F. Sectoroverschrijdende aspecten van prudentiële regelgeving en toezicht

De Bank is als prudentieel toezichthouder bevoegd voor een aantal domeinen die meerdere sectoren betreffen en bijgevolg niet werden behandeld bij de bespreking van de banken, de verzekeringsondernemingen of de FMI's in dit Verslag. Zo heeft de Bank in de voorbije jaren actief deelgenomen aan de nationale en internationale werkzaamheden ter bestrijding van het witwassen van geld en de financiering van terrorisme en heeft zij hiertoe tijdens het verslagjaar haar interne organisatie aangepast en versterkt, in het verlengde van de in 2015 geformuleerde aanbeveling van de Financiële Actiegroep (FAG). Tevens werden horizontale toezichtacties ondernomen met betrekking tot de tenuitvoerlegging van financiële sancties tegen terroristen en terroristische organisaties en van maatregelen tot voorkoming van bijzondere fiscale mechanismen en het witwassen van geld afkomstig van ernstige fiscale fraude in het kader van het onderzoek naar de 'Panama Papers'.

Tijdens het verslagjaar heeft de Bank ook een nieuwe kwaliteitswaarborgingsfunctie in het leven geroepen. Deze functie moet ervoor zorgen dat het financieel toezicht voldoet aan de kwaliteitsvereisten bepaald door het GTM.

De technologische ontwikkelingen in de financiële sector hebben verder geleid tot de intrede op de markt van nieuwe spelers die hun bedrijfsmodel baseren op financiële innovaties. Deze FinTech-spelers gebruiken nieuwe applicaties, processen of producten en oefenen hiermee een materiële invloed uit op de bestaande financiële markten en instellingen en op de financiële dienstverlening in de brede zin. Een interne werkgroep van de Bank heeft tijdens het verslagjaar de impact op de bestaande bedrijfsmodellen en op de prudentiële risico's opgevolgd.

Cyberaanvallen worden alsmaar geavanceerder en richten steeds meer schade aan. De Bank besteedde bijzondere aandacht aan het cyberrisicobeheer in individuele financiële instellingen en FMI's en in de sector als geheel. De inspanningen ter verbetering van de cyberweerbaarheid werden verder opgedreven, met specifieke aandacht voor het beheer van het risico door de financiële actoren en voor het uitvoeren van tests om de mate van bescherming tegen aanvallen te beoordelen.

1. Bestrijding van het witwassen van geld en de financiering van terrorisme

1.1 Follow-up van de wederzijdse evaluatie van België door de FAG : voortzetting van de reorganisatie van het toezicht

Teneinde passend te reageren op de door de FAG geformuleerde kritiek op het niveau van overeenstemming van de Belgische wet- en regelgeving met de nieuwe FAG-normen, en gelet op de beslissing die de Belgische regering na de aanslagen in Parijs van 13 november 2015 heeft genomen om de vierde Europese Richtlijn inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering[1] zo vroeg mogelijk om te zetten, was de Bank, samen met de

(1) Richtlijn (EU) 2015/849 van het Europees Parlement en de Raad van 20 mei 2015 inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, tot wijziging van Verordening (EU) nr. 648/2012 van het Europees Parlement en de Raad en tot intrekking van Richtlijn 2005/60/EG van het Europees Parlement en de Raad en Richtlijn 2006/70/EG van de Commissie, Publicatieblad van de Europese Unie, L 141 van 5 juni 2015.

andere betrokken overheden, nauw betrokken bij de werkgroep die was belast met de uitwerking, binnen de korte termijn die haar was toegekend, van een voorontwerp van wet tot omzetting van de voornoemde richtlijn, dat voldoet aan alle in deze richtlijn geformuleerde vereisten en de Belgische wetgeving zo goed mogelijk in overeenstemming brengt met de 40 FAG-aanbevelingen.

Voorts heeft de Bank in 2016, zoals in haar jaarverslag 2015 was aangekondigd, haar interne organisatie aangepast om de efficiëntie te verbeteren van de controles op het gebied van de strijd tegen het witwassen van geld en de financiering van terrorisme (SWG/FT), die ze dient uit te voeren bij de financiële instellingen waarvoor ze bevoegd is. Zo werd een gespecialiseerde groep opgericht die verantwoordelijk is voor zowel de werkzaamheden met betrekking tot de vaststelling van het prudentieel beleid ter zake als het off-site toezicht op de financiële instellingen, en die daarbij hechte betrekkingen handhaaft met, enerzijds, de diensten belast met het algemeen off-site toezicht en, anderzijds, de dienst belast met de inspecties ter plaatse. Naast het feit dat de centralisatie van de taken inzake off-site toezicht binnen een team van specialisten er op zich garant voor staat dat de Bank meer aandacht besteedt aan de uitoefening van deze toezichtsopdracht, werden er in 2016 reeds aanzienlijk meer middelen specifiek hiervoor toegewezen, zowel binnen het team voor off-site toezicht als binnen de dienst die is belast met de inspecties ter plaatse. Verwacht wordt dat de middelen in 2017 nog verder zullen worden opgetrokken.

