E. Digitalisering

Disruptieve technologieën en innovatieve bedrijfsmodellen hebben een steeds grotere impact op de financiële dienstverlening. Hoogtechnologische nieuwkomers hebben zich de laatste jaren sterk gefocust op bepaalde segmenten, waaronder betalingen, kredietscoring en geautomatiseerd beleggingsadvies. Met innoverende werkwijzen en platformen spelen deze nieuwkomers direct in op de gewijzigde noden van de eindgebruikers, bijvoorbeeld gebruiksgemak, onmiddellijke verwerking en kostefficiëntie. In dit hoofdstuk worden twee trends verder toegelicht: de innovaties in de betalingssector dankzij de introductie van Open Banking, en de wereldwijde stablecoins. De toenemende digitalisering van de financiële dienstverlening heeft ook als gevolg dat IT- en cyberrisico's nauwgezet opgevolgd moeten worden. De ontwikkelingen op dit vlak worden in de laatste paragraaf behandeld.

1. Open Banking

De tweede Europese richtlijn betreffende betalingsdiensten (PSD2)[1], die werd omgezet in Belgisch recht door de wet van 11 maart 2018, heeft betrekking op innovaties in de betalingssector en verplicht rekeninghoudende betalingsdienstaanbieders (zoals banken) om hun online betaalrekeningeninfrastructuur open te stellen (*Open Banking*). Dit maakt het mogelijk voor betalingsinitiatie- en rekeninginformatiedienstaanbieders (zowel banken, betalingsinstellingen als instellingen voor elektronisch geld) om de markt voor betalingsdiensten te betreden.

Het openstellen van die betaalrekeningeninfrastructuur gaat gepaard met strenge veiligheidsvoorschriften, die moeten kunnen worden nageleefd door alle betrokken betalingsdienstaanbieders (banken, betalingsinstellingen en instellingen voor elektronisch geld). Deze veiligheidsvoorschriften zitten vervat in de Gedelegeerde Verordening (EU) 2018/389 van de Commissie[2], welke in werking trad op 14 september 2019.

De banksector heeft de inwerkingtreding van deze veiligheidsvoorschriften niet afgewacht om deze nieuwe betalingsdiensten zelf te ontplooien op de Belgische markt. Enkele Belgische banken lanceerden reeds de mogelijkheid om zowel betaalrekeningen aangehouden bij andere Belgische banken te consulteren via hun eigen kanalen als om betalingsopdrachten te initiëren vanop die andere betaalrekeningen. Daarnaast verleende de Bank in 2019 aan zeven betalingsinstellingen en twee instellingen voor elektronisch geld een (uitbreiding van de) vergunning als betalingsinitiatie- en/of rekeninginformatiedienstaanbieder.

1 Richtlijn (EU) 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.

2 Gedelegeerde Verordening (EU) 2018/389 van de Commissie van 27 november 2017 tot aanvulling van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad wat betreft technische reguleringsnormen voor sterke cliëntauthenticatie en gemeenschappelijke en veilige open communicatiestandaarden.

De verplichte openstelling van betaalrekeningen door Belgische rekeninghoudende betalingsdienstaanbieders (voornamelijk banken) werd vooral verwezenlijkt middels een speciale interface, die door de betrokken banken werd opgesteld. Op vraag van de betrokken banken en na verificatie of aan de wettelijke vereisten werd voldaan, heeft de Bank een aantal van deze speciale interfaces vrijgesteld van de verplichting om over een terugvalmechanisme te beschikken overeenkomstig de Gedelegeerde Verordening (EU) 2018/389. Verwacht wordt dat nog een groot aantal banken een gelijkaardige vraag tot vrijstelling zullen richten aan de Bank eens hun speciale interface voldoet aan de wettelijke vereisten ter zake. Gelet op de complexiteit en de veelheid van de betalingsproducten die de banken aanbieden, vergt het op punt stellen van de speciale interface meer tijd dan aanvankelijk voorzien.

