Dit artikel uit Onderneming en Financiering is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

Regulering van betaaldienstverlening onder PSD II – is tech eating everything?*

J. den Hamer & R. Middelburg

1 Inleiding

Op 13 januari 2018 moet de herziene richtlijn betaaldiensten[1] zijn omgezet in Nederlandse wet- en regelgeving. Deze richtlijn is beter bekend als 'PSD II'. Over PSD II is al veel gezegd en geschreven, en niet alleen in de juridische literatuur. Zo heeft het FD recent bericht dat met het naderen van de implementatiedeadline de 'strijd' tussen banken en FinTechs zijn climax nadert. Dit omdat banken onder PSD II aan derden toegang moeten verlenen tot betaalsystemen, betaalrekeningen en rekeninginformatie. Andere dienstverleners dan banken, zoals *start-ups, FinTechs* en *BigTechs* als Alibaba, Amazon, Apple en Google, zouden dankzij PSD II een grote bedreiging kunnen gaan vormen voor de traditionele banken. Als zij de beschikking krijgen over de data van bankklanten, kunnen zij namelijk diensten leveren aan consumenten die nu alleen de traditionele banken aanbieden.[2]

Ook het – in sommige kringen beruchte – televisieprogramma Radar van AVROTROS heeft een duit in het zakje gedaan en meldde dat als gevolg van PSD II er een machtsstrijd zou plaatsvinden tussen banken en de nieuwe aanbieders. Volgens Radar zouden de banken bang zijn dat ze het contact met de klant verliezen en hun 'kapitaal' kwijtraken. De strijd tussen FinTechs en de banken is volgens Radar voor de Europese Commissie (EC) de aanleiding geweest om op 3 oktober 2017 een inval te doen bij de Nederlandse Vereniging van Banken (NVB) en de Betaalvereniging Nederland.[3] Banken zouden nieuwkomers in de financiële sector tegenwerken.[4]

In het licht van deze berichtgeving bespreken wij in deze bijdrage enkele aspecten van PSD II die deze berichtgeving kleuren: de twee onder PSD II nieuw gereguleerde, innovatieve betaaldiensten (par. 4), de toegang tot betaalsystemen en

* De auteurs hebben dit artikel op persoonlijke titel geschreven.

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) 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG.

2 Zie fd.nl/ondernemen/1222843/strijd-tussen-banken-en-FinTechs-nadert-climax.

3 Zie www.amweb.nl/financiele-planning/nieuws/2017/10/radar-psd2-rabobank-vraagt-nu-al-aan-klanten-toegang-betaalrekeningen-101104380.

4 Zie ook 'Nieuwe betaalrichtlijn Brussel leidt tot flinke ruzie tussen banken en FinTechs', FD 29 mei 2017.

Dit artikel uit Onderneming en Financiering is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

betaalrekeningen die noodzakelijk is voor het kunnen verrichten van deze diensten (par. 5), en de privacyaspecten hiervan (par. 6). Wij ronden af met enkele beschouwingen (par. 7). Omwille van de leesbaarheid besteden wij eerst kort aandacht aan de overgang van PSD naar PSD II (par. 2) en de doelstellingen en hoofdpunten van PSD II, alsmede de stand van zaken van het Nederlandse implementatieproces (par. 3).

2 Van PSD naar PSD II

2.1 PSD (2007)

PSD II vervangt de originele richtlijn betaaldiensten van 2007 (beter bekend als de 'Payment Services Directive' of 'PSD').[5] PSD is in Nederland geïmplementeerd in de Wet op het financieel toezicht (Wft) en het Burgerlijk Wetboek (BW). Met PSD is in 2007 een vergunningplicht geïntroduceerd voor een nieuw type financiele onderneming: de betaaldienstverlener. Een betaaldienstverlener is degene die zijn bedrijf maakt van het verlenen van betaaldiensten. Wat 'betaaldiensten' zijn, staat in bijlage 1 van PSD. Het gaat om een breed scala aan diensten, zoals het beheren van betaalrekeningen, het uitvoeren van betalingstransacties, het verrichten van geldtransfers en de uitgifte van betaalinstrumenten zoals credit- en debitcards.