Al deze maatregelen hebben ertoe geleid dat de Bank bij de uitoefening van het off-site toezicht vaker contact heeft opgenomen met de financiële instellingen, en dat het aantal inspecties ter plaatse aanzienlijk is toegenomen. Deze toezichtacties beogen er in de eerste plaats voor te zorgen dat de rechtstreeks betrokken instellingen een passende oplossing vinden voor de specifieke tekortkomingen die bij hen zijn vastgesteld. Daarnaast zal de verscherping van de SWG/FT-controles, die in 2017 zal worden voortgezet en die zal worden gecombineerd met de hervorming van het wettelijke en reglementaire kader als gevolg van de omzetting van de vierde Europese Richtlijn, er ook toe leiden dat alle financiële instellingen bewuster zullen worden gemaakt van de absolute noodzaak om over efficiënte interne mechanismen inzake SWG/FT te beschikken.

Een van de in deze context door de Bank nagestreefde doelstellingen bestaat erin de uitoefening van het toezicht ter zake meer systematisch te baseren op een analyse van de specifieke risico's met betrekking tot het witwassen van geld en de financiering van terrorisme waaraan de financiële instellingen onder toezicht zijn blootgesteld. Hiertoe zijn reeds maatregelen genomen, met name op basis van de door de financiële instellingen verstrekte antwoorden op de jaarlijkse vragenlijst die zij dienen in te vullen[1], van de jaarverslagen van hun verantwoordelijken voor de SWG/TF, en van de informatie waarover de Bank beschikt in het kader van de uitoefening van haar bevoegdheden inzake prudentieel toezicht. Het is echter van belang dat deze toezichtsbenadering, waarop de Bank een beroep zal doen, strookt met de praktijken die in de andere lidstaten van de Europese Unie ten uitvoer zullen worden gelegd. Bijgevolg heeft de Bank actief deelgenomen aan de uitwerking van de richtsnoeren die krachtens de voornoemde vierde Richtlijn door de Europese toezichthoudende autoriteiten moeten worden opgesteld. De recente publicatie van deze richtsnoeren[2] zal de Bank in staat stellen haar eigen model voor de analyse van de risico's verder uit te werken en erover te waken dat deze praktijken afgestemd worden op die van de andere nationale autoriteiten in Europa.

1.2 Horizontale toezichtacties inzake de bevriezing van de tegoeden van terroristen en 'Panama Papers'

Na de terroristische aanslagen van 13 november 2015 in Frankrijk en van 22 maart 2016 in België besloot de Bank een horizontale toezichtactie uit te voeren met betrekking tot de organisatie die alle financiële instellingen hebben opgezet om te voldoen aan hun verplichtingen met betrekking tot de tenuitvoerlegging van de gerichte financiële sancties tegen de terroristen en de terroristische organisaties die zijn opgenomen in de Belgische en Europese lijsten voor de bevriezing van tegoeden en economische middelen. Afgezien van de uit deze horizontale actie voortvloeiende individuele acties om de bij een aantal instellingen vastgestelde leemten op te vullen, achtte de Bank het bijzonder nuttig al deze instellingen bewuster te maken van hun verantwoordelijkheden ter zake. Hiertoe stuurde de Bank hen een brief waarin ze uitlegt welke lessen ze uit haar toezichtactie heeft getrokken, verduidelijking tracht te verschaffen bij sommige aspecten van de geldende wettelijke regeling die onvoldoende begrepen lijken te zijn, en uitdrukking geeft aan haar verwachtingen en aanbevelingen voor een betere toepassing van deze financiële sancties[3].

(1) De nieuwe versie van de periodieke vragenlijst met betrekking tot de bestrijding van het witwassen van geld en de financiering van terrorisme, die de financiële instellingen tussen 1 januari en 28 februari 2017 dienen in te vullen op basis van hun situatie op 31 december 2016, werd hen toegezonden via de circulaires NBB_2016_42 en NBB_2016_43 van 26 oktober 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 November 2016.

(3) De horizontale brief van 6 december 2016 m.b.t. de toepassing van het financieel sanctieregime (anti-terrorismefinanciering) kan geraadpleegd worden op www.nbb.be.

Naar aanleiding van de publicatie van de 'Panama Papers' in de pers, in april 2016, voerde de Bank bovendien een horizontale toezichtactie uit met betrekking tot de tenuitvoerlegging van zowel de maatregelen tot voorkoming van de bijzondere fiscale mechanismen als de maatregelen tot voorkoming van het witwassen van geld afkomstig van ernstige fiscale fraude (zie kader 14).