Betreffende de toepassing van sterke cliëntauthenticatie voor het veilig initiëren en uitvoeren van betalingen (zowel kaartbetalingen als overschrijvingen), publiceerde de EBA in juni 2019 een Opinion, die nader toelicht welke elementen in aanmerking komen voor sterke cliëntauthenticatie[1]. Het bleek echter dat er voor de kaartindustrie nood was aan een overgangsregeling voor het gebruik van betaalkaarten in de online handel (*e-commerce*). In lijn met de betrokken EBA Opinion en in navolging van alle andere EU-toezichthouders publiceerde de Bank daarom een Mededeling op 28 augustus 2019. Daarin erkent de Bank de uitdagingen die het naleven van sterke cliëntauthenticatie stelt voor Belgische uitgevers van betaalkaarten en Belgische *acquirers* van kaarttransacties die geschieden in het kader van online handel, alsook de noodzaak om samen te werken met de relevante belanghebbenden (betalingsdienstaanbieders, kaartschema's, handelaren en consumenten-vertegenwoordigers,...) om tot een akkoord te komen over een redelijk en aanvaardbaar plan om op sectorniveau – zo snel mogelijk na 14 september 2019 – over te gaan tot de implementatie van sterke cliëntauthenticatie voor kaartbetalingen in de onlinehandel. De Bank verwacht dat de sector een migratieplan zal opstellen, dat goedgekeurd moet worden door de Bank in het eerste deel van 2020, en dat het mogelijk maakt uiterlijk op 31 december 2020 te migreren.

Het openstellen van de betaalrekeningen-infrastructuur gaat gepaard met strenge veiligheidsvoorschriften

2. Wereldwijde *stablecoins*

Een van de meest in het oog springende trends van 2019 was de opkomst van global stablecoins die gesteund worden door internationale consortia. Global stablecoin-initiatieven willen een internationale financiële infrastructuur opbouwen die gekenmerkt wordt door een prijsstabiele virtuele munt en een uitgebreid gebruikersnetwerk. De prijsstabiliteit zou gecreëerd worden door het koppelen van de virtuele munt aan waardevaste bezittingen zoals deposito's en kortlopende staatsobligaties. Daarnaast beschikken de partners in de internationale consortia die dergelijke global stablecoins willen lanceren, typisch over een uitgebreid gebruikersnetwerk – bijvoorbeeld Facebook als partner in Libra – die het gebruik van de stablecoin als betaalmiddel moeten ondersteunen. Prijsstabiliteit en netwerkgrootte zijn typische uitdagingen voor eerste generatie cryptomunten zoals Bitcoin.

Daarnaast leggen de wereldwijde stablecoins ook belangrijke uitdagingen voor het huidige financiële stelsel bloot. De verwerking van internationale betalingen is vandaag nog vaak inefficiënt en niet-transparant. Voorts worden bepaalde werelddelen gekenmerkt door een lage financiële inclusie.

De introductie van global stablecoins kan echter ook belangrijke risico's inhouden. De Bank bekijkt samen met andere internationale autoriteiten welke risico's dit zijn, bijvoorbeeld het gebruik van global stablecoins voor witwasdoeleinden, terrorismefinanciering of belastingontduiking, of bedreigingen voor de privacy, mededinging en consumentenbescherming (o.a. terugbetaalbaarheid). Daarnaast zijn er mogelijk belangrijke implicaties voor de financiële stabiliteit als het private consortium of een van zijn partners het vertrouwen van het publiek verliest.

Verder moet ook nagegaan worden of de effectiviteit van belangrijke macro-economische beleidsinstrumenten zoals het monetair beleid van de centrale banken zou kunnen worden aangetast door een succesvolle doorbraak van stablecoins.

1 Sterke cliëntauthenticatie vereist het gebruik van twee of meer van de volgende drie factoren, die onderling onafhankelijk en vertrouwelijk dienen te zijn: iets wat alleen de gebruiker weet (bijvoorbeeld een pincode), iets wat alleen de gebruiker heeft (bijvoorbeeld een betaalkaart) en iets wat de gebruiker is (bijvoorbeeld biometrische gegevens zoals een vingerafdruk).

In welke mate het bestaand regelgevend en prudentieel kader toereikend is, kon niet bepaald worden op het moment waarop dit verslag werd opgesteld. Via internationale samenwerkingsverbanden proberen de autoriteiten gedetailleerde informatie over het technisch, operationeel en organisatorisch ontwerp van de global stablecoins te verkrijgen. Met een internationaal gecoördineerde aanpak proberen de autoriteiten regelgevingsarbitrage te vermijden.

De Bank bekijkt samen met andere internationale autoriteiten welke risico's global stablecoins kunnen inhouden

De Bank is actief betrokken bij de continue verbetering van de door centrale banken uitgebate betalingssystemen en neemt actief deel aan hiermee verband houdende analyses in internationale werkgroepen, bijvoorbeeld het Committee on Payments and Market Infrastructures (CPMI).