Er is alleen sprake van een vergunningplicht wanneer degene die de betaaldienst(en) verleent hiervan zijn 'bedrijf' maakt. De Nederlandsche Bank (DNB) heeft aangegeven dat dit het geval is wanneer de 'hoofdactiviteit' van deze persoon bestaat uit het verlenen van betaaldiensten. Hiervan is sprake als de betaaldiensten (1) als 'zelfstandige activiteit' zijn te identificeren en (2) niet enkel dienen om één of meer hoofdactiviteiten te ondersteunen die niet kwalificeren als betaaldiensten.[6] Voor beantwoording van de vraag of er in een concreet geval sprake is van het 'bedrijf' maken van betaaldienstverlener, zijn de specifieke omstandigheden van het geval doorslaggevend. Feitelijke aanknopingspunten dat dit zo is, kunnen worden afgeleid uit de omstandigheid dat het verrichten van de betaaldiensten niet slechts incidenteel plaatsvindt en dat degene die de financiële dienst verleent een beloning ontvangt voor zijn diensten.

Van oudsher was betaaldienstverlening het domein van banken en elektronischgeldinstellingen. Door PSD konden ook andere typen ondernemingen

5 Richtlijn 2007/64/EG van het Europees Parlement en de Raad van 13 november 2007 betreffende betalingsdiensten in de interne markt tot wijziging van de Richtlijnen 97/7/EG, 2002/65/EG, 2005/60/EG en 2006/48/EG, en tot intrekking van Richtlijn 97/5/EG.

6 Zie ook J.Ph. Broekhuizen, 'Extensies van de betaalketen. Regulering van betaaldiensten en PSD II', IR 2017, afl. 3, p. 101.

Onderneming en Financiering 2017 (25) 4
doi: 10.5553/OenF/157012472017025004002

Dit artikel uit Onderneming en Financiering is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

betaaldiensten gaan verlenen. Relatief nieuwe spelers als Adyen, Buckaroo en Mollie hebben hiervan gebruik gemaakt.[7]

2.2 PSD II

Uit een evaluatie van de effecten van PSD door de EC is gebleken dat PSD niet langer de tand des tijds doorstaat. Dit is niet zo gek. PSD stamt uit een tijd dat er gebruik werd gemaakt van de chipknip en de acceptgiro het belangrijkste online betaalmiddel was.[8] De ontwikkelingen gaan echter razendsnel. Denk aan het enorme belang van internet, de opkomst van 4G en de mogelijkheid tot het doen van mobiele betalingen via smartphoneapps. Dit was destijds simpelweg niet voorzien. Zodoende valt een aantal innovatieve betaalproducten en diensten buiten het toepassingsbereik van PSD, waardoor adequaat toezicht hierop niet mogelijk is. De EC heeft dan ook gemeend dat het de interne markt en het vertrouwen van betaaldienstgebruikers ten goede komt om deze producten en diensten onder het bereik van PSD II te brengen. Daarnaast kwam naar voren dat het toepassingsgebied van PSD en de uitzonderingen hierop te vaag of te algemeen waren geformuleerd, of gelet op de ontwikkeling van de betalingsmarkt waren achterhaald. Ook is gebleken dat deze markt voor een deel nog wordt bepaald door nationale grenzen. Volgens de EC leidt dit allemaal tot rechtsonzekerheid, potentiële veiligheidsrisico's in de betalingsketen en een gebrek aan consumentenbescherming. Dit heeft nadelige effecten voor de concurrentie, waardoor betaaldienstgebruikers onvoldoende kunnen profiteren van de voordelen van de interne markt.