Kader 14 – Horizontale actie betreffende de publicatie van de 'Panama Papers' en hoorzitting van de Gouverneur voor de Bijzondere commissie binnen de Kamer van Volksvertegenwoordigers

In de dagen na de publicatie in de pers, in april 2016, van een lijst met offshoreconstructies die via een Panamees advocatenkantoor waren opgezet om fiscale fraude of belastingontwijking te plegen (de publicatie van de 'Panama Papers'), en rekening houdend met de mogelijkheid dat sommige Belgische financiële instellingen op enigerlei wijze hebben kunnen deelnemen aan de ontwikkeling of het gebruik van dergelijke bijzondere fiscale mechanismen, heeft de Bank een horizontale actie ondernomen om na te gaan of de instellingen waarvoor zij bevoegd is, voldoen aan hun verplichtingen met betrekking tot het verbod op en de voorkoming van de bijzondere mechanismen die tot doel of gevolg hebben fiscale fraude van hun cliënten te bevorderen, en of ze effectief de mechanismen toepassen die vereist zijn om te voorkomen dat geld afkomstig van, met name, ernstige fiscale fraude wordt witgewassen. In een eerste fase vroeg de Bank al deze financiële instellingen op korte termijn een aantal vragen te beantwoorden, om vast te stellen welke instellingen hun cliënten mogelijk hadden geholpen schermvennootschappen op te richten in belastingparadijzen, en om na te gaan of hun internecontrolesystemen verdachte verrichtingen in verband met deze bijzondere fiscale mechanismen aan het licht hadden gebracht. Na de analyse van de antwoorden werden gesprekken georganiseerd met de vertegenwoordigers van een aantal financiële instellingen. Hoewel deze actie de Bank er niet toe heeft gebracht ingrijpende maatregelen te nemen, zullen de in het kader van deze horizontale actie ontvangen gegevens ook in aanmerking worden genomen voor de risicobeoordeling die ten grondslag ligt aan de uitoefening van het prudentieel toezicht inzake de bestrijding van het witwassen van geld en de financiering van terrorisme (zie hierboven).

Tijdens zijn hoorzitting voor de Bijzondere commissie 'internationale fiscale fraude/Panama papers' binnen de Kamer van Volksvertegenwoordigers heeft de Gouverneur van de Bank benadrukt dat er nood is aan een grotere harmonisatie, onder meer op Europees niveau, op het vlak van de twee toezichtsdimensies die raakvlakken hebben met de Panama Papers, met name de bestrijding van bijzondere fiscale mechanismen en de definitie van de onderliggende misdrijven van het witwassen van geld, bijvoorbeeld fiscale fraude. Beide dimensies hebben immers door hun aard (link met fiscale bepalingen voor de preventie van bijzondere mechanismen en link met strafrechtelijke bepalingen voor het antiwitwasdispositief) een territoriaal karakter : de bepalingen over bijzondere mechanismen zijn specifiek voor ons land en hebben geen gemeenschappelijke Europese basis, terwijl voor de bestrijding van witwassen van geld de onderliggende misdrijven nog niet geharmoniseerd zijn. Bij gebrek aan Europese harmonisatie en gelet op het territoriale karakter van deze bepalingen beschikt de Bank in haar hoedanigheid van toezichthouder over geen enkele bevoegdheid op basis waarvan zij zou kunnen optreden tegen het opzetten van een dergelijke constructie bij een buitenlandse dochteronderneming van een Belgische financiële instelling. Er zal een belangrijke stap worden gezet met de omzetting door de lidstaten van de vierde Europese Richtlijn inzake de voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld of terrorismefinanciering, waardoor ernstige fiscale fraude in alle lidstaten zal worden erkend als een onderliggend misdrijf van het witwassen van geld. Bovendien zullen de ondernemingsgroepen, waaronder de grensoverschrijdende groepen, een algemene antiwitwasbenadering moeten vaststellen die op alle entiteiten van de groep van toepassing is.

In het verslag dat ze aan de Bijzondere commissie heeft bezorgd, pleitte de Bank voor een betere samenwerking op internationaal niveau tussen de verschillende autoriteiten die bevoegd zijn op het vlak van de bestrijding van het witwassen van geld en de financiering van terrorisme ; voor de invoering van een klokkenluidersregeling binnen

de onderworpen entiteiten; voor een versterking van de compliancefuncties en voor de toepassing van de wet van 11 januari 1993 tot voorkoming van het gebruik van het financiële stelsel voor het witwassen van geld en de financiering van terrorisme op ondernemingen die advies verstrekken inzake kapitaalstructuur en bedrijfsstrategie, en die advies en diensten verlenen op het gebied van fusie en overname van ondernemingen.

1.3 Waakzaamheidsplichten ten aanzien van asielzoekers

Gelet op de instroom van asielzoekers in Europa heeft EBA op 12 april 2016 een advies[1] gepubliceerd waarin ze richtsnoeren verstrekt aan de financiële instellingen over de manier waarop ze kunnen voldoen aan hun wettelijke SWG/FT-verplichtingen zonder dat ze asielzoekers de toegang tot het financieel stelsel moeten ontzeggen. Deze richtsnoeren zijn gebaseerd op de overweging dat het belangrijk is dat deze asielzoekers toegang kunnen hebben tot het financieel stelsel terwijl ze in Europa verblijven, niet alleen omdat een dergelijke toegang essentieel is voor hun integratie in het maatschappelijk leven tijdens hun verblijf in Europa, maar ook om te vermijden dat, als ze geen toegang krijgen, niet-gereguleerde financiële dienstverleners die zich trachten te onttrekken aan elke vorm van toezicht, met name op het gebied van SWG/FT, van deze situatie misbruik zouden kunnen maken om onwettige activiteiten te ontwikkelen door hun diensten aan deze kwetsbare personen aan te bieden, wat zou leiden tot een verdere toename van de risico's verbonden aan het witwassen van geld en de financiering van terrorisme waarmee Europa wordt geconfronteerd.

