opérationnels, d'autre part. Il importe en outre d'établir une structure de gestion claire où les rôles et les

obligations sont bien définis. Par ailleurs, de nouveaux défis apparaissent, comme la détection d'éventuelles erreurs dans les algorithmes utilisés, l'identification des clients lors de transactions à distance et la détection d'opérations de blanchiment à l'aide de nouvelles technologies. Dans une perspective plus large, des questions se posent quant à la protection du consommateur et des données personnelles, et ce eu égard au fait qu'à l'avenir ce seront des entreprises à la base non financières qui offriront de plus en plus souvent des services financiers.

La Banque constate qu'un nombre relativement restreint de nouveaux acteurs ont à ce jour introduit une demande d'agrément pour des modèles d'entreprise en lien avec les *FinTech*, alors que la plupart des acteurs existants offrent déjà des services aux client par le biais d'applications mobiles. En outre, des initiatives sont mises en place pour rendre la gestion de l'architecture informatique plus efficace, entre autres grâce à des solutions de *cloud computing*. Dans beaucoup de cas, il s'avère que les nouveaux acteurs collaborent avec les banques traditionnelles et n'ambitionnent pas de développer eux-mêmes une gamme complète d'activités bancaires. S'agissant des IMF, la Banque constate qu'elles se trouvent dans une phase exploratoire, et examinent dans quelle mesure des applications FinTech leur permettraient d'accroître l'efficacité et la pertinence des processus existants. Tant les banques que les IMF étudient de même les avantages possibles des technologies de « registres distribués » et d'analyse des données. Par une analyse des données générales de transactions, les banques pourront élaborer une offre personnalisée pour leurs clients et ainsi améliorer leur offre de services. S'agissant des clients des infrastructures, les nouvelles technologies offriront des solutions permettant de mieux respecter leurs obligations de conformité (*compliance*). De plus, les techniques d'analyse de données permettront de détecter rapidement des schémas de transactions suspects et ainsi de limiter autant que possible l'impact de ces fraudes. Via sa révision de sa directive sur les services de paiement (Payment Services Directive, PSD2 [1]), l'Union européenne a ouvert le marché à des entreprises qui donnent aux consommateurs et aux fournisseurs de services l'accès à des informations relatives aux comptes bancaires. La Banque constate que le nouveau statut de prestataire de services d'initiation de paiement rencontre un vif intérêt. Ces prestataires font office de passerelle virtuelle entre un donneur d'ordre et son compte bancaire en ligne. Ils indiquent de plus si le solde du compte du donneur d'ordre est suffisant et si la transaction sous-jacente peut donc s'effectuer.

(1) Directive (UE) n° 2015/2366 du Parlement européen et du Conseil du 25 novembre 2015 concernant les services de paiement dans le marché intérieur, modifiant les directives 2002/65/CE, 2009/110/CE et 2013/36/UE et le règlement (EU) n° 1093/2010 et abrogeant la directive 2007/64/CE.

Sous l'angle réglementaire et du contrôle, il importe que tant les établissements existants que les nouveaux acteurs trouvent un juste équilibre entre éviter de ralentir inutilement l'innovation et maîtriser les risques. Parmi les points d'attention à cet égard figure entre autres le fait que la *FinTech* met à mal le modèle de revenus traditionnel, ce qui peut mettre en péril la stabilité d'établissements individuels et, par extension, le système financier. Il est donc important que les nouveaux acteurs soient dotés de l'intégrité nécessaire et disposent d'un capital de départ suffisant. Il convient également d'assurer la stabilité et la sécurité des systèmes informatiques et de prendre en compte les aspects « vie privée » lors de l'utilisation des nombreuses bases de données connectées (*big data* ou mégadonnées). À la fin de 2015, la Banque a mis sur pied un groupe de travail interne qui est entre autres chargé d'examiner quel sera l'impact de la *FinTech* sur les modèles d'entreprise des établissement existants et sur les risques prudentiels.

Par ailleurs, dans le cadre du HLEG, la Banque participe en collaboration avec le législateur à différentes initiatives qui ont pour but d'adapter le cadre règlementaire à ce nouvel environnement financier évolutif. En coopération avec la FSMA, la Banque a par exemple entamé une analyse de la réglementation afin d'éliminer les entraves superflues aux modèles d'entreprise innovants. La Banque prépare en outre un point de contact central pour les initiatives *FinTech* venant d'acteurs tant existants que nouveaux. Au travers d'un dialogue actif avec les intervenants de marché, ce point de contact central suivra de près les innovations en évolution rapide et parfois complexes et répondra aux questions relatives à la réglementation, au contrôle et aux agréments. De par la nature de la révolution *FinTech*, il va de soi que la réponse apportée par les autorités de contrôle doit être coordonnée et développée à un niveau européen et même paneuropéen. La Banque collabore à cet effet au sein de plusieurs institutions internationales à la mise au point d'une réglementation à jour qui tient adéquatement compte des risques prudentiels et qui garantit la stabilité du système financier sans toutefois limiter les chances et les opportunités indissolublement liées aux innovations *FinTech*. Dans ce cadre, la Banque participe à différents groupes de travail traitant entre autres des modalités d'agrément applicables aux acteurs *FinTech*, des exigences liées à la sous-traitance d'activités et de l'adéquation du cadre prudentiel existant, et ce en tenant compte des innovations *FinTech*.