3 Wat brengt PSD II?

3.1 Doelstellingen

Tegen de hiervoor geschetste achtergrond heeft PSD II drie doelstellingen. Ten eerste het versterken van een interne markt voor kaartbetalingen, internetbetalingen en mobiele betalingen, ten tweede het stimuleren en faciliteren van innovaties door het reguleren van belangrijke betaaldiensten die zijn ontstaan na PSD, en ten derde het repareren van problemen van PSD. Om het vertrouwen van consumenten in een geharmoniseerde betalingsmarkt te versterken, worden bepaalde begrippen in PSD II verduidelijkt, vergunningvoorschriften aangescherpt en uitzonderingen op de vergunningen ingeperkt. Al met al is gezocht naar een balans tussen het stimuleren van innovatie enerzijds en veiligheid en consumentenbescherming anderzijds.

7 Zie het register op www.dnb.nl/toezichtprofessioneel/de-consument-en-toezicht/registers/WFTBI/?&page=2&filter-_value=2:3b%20Vergunning%20voor%20het%20uitoefenen%20van%20het%20bedrijf%20van%20betaaldienstverlener&filter_type=wetsartikel#overzicht voor de overige 35 vergunninghoudende betaaldienstverleners.

8 Vgl. het rapport 'De Nederlandse thuiswinkelbranche anno 2007', www.thuiswinkel.org/data/uploads/marktonderzoeken/Thuiswinkel_Markt_Monitor/Essential_Facts_Thuiswinkel_Markt_Monitor_2007-2.pdf.

Dit artikel uit Onderneming en Financiering is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

3.2 In het oog springende onderdelen PSD II

In het oog springend is de introductie van twee nieuwe betaaldiensten: betaalinitiatiediensten en rekeninginformatiediensten. Onder PSD II krijgen aanbieders van deze nieuwe betaaldiensten met toestemming van rekeninghouders – de betaaldienstgebruikers – toegang tot (betaal)rekeningdata van banken om betalingen te kunnen initiëren, of voor de betaaldienstgebruikers rekeninginformatie inzichtelijk te maken. Het is de regulering van déze diensten die heeft geleid tot de berichtgeving die wij hierboven hebben beschreven. Immers, om aanbieders van deze nieuwe betaaldiensten in staat te stellen deze diensten ook daadwerkelijk en zonder obstakels te kunnen verlenen, verplicht PSD II banken betaaldata en rekeninginformatie van klanten te delen (als de betaaldienstgebruikers daarvoor toestemming hebben gegeven) met deze aanbieders.

Maar zoals hierna zal blijken brengt PSD II méér. PSD II introduceert als één van de maatregelen om de veiligheid van het betalingsverkeer te vergroten 'sterke clientauthenticatie'. Daarnaast bevat PSD II diverse verplichtingen voor de bescherming van persoonsgegevens. Zo moet een aspirant betaaldienstverlener bij een vergunningaanvraag bijvoorbeeld een beschrijving geven van zijn beveiligingsbeleid, met inbegrip van een gedetailleerde risicoanalyse met betrekking tot de betalingsdiensten en een beschrijving van de maatregelen op het gebied van beveiliging en risicobeperking die worden genomen om de gebruikers van de betalingsdiensten afdoende tegen de vastgestelde beveiligingsrisico's, waaronder fraude en illegaal gebruik van gevoelige gegevens en persoonsgegevens, te beschermen. Belangrijk is dat op grond van PSD II de verwerking van persoonsgegevens door betaaldienstverleners uitsluitend is toegestaan met de uitdrukkelijke toestemming van de betaaldienstgebruiker. Ook over deze aspecten van PSD II is in de media het nodige te doen geweest.[9]

3.3 Andere noviteiten

Door de beperktere – en scherpere – definiëring van de uitzonderingen op het toepassingsbereik wordt de reikwijdte van PSD II ten opzichte van PSD vergroot.[10] Hierdoor zullen meer betaaldienstverleners onder de vergunningplicht als betaalinstelling[11] vallen. Dit betekent dat betaaldienstverleners eerder een vergunning nodig hebben indien zij betaaldiensten verrichten in de uitoefening van beroep of bedrijf. De wetgever heeft in dit verband gesignaleerd dat in de implementatiewerkgroepen in Brussel is aangegeven dat het niet relevant is of dit wel of geen hoofdactiviteit van de onderneming is. Het is onduidelijk wat dit betekent voor de hiervoor in par. 2.1 uiteengezette interpretatie van DNB op dit punt.