De Bank heeft dit advies van de EBA doorgegeven aan alle financiële instellingen via een circulaire[2], waarin de modaliteiten worden aangegeven voor de toepassing in België van de principes die EBA voorstaat, door te verwijzen naar de Belgische wettelijke en reglementaire bepalingen die worden toegelicht in circulaire CBFA_2010_09 van 6 april 2010 betreffende de waakzaamheidsplicht ten aanzien van het cliënteel, voorkoming van het gebruik van het financiële stelsel voor witwassen van geld en terrorismefinanciering, en voorkoming van de financiering van de proliferatie van massavernietigingswapens (gecoordineerde versie)[3].

2. Kwaliteitswaarborging (Quality assurance)

De Bank heeft in 2016 een nieuwe kwaliteitswaarborgingsfunctie in het leven geroepen, ter aanvulling van haar bestaand arsenaal aan instrumenten voor het beheer van de kwaliteit van haar activiteiten inzake financieel toezicht. Deze functie, die deel uitmaakt van de tweede linie binnen het model met drie verdedigingslinies van de Bank[4], moet ervoor zorgen dat het financieel toezicht van de Bank voldoet aan de kwaliteitsvereisten ter zake, die betrekking hebben op de volgende vier dimensies: homogeniteit en consistentie, naleving van de termijnen, inhoud en compliance met het regelgevend kader en de 'goede praktijken' (best practices) die een effectief, efficient en strikt toezicht bevorderen.

Het interventiegebied van deze nieuwe functie omvat alle activiteiten inzake financieel toezicht van de Bank, zowel in haar hoedanigheid van afwikkelingsautoriteit als in haar hoedanigheid van autoriteit die belast is met de aspecten inzake regelgeving en (macro- en micro-) prudentieel toezicht, ongeacht of deze activiteiten in het kader van haar verantwoordelijkheden met betrekking tot de banksector, de verzekeringssector of de sector van de FMI's worden uitgeoefend. Met name in de context van het GTM werkt de nieuwe kwaliteitswaarborgingsfunctie van de Bank actief samen met haar tegenhangers bij de ECB en bij andere nationale autoriteiten, om dit specifieke interventiegebied op de meest passende wijze te bestrijken. Zo is in overeenstemming met de binnen het GTM ingestelde samenwerkingsregelingen bepaald dat de kwaliteitswaarborgingsfuncties van de nationale autoriteiten rechtstreeks verantwoordelijk dienen te zijn voor het waarborgen van de kwaliteit van de werkzaamheden die

(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 van 12 juli 2016 betreffende de opinie van de Europese Bank Autoriteit (EBA) 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 van 6 april 2010, gewijzigd door de circulaire CBFA_2011 van 1 maart 2011, betreffende de waakzaamheidsplicht ten aanzien van het cliënteel, voorkoming van het gebruik van het financiële stelsel voor witwassen van geld en terrorismefinanciering, en voorkoming van de financiering van de proliferatie van massavernietigingswapens (gecoördineerde versie).

(4) De governance van de Bank voorziet in een risicobeheermodel dat steunt op drie verdedigingslinies. Zo is het de taak van het Directiecomité en het operationeel management, als eerste verdedigingslinie, om de risico's op zich te nemen en te beheren aan de hand van een geschikt en efficiënt internecontrolesysteem. De tweede verdedigingslinie legt het risicobeheerkader van de Bank vast, draagt bij aan de tenuitvoerlegging ervan binnen de eerste linie en ziet erop toe dat deze laatste het kader op passende en doeltreffende wijze ten uitvoer legt. In het kader van dit model treedt de interne audit op als derde, onafhankelijke verdedigingslinie, die een systematische en methodische benadering hanteert om de internecontrole-, risicobeheer- en governanceprocessen te beoordelen en aanbevelingen te formuleren voor de verbetering ervan.

door hun respectieve autoriteiten worden uitgevoerd met betrekking tot de minder belangrijke kredietinstellingen, en dat ze hun tegenhanger bij de ECB moeten bijstaan in diens werkzaamheden ter zake met betrekking tot de belangrijke instellingen.

De aanpak die door deze nieuwe functie gehanteerd wordt, is in overeenstemming met de door de Bank gehanteerde aanpak van het financieel toezicht, die deel uitmaakt van een risicogebaseerde benadering en waarbij er met name over wordt gewaakt dat de Bank voldoet aan de verwachtingen van de ECB op het gebied van kwaliteitswaarborging in de context van het GTM.