4. Cyber-risques

Le secteur financier est déjà fortement informatisé et la numérisation de ses processus d'entreprise poursuit

encore sa progression. Le degré d'interconnexion entre les processus opérationnels des différents intervenants financiers est également très élevé. Les établissements financiers optent de surcroît de plus en plus souvent pour des modèles d'entreprise qui sous-traitent les services informatiques, selon une spécialisation opérationnelle ou fonctionnelle. Cette numérisation plus poussée et plus diversifiée des canaux d'accès des clients particuliers des banques n'est que l'un des aspects dont l'analyse du risque opérationnel dans les établissements financiers et les IMF doit tenir compte.

Au cours de l'année sous revue, tout comme durant les années précédentes, les cyber-risques ont fait l'objet d'une attention toujours plus soutenue dans le secteur financier. L'évaluation et la promotion de la maîtrise des cyber-risques figurent en tête des priorités du contrôle prudentiel et de l'*oversight* exercés vis-à-vis des établissements financiers et des IMF. Le secteur a été encouragé à continuer à renforcer ses mesures et efforts de protection contre les cyber-risques, en tenant compte des stratégies de gestion du cyber-risque qui se développent de manière intersectorielle en Belgique et à l'étranger.

4.1 Poursuite de la hausse des cybermenaces

Les cyberattaques sont de plus en plus sophistiquées et provoquent toujours davantage de dégâts. Le nombre d'attaques portant atteinte à l'intégrité des systèmes et des données informatiques progresse également. En tant qu'autorité prudentielle, la Banque en conçoit des inquiétudes. Elle s'intéresse dans ce domaine avant tout à la sécurisation des établissements financiers et des IMF individuels et de l'ensemble du secteur, ainsi qu'à la confiance qu'ils inspirent. La sécurisation opérationnelle et la robustesse des services critiques pour le bon fonctionnement du secteur sont à cet égard d'une importance cruciale.

L'approche du cyber-risque est double. D'une part, les établissements sont tenus de détenir des fonds propres en couverture de leurs risques opérationnels, dont font partie les cyber-risques. D'autre part, la sûreté opérationnelle et la robustesse des processus critiques des établissements financiers et des IMF sont surveillées de près. La disponibilité et l'intégrité des systèmes informatiques jouent un rôle central en la matière.

Les cyber-attaques peuvent être internes ou externes à l'établissement et les motifs des attaquants peuvent être divers, allant du vol financier à l'espionnage et au sabotage géostratégiques en passant par le terrorisme. Les infrastructures et les établissements financiers éprouvent pour cette raison beaucoup de peine à protéger parfaitement leurs systèmes, données et services informatiques contre les attaques de tous types. Comme les cybermenaces évoluent très rapidement, il convient de s'assurer que la capacité défensive des établissements et des IMF soit plus que jamais en mesure de réagir avec souplesse aux changements de schémas des attaques. Il est essentiel de détenir des solutions permettant de rassembler des informations sur les menaces potentielles, les attaquants et les types d'attaque. Pour se protéger de cyber-attaques portant atteinte à l'intégrité des systèmes et données informatiques, les établissements financiers doivent disposer, à côté des systèmes classiques de continuité reposant sur des centres de données distincts, de mécanismes adéquats de redémarrage.

4.2 Recommandations en matière de cyber-résistance

La circulaire prudentielle relative aux attentes de la Banque en matière de continuité et de sécurité opérationnelles des établissements d'importance systémique est entrée en vigueur le 1er janvier 2016 (1). Cette circulaire se focalise particulièrement sur la cyber-résistance (*cyber resilience*). Au mois de juin 2016, le CPIM et l'OICV ont publié des recommandations (2) concernant la cyber-résistance, d'application immédiate pour les IMF. La Banque contrôlera si les IMF établies en Belgique les respectent.