9 Bijv. ellentimmer.wordpress.com/2016/12/08/psd2/; community.consumentenbond.nl/geldverzekeringen-6/psd2-wet-privacy-wangedrocht-2441.

10 Artikel 3 PSD II.

11 Een betaalinstelling is op grond van art. 1:1 Wft een betaaldienstverlener waaraan een vergunning ex art. 2:3a Wft is verleend.

doi: 10.5553/OenF/157012472017025004002

Dit artikel uit Onderneming en Financiering is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

Een uitzondering die is aangepast, is die voor betaaldiensten die worden verricht binnen een 'beperkt netwerk'.[12] Hierbij gaat het om betaalproducten die iemand kan gebruiken voor de afname van specifieke goederen en diensten, zoals klantenkaarten, tankkaarten, lidmaatschapskaarten, kaarten voor openbaar vervoer en maaltijdcheques. Onder PSD mochten deze producten niet worden gebruikt voor betalingstransacties ten behoeve van de aankoop van goederen en diensten binnen meer dan één beperkt netwerk. Onder PSD II mogen deze betaalinstrumenten ook niet meer worden gebruikt voor de aankoop van een onbeperkte reeks goederen en diensten. Onder PSD II zullen alleen kleine, beperkte netwerken buiten de reikwijdte van de vergunningplicht vallen.

Een andere uitzondering die is aangepast, is die voor handelsagenten. Een handelsagent treedt op als een bemiddelaar tussen de aanbieder van een goed of dienst en de afnemer daarvan. Een handelsagent treedt op 'voor rekening' van de opdrachtgever. Voorwaarde om te kunnen worden aangemerkt als handelsagent is dat er een duurzame (commerciële) samenwerking is tussen de bemiddelaar en zijn opdrachtgever. Deze uitzondering geldt onder PSD II alleen nog maar wanneer handelsagenten voor rekening van ofwel de betaler, ofwel de begunstigde handelen, ongeacht of zij daadwerkelijk in het bezit zijn van de geldmiddelen van de cliënten. Wanneer agenten voor rekening van zowel de betaler als de begunstigde handelen (zoals op platformen voor elektronische handel als bol.com), worden zij slechts van het toepassingsbereik van PSD II uitgesloten indien zij op geen enkel moment over de geldmiddelen van de cliënten kunnen beschikken of de controle daarover hebben.

Verder is van belang dat de uitzondering voor technische dienstverleners (waaronder ook aanbieders van IT en communicatienetwerken) blijft bestaan. Zij mogen alleen geen betaalinitiatiediensten of rekeninginformatiediensten aanbieden.[13]

In het kader van het waarborgen van veilig betalingsverkeer stelt PSD II meer voorwaarden aan de vergunningverlening dan PSD. Betaaldienstverleners moeten onder andere kunnen aantonen hoe wordt omgegaan met veiligheidsincidenten en consumentklachten, het opslaan, monitoren, traceren en beperken van toegang tot gevoelige betaalgegevens, de bedrijfscontinuïteit, de wijze waarop statistieken worden bijgehouden van transacties en fraude, het veiligheidsbeleid inclusief risicoanalyse en hoe (*on-site/off-site*) controle wordt gehouden op agenten en bijkantoren. Ten aanzien van operationele risico's, beveiligingsrisico's en authenticatie stelt de European Banking Association (EBA) richtsnoeren en technische standaarden (Regulatory Technical Standards (RTS)) op.

PSD II bevat voorts regels over onjuiste overboekingen, betalingstransacties waarbij het transactiebedrag niet vooraf bekend is (bijvoorbeeld bij betalen aan de benzinepomp) en het in rekening brengen van vergoedingen voor het gebruik van

12 Vgl. art. I onder B Implementatiewet.

13 Art. 3 onder j PSD II, ex de Implementatiewet geïmplementeerd in art. 1:5a lid 2 onder j Wft.

Dit artikel uit Onderneming en Financiering is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

een betaalinstrument. Op grond van PSD II hoeven deze vergoedingen alleen te worden betaald wanneer de betaaldienstgebruiker hierover voorafgaand aan de betaling is geïnformeerd.