Tegen deze achtergrond worden momenteel de eerste werkzaamheden inzake kwaliteitswaarborging uitgevoerd in het domein van het bankentoezicht, in de eerste plaats voor de minder belangrijke kredietinstellingen. Deze projectbenadering maakt deel uit van de instrumenten die ter beschikking staan van de kwaliteitswaarborgingsfunctie. Hiertoe behoren ook de invoering en de follow-up van instrumenten voor permanent toezicht op de kwaliteit van het financieel toezicht in het algemeen, of de uitvoering van ad-hocopdrachten. Het doel van het huidige kwaliteitswaarborgingsproject is de identificatie, de aanvulling (indien nodig) en de verbetering (indien nodig) van de processen, procedures en controles die worden toegepast binnen de eerste verdedigingslinie die belast is met het toezicht op de minder belangrijke instellingen. Bijgevolg beoogt het project ook dat het ingestelde kader een toezicht van hoge kwaliteit kan garanderen conform de vier bovengenoemde dimensies.

3. FinTech

De jongste jaren wordt de financiële sector geconfronteerd met tal van vernieuwingen, onder impuls van technologische innovaties die steeds toegankelijker worden. De intrede op de markt van talrijke nieuwe spelers die hun bedrijfsmodel baseren op deze ontwikkelingen, wordt geschraagd door een aanmerkelijke groei van durfkapitaal dat in deze nieuwkomers en hun financiële technologie wordt geïnvesteerd. Die evolutie wordt daarenboven versterkt door de gewijzigde voorkeuren van de consument. Deze trend wordt ook wel 'de FinTech-evolutie' genoemd, waarbij 'FinTech' de verzamelnaam is voor alle financiële innovaties die leiden tot nieuwe applicaties, processen of producten die een materiële impact hebben op de bestaande financiële markten en instellingen en op de financiële dienstverlening in de brede zin.

FinTech-innovaties richten zich over het algemeen op marktsegmenten waar de verwachtingen van de klant niet volledig worden ingelost terwijl er toch een aantrekkelijke marge wordt gerealiseerd. In diverse segmenten van de financiële sector duiken nieuwe FinTech-spelers op met een innovatief bedrijfsmodel, zoals crowdfunding, peer-to-peerleningen, alternatieve manieren voor transfers en internationale betalingen, gerobotiseerde adviesverlening, nieuwe elektronische handelsplatformen,... Deze ontwikkelingen zullen ontegensprekelijk positieve gevolgen hebben, zoals een verbeterde klantenervaring, lagere transactiekosten en uitbreiding van de dienstverlening naar bepaalde klantensegmenten die voorheen niet of onvoldoende bediend werden. Tegelijkertijd is er ook een nieuwe vorm van ondersteunende dienstverlening aan het ontstaan, waarbij FinTech-spelers zich richten op bestaande actoren en bepaalde bedrijfsprocessen efficiënter, veiliger of beter aanbieden, zoals cloudcomputing-oplossingen, mogelijkheid tot elektronische identificatie van klanten, software voor data-analyse, die toelaat klantengedragingen te analyseren, en 'distributed ledger'-oplossingen, die het mogelijk maken zonder tussenpersonen te werken en transacties veiliger en efficiënter af te handelen.

De potentieel disruptieve impact van deze FinTech-ontwikkelingen op de bestaande financiële instellingen was de voorbije jaren een veel besproken onderwerp en leidde tot tal van projecties door o.a. toezichthouders, regelgevers en financiële instellingen. In een eerste scenario, dat tevens het meest extreme scenario is, verdwijnen de huidige financiële instellingen volledig en wordt hun plaats ingenomen door nieuwe digitale spelers. In een tweede scenario worden de diensten verleend via FinTech-spelers die rechtstreeks (alternatieve) financiële producten aanbieden, waardoor de financiële instellingen gedesintermedieerd worden. We denken hierbij aan initiatieven die in de financiële sector worden genomen door technologiereuzen zoals Google, Facebook, Apple, Amazon, Samsung, Alibaba,… De bestaande financiële instellingen verlenen in dit scenario diensten aan deze nieuwe spelers zoals het ter beschikking stellen van hun infrastructuur, het ontwikkelen van producten, het verzorgen van de compliance met het reglementair kader,... In een derde scenario slagen de financiële instellingen erin – al dan niet door overname, integratie of samenwerking met nieuwe spelers – zelf bedrijfsmodellen te ontwikkelen die beantwoorden aan de vereisten van de klanten. Zo kunnen zij de relatie met de klant behouden. Op dit ogenblik is het onmogelijk te voorspellen hoe snel een bepaald scenario zal optreden en welk effect het zal hebben. In de praktijk zal eerder een combinatie van deze scenario's optreden en kan het resultaat verschillen naargelang van het marktsegment.