L'un des principaux points d'attention de cette circulaire prudentielle et des directives en matière d'*oversight* est la gestion des cyber-risques par les acteurs financiers. La maîtrise des cyber-risques n'implique pas seulement que l'on se concentre sur la technologie, mais nécessite aussi que l'on se penche suffisamment sur les menaces internes à l'entreprise, provenant d'employés ou de la direction. Les intervenants financiers doivent mettre leurs collaborateurs au courant des cyber-risques, de manière à ce qu'ils sachent comment ces risques peuvent surgir et comment il convient qu'ils réagissent. Les organes de gestion doivent disposer de l'expertise et des informations nécessaires pour pouvoir suivre adéquatement les cybermenaces et les maintenir dans des limites acceptables.

Les deux directives précitées recommandent également que les acteurs financiers réalisent des tests afin d'évaluer leur degré de protection contre les cybermenaces. Ces tests sont de plus en plus sophistiqués et s'appuient, dans certaines juridictions, sur des cadres spécifiques comportant une méthodologie de test harmonisée. La Banque

(1) Circulaire NBB_2015_32 du 18 décembre 2015 concernant les attentes prudentielles complémentaires en matière de continuité et de sécurité opérationnelles des établissements financiers d'importance systémique.
(2) *Guidance on cyber resilience for financial market infrastructures.*

surveille les évolutions dans ce domaine afin que de saines pratiques de gestion soient également introduites en Belgique, en tenant compte d'éventuelles initiatives européennes ou internationales en la matière.

La Banque suit également les avancées en la matière réalisées en dehors du secteur financier. Ainsi, le G7 a publié des lignes directrices portant sur un cadre adéquat de maîtrise des cyber-risques et plusieurs pays mettent sur pied une cyber-stratégie nationale pour les principaux secteurs, dont le secteur financier fait la plupart du temps partie.

4.3 Sélections choisies (*Capita selecta*)

SWIFT

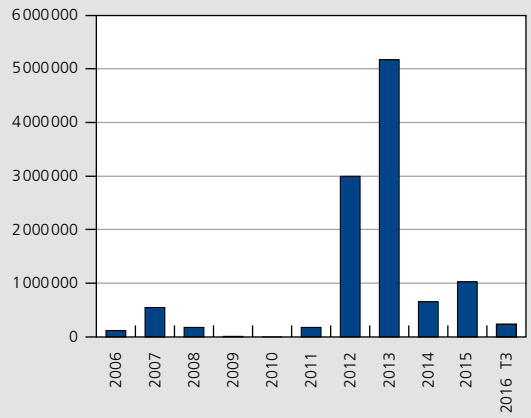
La Banque est le contrôleur principal de SWIFT et exerce cet *oversight* en collaboration avec d'autres banques centrales du G10. Cette année, une attention particulière a été réservée à la cyber-attaque au cours de laquelle 81 millions de dollars ont été dérobés à la Banque centrale du Bangladesh, ainsi qu'à d'autres cas rapportés par la presse où des établissements financiers ont été victimes de messages SWIFT frauduleux. Les systèmes centraux de traitement d'opérations de SWIFT n'ont jamais été menacés au cours de ces attaques mais les malfaiteurs ont exploité des failles de sécurité au sein des établissements financiers qui participent à SWIFT. Ces piratages démontrent combien il est important que les établissements financiers membres de SWIFT se dotent de mécanismes adéquats de cyberdéfense. Pour les y aider, SWIFT a mis sur pied un vaste programme de soutien et de conseil à ses clients, suivi de près par les banques centrales du G10 chargées de son *oversight*.

Fraude dans les services bancaires par internet (e-banking) et par téléphone

Febelfin et la *Federal Computer Crime Unit*, notamment, ont poursuivi en 2016 leur collaboration étroite entamée ces dernières années afin de limiter la fraude en *e-banking*. Il est relevé que, grâce aux efforts des établissements financiers et à quelques interventions fructueuses des services de police et de l'appareil judiciaire belges, le niveau des pertes financières annuelles dues à la fraude en *e-banking* au cours des trois dernières années est resté faible.

Comme lors des années précédentes, les cas enregistrés de fraude en *e-banking* auprès des particuliers en 2016 étaient quasi exclusivement imputables à des techniques de fraude par lesquelles les cybercriminels trompent les utilisateurs d'*e-banking* pour obtenir leurs codes de sécurité personnels (le plus souvent après un contact téléphonique ou par l'intermédiaire d'un site internet frauduleux). Les établissements analysent les transactions illicites une à une et remboursent les victimes, sauf en cas de négligence grave ou d'intention frauduleuse de leur part.

GRAPHIQUE 107 PERTE FINANCIÈRE ANNUELLE PROVOQUÉE PAR LA FRAUDE EN E-BANKING EN BELGIQUE
(en euros)



Source : Febelfin.