3.4 Implementatietraject

Zoals aangegeven moet op 13 januari 2018 PSD II in Nederland zijn geïmplementeerd. PSD II zal in Nederland worden geïmplementeerd in de Wft en in het BW door middel van de Implementatiewet herziene richtlijn betaaldiensten. Op 17 november 2016 is het wetsvoorstel voor de wet met de daarbij behorende memorie van toelichting gedurende vier weken ter consultatie aangeboden (hierna: de Implementatiewet).[14] Het streven was om het wetsvoorstel voor de Implementatiewet eind november naar de Tweede Kamer te sturen. Uit een Kamerbrief van (oud-)minister van Financiën Dijsselbloem van 22 oktober 2017 blijkt dat dat niet gaat lukken, en dat het streven nu is om de Implementatiewet in het voorjaar van 2018 in werking te laten treden.[15]

Duidelijk is dus dat Nederland de implementatietermijn niet zal halen. Voor marktpartijen betekent dit dat de aanbieders van betaalinitiatiediensten en rekeninginformatiediensten deze diensten vooralsnog ongereguleerd kunnen blijven verrichten. Complicatie hierbij is wel dat de Nederlandse banken nog niet wettelijk *verplicht* zijn om deze aanbieders toegang te verlenen tot de betaal- en rekeninginformatie. Zij kunnen dit uiteraard wel onverplicht doen, maar dan alleen als een betaaldienstgebruiker hiervoor uitdrukkelijk toestemming heeft gegeven. Een andere complicatie doet zich voor wanneer een andere lidstaat de implementatietermijn wel gehaald heeft, en een (aldaar vergunninghoudende) aanbieder uit die lidstaat na de uiterste omzettingsdatum op basis van het zogeheten Europees paspoort grensoverschrijdend in Nederland betaalinitiatiediensten en rekeninginformatiediensten wil aanbieden. Is er dan nog ruimte voor de bank om voor die (vergunninghoudende) aanbieder de toegang tot (betaal)rekeningdata te weigeren?

Voor Nederland betekent het niet halen van de implementatietermijn - zoals de minister van Financiën ook onderkent - dat de EC theoretisch Nederland daarvoor in gebreke zou kunnen stellen en een inbreukprocedure zou kunnen starten tegen Nederland. Dit zou er op termijn dan toe kunnen leiden dat Nederland door het Hof van Justitie in Luxemburg een boete opgelegd krijgt wegens niet-tijdige implementatie.[16]

14 Wijziging van de Wet op het financieel toezicht en het Burgerlijk Wetboek ter implementatie van Richtlijn 2015/2366/EU van het Europees Parlement en de Raad van 25 november 2015 betreffende betaaldiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG (PbEU 2015, L 337) (Implementatiewet herziene richtlijn betaaldiensten). Zie www.internetconsultatie.nl/implementatiewetherzienerichtlijnbetaaldiensten/details.

15 Kamerbrief van 22 september 2017 betreffende Voortgang implementatie herziene betaaldienstenrichtlijn (PSD II), kenmerk 2017-0000188569.

16 Kamerbrief van 23 september 2017 betreffende Reactie verzoek voortgang implementatie herziene betaaldienstenrichtlijn (PSD II), kenmerk 2017-0000195075.

doi: 10.5553/OenF/157012472017025004002

Dit artikel uit Onderneming en Financiering is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

Op 26 september 2017 is het Implementatiebesluit herziene richtlijn betaaldiensten (hierna: het Implementatiebesluit)[17] ter consultatie aangeboden. Dit besluit zal een aantal algemene maatregelen van bestuur (AMvB's) wijzigen die als gevolg van PSD II dienen te worden aangepast. Kort gezegd worden de uit PSD II voortvloeiende vergunningseisen geïmplementeerd in het Besluit markttoegang financiële ondernemingen (Bmfo), de eisen aan de interne bedrijfsvoering in het Besluit prudentiële regels (Bpr) en de informatieverplichtingen in het Besluit gedragstoezicht financiële ondernemingen (Bgfo).