De FinTech-evolutie houdt mogelijk ook nieuwe risico's in, met name voor de winstgevendheid van de bestaande

financiële instellingen, aangezien zij bepaalde rendabele activiteiten verliezen aan nieuwe spelers, terwijl hun rentabiliteit in de huidige omgeving reeds onder druk staat. Vandaar dat deze ontwikkelingen een alert beleid vergen van de financiële instellingen, zodat zij nuttige innovaties snel in het bedrijfsmodel kunnen integreren en hun strategie aan deze innovaties kunnen aanpassen. Verder scheppen deze ontwikkelingen ook nieuwe operationele risico's, die verband houden met de verhoogde afhankelijkheid van IT-systemen en de verwachte toename van de uitbesteding van activiteiten aan nieuwe spelers die niet vertrouwd zijn met het reglementair kader. Er dient bijzondere aandacht te worden besteed aan de bescherming van data en privacy, alsook aan de betrouwbaarheid en schaalbaarheid van deze nieuwe technologieën en toepassingen. Het vinden van een goed evenwicht tussen het gebruikersgemak enerzijds en de inperking van de operationele risico's anderzijds is belangrijk hierbij. Daarnaast is een heldere beleidsstructuur met duidelijke rollen en verplichtingen van groot belang. Tevens ontstaan er nieuwe uitdagingen, zoals de detectie van mogelijke fouten in gebruikte algoritmen, klantenidentificatie voor verrichtingen op afstand en detectie van witwasverrichtingen aan de hand van nieuwe technologieën. Vanuit een ruimer perspectief zijn er ook vraagstukken op het gebied van de bescherming van de consument en de persoonsgegevens, in het bijzonder omdat van oorsprong niet-financiële ondernemingen steeds vaker financiële diensten zullen aanbieden.

De Bank stelt vast dat tot op heden een relatief gering aantal nieuwe spelers een licentie heeft aangevraagd voor FinTech-gerelateerde businessmodellen, terwijl de meeste bestaande spelers werken aan een verbetering van de klantenervaring via mobiele apps. Daarnaast worden initiatieven ontwikkeld voor het efficiënter beheren van de IT-architectuur via o.a. cloudcomputing-oplossingen. In veel gevallen wordt vastgesteld dat de nieuwe spelers samenwerken met de traditionele banken en niet de ambitie hebben om zelf een volledig gamma aan bankactiviteiten te ontwikkelen. Met betrekking tot de FMI's stelt de Bank vast dat ze zich in een exploratiefase bevinden, en nagaan in welke mate zij met FinTech-toepassingen een verhoging van de efficiëntie en doeltreffendheid van de bestaande processen kunnen bereiken. Zowel de banken als de FMI's analyseren ook de mogelijke voordelen van 'distributed ledger'-technologieën en data-analyse. Aan de hand van een analyse van de algemene transactiegegevens kunnen banken een gepersonaliseerd aanbod voor hun cliënten opstellen en hen zo een betere dienstverlening aanbieden. Aan klanten van infrastructuurspelers, bieden deze ondersteuning bij het nakomen van hun complianceverplichtingen. Bovendien laten data-analysetechnieken toe verdachte transactiepatronen tijdig te identificeren, zodat de impact van fraudegevallen zoveel mogelijk wordt beperkt. Via de herziene richtlijn betreffende betalingsdiensten (Payment Services Directive, PSD2[1]) opende de EU de markt voor bedrijven die consumenten en dienstenaanbieders toegang geven tot informatie met betrekking tot bankrekeningen. De Bank stelt een sterke interesse vast voor het nieuwe statuut van betalingsinitiatiedienstverlener. Deze dienstverleners vormen een virtuele brug tussen een betalingsopdrachtgever en zijn onlinebankrekening. Bovendien geven ze aan of er voldoende geldmiddelen beschikbaar zijn op de rekening van de opdrachtgever en dus of de onderliggende transactie kan doorgaan.

Vanuit wettelijk- en toezichtstandpunt is het zowel voor bestaande als voor nieuwe spelers belangrijk dat de juiste balans wordt gevonden tussen het niet onnodig afremmen van innovatie en de beheersing van de risico's. Aandachtspunten hierbij zijn onder meer dat door FinTech het klassieke verdienmodel onder druk staat, wat de stabiliteit van individuele instellingen en, bij uitbreiding, het financiële systeem in gevaar kan brengen. Voor nieuwe spelers is het belangrijk dat ze over de nodige integriteit beschikken en voldoende startkapitaal hebben. Ook dient de stabiliteit en de beveiliging van IT-systemen te worden gewaarborgd, en dient de privacy in acht te worden genomen wanneer gebruik wordt gemaakt van de talrijke gekoppelde databestanden (big data). De Bank heeft eind 2015 een interne werkgroep opgezet die onder meer bekijkt welke impact FinTech heeft op bestaande bedrijfsmodellen en op prudentiële risico's.