3. Cyber- & IT-risico's

3.1 Verdere toename van cyber- en IT-gerelateerde dreigingen

Wereldwijd zijn cyberaanvallen de voorbije jaren geevolueerd tot een dagdagelijkse realiteit. Tezelfdertijd wordt vastgesteld dat bepaalde aanvallers de gebruikte technieken en methodes aanscherpen, waardoor een deel van de vastgestelde aanvallen steeds gesofisticeerder en krachtiger wordt. Verwacht wordt dan ook dat het aantal langdurige en doelgerichte cyberaanvallen in de toekomst verder zal toenemen, waarbij de financiële sector logischerwijs één van de potentiële doelwitten blijft. Doordat de cybercriminelen in sommige gevallen de aanval gedurende lange tijd verborgen kunnen houden, kunnen gevoelige of kritische financiële gegevens ondertussen ongemerkt ontvreemd, opzettelijk verspreid, gewijzigd of vernietigd worden. In deze omstandigheden is het voor de financiële instellingen en infrastructuren uitdagend om hun IT-systemen, -data en -diensten adequaat te beveiligen tegen de diverse aanvallen.

Naast cyberrisico's brengt de sterke afhankelijkheid van IT-oplossingen in de financiële sector ook andere uitdagingen met zich mee. Traditionele instellingen worden onder druk gezet – door innovatieve spelers, toegenomen verwachtingen van cliënten betreffende de aangeboden diensten en beschikbaarheid, of toenemende veiligheidsrisico's (bijvoorbeeld door het gebruik van niet langer ondersteunde 'End-of-Life' software) – om hun soms sterk verouderde IT-architecturen op relatief korte termijn te vernieuwen, maar de complexiteit van hun IT-landschap maakt dat het een grote uitdaging is om dit op een verantwoorde manier te realiseren. Tevens is het risico van een toenemende afhankelijkheid van derde partijen voor informaticadiensten en van andere gestandaardiseerde informatiesysteemcomponenten sterk aanwezig. Met name cloudoplossingen worden steeds meer, en voor steeds belangrijker processen, aangewend. Deze ontwikkeling draagt er ook toe bij dat op sectorbreed niveau een beperkt aantal aanbieders van kritieke diensten een alsmaar toenemend concentratierisico voor de financiële industrie inhouden. Ook het voldoende representatief testen van hersteloplossingen blijft een belangrijk aandachtspunt.

De beoordeling en de bevordering van de beheersing van cyber- en IT-risico's vormen dan ook topprioriteiten voor het prudentieel toezicht en het *oversight* op financiële instellingen en FMI's, waarbij de Europese en internationale samenwerking steeds belangrijker wordt. Op het niveau van de individuele instellingen wordt een verdere versterking van de maatregelen en inspanningen ter bescherming tegen cyber- en IT-risico sterk aangemoedigd. Tevens wordt de nodige aandacht besteed aan de sectorbrede beheersingsstrategieën die zich in België en in het buitenland aan het ontwikkelen zijn. Beide aspecten worden in de volgende paragrafen verder toegelicht.

3.2 Richtsnoeren

De Bank heeft de afgelopen jaren in belangrijke mate bijgedragen aan een regelgevend kader om de beheersing van cyber- en IT-risico's te verbeteren. De prudentiële circulaire betreffende de verwachtingen van de Bank op het vlak van de operationele bedrijfscontinuïteit en beveiliging van systeemrelevante instellingen[1] is nog steeds een belangrijke referentie. Verder draagt de Bank actief bij tot de totstandkoming van een Europees regelgevend kader voor het beheer van cyber- en IT-risico's in de schoot van de EBA. Eerder resulteerde dit bijvoorbeeld in de publicatie van EBA-richtsnoeren voor toezichthouders betreffende de beoordeling van het ICT-risico in het kader van het SREP voor kredietinstellingen en beleggingsondernemingen[2]. In 2019 leidde dit enerzijds tot richtsnoeren met betrekking tot uitbesteding[3], die ondertussen werden geïntegreerd in het beleid van de Bank, en anderzijds tot richtsnoeren met betrekking tot het beheer van ICT- en security-risico's[4]. Ook voor verzekeringsondernemingen draagt de Bank bij tot de totstandkoming van een soortgelijk reglementair kader onder de auspiciën van EIOPA.