Daarnaast werkt de Bank ook samen met de wetgever, in het kader van de HLEG, aan verschillende initiatieven om haar aanpak beter te doen aansluiten bij de gewijzigde financiële omgeving. Zo is de Bank samen met de FSMA gestart met een analyse van de regelgeving om onnodige hinderpalen voor innovatieve bedrijfsmodellen weg te werken. De Bank werkt tevens aan een centraal contactpunt voor FinTech-initiatieven van zowel bestaande als nieuwe spelers. Dit centraal contactpunt zal via een actieve dialoog met de marktpartijen de snel veranderende en soms complexe innovaties op de voet volgen en vragen beantwoorden i.v.m. regelgeving, toezicht en vergunningen. Door de aard van de FinTech-evolutie is het vanzelfsprekend dat het antwoord van de toezichthouders gecoördineerd en vanuit een Europees en zelfs pan-Europees perspectief wordt ontwikkeld. De Bank werkt daarom binnen verschillende internationale instellingen mee aan de opstelling van aangepaste regelgeving

(1) Richtlijn (EU) Nr. 2015/2366 van het Europees Parlement en de Raad van 25 november 2015 betreffende betalingsdiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) nr. 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG.

die op passende wijze rekening houdt met de prudentiële risico's en de stabiliteit van het financieel systeem garandeert zonder de kansen en opportuniteiten te beperken die onlosmakelijk zijn verbonden met FinTech-innovaties. In dit kader neemt de Bank deel aan diverse werkgroepen, waarin onder meer aandacht wordt besteed aan de vergunningsmodaliteiten voor FinTech-spelers, de vereisten met betrekking tot de uitbesteding van activiteiten en de gepastheid van het bestaande prudentiële kader, rekening houdend met de FinTech-innovaties.

4. Cyberrisico

De financiële sector is reeds sterk geïnformatiseerd en de digitalisering van haar bedrijfsprocessen neemt nog verder toe. Ook de mate van interconnectiviteit tussen de operationele processen van de verschillende financiële actoren is zeer hoog. Daarenboven kiezen de financiële instellingen steeds vaker voor bedrijfsmodellen waarbij informaticadiensten door derde partijen worden geleverd, volgens een operationele dan wel functionele specialisatie. Deze sterkere en meer gediversifieerde digitalisering van de toegangskanalen voor particuliere bankklanten is slechts één van de aspecten waarmee rekening gehouden moet worden bij de analyse van het operationele risico bij financiële instellingen en FMI's.

In de voorbije jaren, en ook tijdens het verslagjaar, werd in de financiële sector steeds meer specifieke aandacht besteed aan het cyberrisico. De beoordeling en de bevordering van de beheersing van het cyberrisico bij de individuele instellingen vormt een topprioriteit van het prudentieel toezicht en het oversight op financiële instellingen en FMI's. Op sectoraal niveau wordt een verdere versterking van de maatregelen en inspanningen ter bescherming tegen het cyberrisico aangemoedigd, waarbij de nodige aandacht wordt besteed aan de sectoroverschrijdende cyberbeheersingsstrategieën die zich op nationaal en internationaal niveau aan het ontwikkelen zijn.

4.1 Verdere toename van cyberdreigingen

Cyberaanvallen worden alsmaar geavanceerder en richten steeds meer schade aan. Ook aanvallen waarbij de integriteit van de IT-systemen en -data wordt aangetast nemen toe. Dit is een bron van zorg voor de Bank als prudentiële autoriteit. Haar aandacht gaat hierbij vooral uit naar de beveiliging en het vertrouwen in individuele financiële instellingen of FMI's, en in de sector als geheel. De operationele beveiliging en robuustheid van de diensten die kritiek zijn voor het adequaat functioneren van de sector is in dit verband van cruciaal belang.

De benadering van het cyberrisico is tweeledig. Enerzijds dienen de instellingen eigen vermogen aan te houden voor hun operationele risico's, waaronder cyberrisico's. Anderzijds wordt nauw toegezien op de operationele veiligheid en robuustheid van de kritieke processen bij de financiële instellingen en FMI's. De beschikbaarheid en integriteit van de IT-systemen en -data staan hierbij centraal.

Cyberdreigingen kunnen ontstaan binnen en buiten de instellingen en de aanvallers kunnen diverse motieven hebben, zoals financiële diefstal, terrorisme en geostrategische spionage en sabotage. Hierdoor is het voor de financiële instellingen en infrastructuren zeer moeilijk om hun IT-systemen, -data en -diensten steeds en overal voldoende te beveiligen tegen de diverse aanvallen. Omdat cyberdreigingen zeer snel evolueren, dient de defensieve capaciteit van de instellingen en FMI's meer dan voorheen flexibel te kunnen inspelen op veranderende aanvalspatronen. Oplossingen voor het verzamelen van informatie over potentiële bedreigingen, aanvallers en aanvalstypes zijn hierbij essentieel. Als bescherming tegen cyberaanvallen die de integriteit van de IT-systemen of -data aantasten, dienen de financiële instellingen naast de klassieke continuïteitsvoorzieningen op basis van aparte datacentra ook te beschikken over adequate heropstartmechanismen.

4.2 Richtlijnen voor cyberweerbaarheid

Op 1 januari 2016 trad de prudentiële circulaire[1] in werking betreffende de verwachtingen van de Bank op het vlak van de operationele bedrijfscontinuïteit en beveiliging van systeemrelevante instellingen. Deze circulaire besteedt bijzondere aandacht aan de cyberweerbaarheid (cyber resilience). In juni 2016 publiceerden het CPMI en de IOSCO richtlijnen[2] inzake cyberweerbaarheid, die onmiddellijk van toepassing zijn op FMI's. De Bank zal de naleving controleren van deze richtlijnen door de in België gevestigde FMI's.

Eén van de belangrijke aandachtspunten in deze prudentiële circulaire en in de oversight-richtlijnen is het beheer van het cyberrisico door de financiële actoren. Bij de beheersing van het cyberrisico moet niet alleen worden gefocust op technologie, maar moet ook voldoende aandacht worden besteed aan mogelijke bedreigingen binnen de organisatie vanwege de werknemers of het management. De financiële actoren moeten hun medewerkers bewust maken van het

(1) Circulaire NBB_2015_32 van 18 december 2015 betreffende aanvullende prudentiële verwachtingen op het vlak van de operationele bedrijfscontinuïteit en beveiliging van systeemrelevante instellingen.
(2) Guidance on cyber resilience for financial market infrastructures.

cyberrisico, zodat zij weten hoe dit risico kan optreden en hoe zij dienen te reageren. De bestuursorganen moeten over de nodige expertise en informatie beschikken om de cyberbedreigingen op passende wijze te kunnen opvolgen en binnen aanvaardbare perken te kunnen houden.

Het uitvoeren van tests door de financiële actoren om hun mate van bescherming tegen cyberbedreigingen te beoordelen, is een andere aanbeveling in beide bovenvermelde richtlijnen. Deze tests worden steeds geavanceerder en worden in sommige jurisdicties ondersteund door specifieke raamwerken met een geharmoniseerde testmethodologie. De Bank volgt de ontwikkelingen in dit domein op om de gezonde beheerpraktijken ook in België ingang te laten vinden, rekening houdend met mogelijke Europese of internationale initiatieven op dit vlak.

De Bank volgt ook buiten de financiële sector de relevante ontwikkelingen op. Zo publiceerde de G7 richtlijnen voor een adequaat raamwerk ter beheersing van cyberrisico's, en verschillende landen zetten een nationale cyberstrategie op voor de belangrijkste sectoren, waartoe meestal ook de financiële sector behoort.

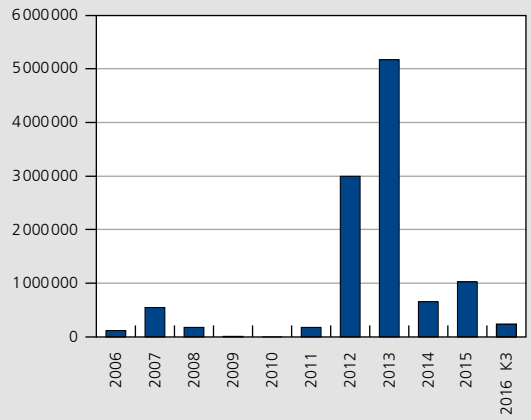
4.3 Capita selecta

SWIFT

De Bank is lead overseer van SWIFT en oefent dit oversight samen met de andere centrale banken van de G10 uit. Dit jaar werd bijzondere aandacht besteed aan de cyberaanval waarbij van de rekening van de centrale bank van Bangladesh $ 81 miljoen werd weggesluisd, en aan andere gevallen, die de pers haalden, waarbij financiële instellingen het slachtoffer werden van frauduleuze SWIFT-berichten. Bij deze aanvallen werden de centrale verwerkingssystemen van SWIFT nooit in het gedrang gebracht, maar werd misbruik gemaakt van veiligheidsleemten bij de financiële instellingen die gebruikmaken van SWIFT. Deze aanvallen tonen het belang aan van een adequate cyberbescherming bij de financiële instellingen die deelnemen aan SWIFT. Om haar klanten hierbij te ondersteunen en te begeleiden, heeft SWIFT een omvangrijk programma opgezet, dat nauwgezet wordt opgevolgd door de G10 overseers van SWIFT.

GRAFIEK 107 JAARLIJKS FINANCIEEL VERLIES ALS GEVOLG VAN E-BANKINGFRAUDE IN BELGIË

(in €)



Bron : Febelfin.

E-banking-fraude en fraude bij mobiel bankieren

Ook in 2016 werd de nauwe samenwerking met onder meer Febelfin en de Federale Computer Crime Unit voortgezet om e-bankingfraude te beperken. Opmerkelijk is dat de jaarlijkse financiële verliezen als gevolg van e-bankingfraude in de voorbije drie jaar op een laag niveau zijn gestagneerd als gevolg van de inspanningen van de financiële instellingen en enkele succesvolle interventies door de Belgische politiediensten en het justitieapparaat.

Net zoals de voorbije jaren waren de opgetekende gevallen van e-bankingfraude bij particulieren ook in 2016 quasi uitsluitend het gevolg van fraudetechnieken waarbij cybercriminelen e-bankinggebruikers misleiden om hun persoonlijke beveiligingscodes te verkrijgen (meestal na telefonisch contact of via een malafide website). Frauduleuze transacties worden door de instellingen geval per geval onderzocht en terugbetaald, tenzij in geval van grove nalatigheid of bedrieglijk opzet.