Wereldwijd zijn cyberaanvallen de voorbije jaren geëvolueerd tot een dagdagelijkse realiteit

Wat de FMI's betreft, bracht het CPMI in december 2019 experten uit de sector samen om haar strategie ter beperking van het frauderisico bij wholesalebetalingen verder te concretiseren. Dit leidde tot het identificeren en formaliseren van nieuwe maatregelen waarvan de effectiviteit bewezen is. In haar hoedanigheid van medevoorzitter van deze CPMI-werkgroep leverde de Bank een significante bijdrage. Net als de andere centrale banken die lid zijn van de werkgroep, werkt de Bank aan de implementatie van deze strategie.

3.3 Operationele activiteiten

Cyber- en IT-risico's vormen een aandachtspunt voor de Bank in het kader van haar prudentieel toezicht en haar oversight. Haar aandacht gaat hierbij enerzijds uit naar de beveiliging van en het vertrouwen in individuele financiële instellingen of FMI's, en, anderzijds, naar de sector als geheel.

De benadering voor de individuele instellingen is tweeledig. Enerzijds dienen de instellingen onderworpen aan prudentieel toezicht eigen vermogen aan te houden ter dekking van hun operationele risico's, waaronder cyber- en IT-risico's. Anderzijds wordt nauw toegezien op de operationele veiligheid en robuustheid van de kritieke processen bij de financiële instellingen en FMI's. De beschikbaarheid, integriteit en vertrouwelijkheid van de IT-systemen en -data staan hierbij centraal. De Bank voerde in 2019 diverse inspectieopdrachten uit (voor banken, in het kader van het SSM) om na te gaan of het regelgevend kader wordt nageleefd en of de IT-systemen met betrekking tot het cyber- en IT-risico adequaat worden beheerd. Daarnaast volgt zij deze risico's op bij de financiële instellingen en FMI's in het kader van haar permanente en recurrente toezichtswerkzaamheden.

De Bank besteedt ook in toenemende mate aandacht aan sectorbrede initiatieven. In het kader van het SSM worden bijvoorbeeld op regelmatige basis transversale analyses uitgevoerd over cyber- en IT-gerelateerde thema's. Zo werden alle significante banken alsook een aantal minder significante banken in 2019 gevraagd om een IT-vragenlijst in te vullen, die belangrijke informatie levert voor het jaarlijkse SREP, en tevens toelaat transversale analyses uit te voeren. Ook aan een aantal verzekeringsondernemingen werd gevraagd soortgelijke informatie te verschaffen voor een vergelijkbaar doeleinde.

In haar rol als sectorale autoriteit voor de toepassing van de wet betreffende de beveiliging en de bescherming

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 EBA Guidelines on ICT Risk Assessment under the Supervisory Review and Evaluation Process (SREP) (mei 2017).
3 EBA Guidelines on outsourcing arrangements (februari 2019).
4 EBA Guidelines on ICT and security risk management (november 2019).

van de kritieke infrastructuren (voornamelijk systeemkritische banken en FMI's), beoordeelt de Bank tevens de doeltreffendheid van controlesystemen bij deze kritieke financiële infrastructuren. Eveneens in deze context organiseert en coördineert de Bank sectorbrede crisissimulatieoefeningen, om de Belgische financiële sector voor te bereiden op potentiële operationele incidenten met een systemisch karakter. In het kader van de wet ter beveiliging van netwerk- en informatiesystemen fungeert de Bank als sectoraal meldpunt voor incidenten in de financiële sector.

Tot slot heeft de Bank vanaf de tweede jaarhelft van 2018 een raamwerk voor ethische hacking uitgewerkt, namelijk TIBER-BE (*Threat Intelligence Based Ethical Red Teaming Belgium*). Dit programma vormt het Belgische onderdeel van een methodologie die werd ontwikkeld door het Eurosysteem, en beoogt via gesofisticeerde tests de cyberweerbaarheid van individuele FMI's en financiële instellingen te verhogen, alsook tot belangrijke inzichten te komen met betrekking tot de cyberbeveiliging van de Belgische financiële sector in zijn geheel. De Bank stimuleert deze oefeningen in haar rol als bewaker van de financiële stabiliteit; deze testen staan bijgevolg los van haar verantwoordelijkheden als prudentieel toezichthouder en *overseer*. Gedurende het verslagjaar werd TIBER-BE verder geoperationaliseerd.