4 Innovatieve betaaldiensten

4.1 Betaalinitiatiediensten

De eerste nieuwe, innovatieve betaaldienst die PSD II zal reguleren, is de 'betaalinitiatiedienst'. Dit is een dienst voor het initiëren van betaalopdrachten door een betaaldienstverlener op verzoek van een betaaldienstgebruiker. De betaaldienstgebruiker is kort gezegd de betaler of begunstigde. Het dient hierbij te gaan om het initiëren van betaalopdrachten voor een *online* raadpleegbare betaalrekening,[18] die de betaaldienstgebruiker bij een rekeninghoudende betaaldienstverlener aanhoudt. Deze rekeninghoudende betaaldienstverlener zal vaak een bank zijn in de zin van art. 1:1 Wft, maar kan ook een betaalinstelling zijn die betaalrekeningen aanbiedt.[19] Kortheidshalve en voor de leesbaarheid zullen we de rekeninghoudende betaaldienstverlener hierna aanduiden als: bank.

17 Besluit tot wijziging van het Besluit Prudentiële regels Wft, het Besluit Markttoegang financiële ondernemingen Wft en het Besluit Gedragstoezicht financiële ondernemingen Wft ter implementatie van Richtlijn 2015/2366/EU van het Europees Parlement en de Raad van 25 november 2015 betreffende betaaldiensten in de interne markt, houdende wijziging van de Richtlijnen 2002/65/EG, 2009/110/EG en 2013/36/EU en Verordening (EU) 1093/2010 en houdende intrekking van Richtlijn 2007/64/EG (PbEU 2015, L 337) (Implementatiebesluit herziene richtlijn betaaldiensten).

18 Volgens de definitie van 'betaalrekening' in art. 4 lid 14 PSD is dit een rekening, aangehouden op naam van één of meer betaaldienstgebruikers, die voor de uitvoering van betalingstransacties wordt gebruikt. In beginsel brengt deze definitie met zich dat een bankrekening die bijvoorbeeld dient als (vrij opneembare) spaarrekening, maar waarvan betalingstransacties zoals girale overboekingen (kunnen) worden uitgevoerd, ook als betaalrekening kwalificeert. Bij veel (online) spaarrekeningen kan echter alleen van en naar een vaste tegenrekening (die ook op naam van de rekeninghouder staat) worden overgeboekt. Ten tijde van PSD is daarom de vraag opgekomen of deze spaarrekeningen ook onder de definitie van betaalrekening vallen. De EC heeft in een Q&A destijds aangegeven dat vrij opneembare spaarrekeningen inderdaad onder de definitie van betaalrekening vallen (en depositospaarrekeningen niet). Bij de implementatie van PSD heeft de Nederlandse wetgever in de MvT opgemerkt dat rekeningen die niet worden aangehouden met als hoofddoel betalingen te kunnen verrichten, maar waarvan wel betalingen worden verricht '*niet direct [kunnen] worden aangemerkt als betaalrekening*', een visie die destijds door de EC is goedgekeurd. PSD II hanteert exact dezelfde definitie van betaalrekening als PSD. Vgl. Kamerstukken II 2008/09, 31892, 3, p. 16; Q&A EC on PSD Payment Services Directive 2007/64/EC, Question 25, htttp://ec.europa.eu/internal_market/payments/docs/framework/transposition/faq_en.pdf.

19 Vgl. Bijlage 1 PSD II, nrs. 1 en 2.

Dit artikel uit Onderneming en Financiering is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

De betaaldienstverlener initieert een betalingsopdracht voor de betaaldienstgebruiker, bijvoorbeeld een consument die online aankopen doet.[20] Wanneer de betaaldienstverlener een betaling heeft geïnitieerd op verzoek van de betaaldienstgebruiker, dient de bank onmiddellijk informatie over de initiëring van de betalingstransactie aan de betaaldienstverlener te verstrekken. De betaaldienstverlener kan vervolgens aan de online verkoper (*merchant*) doorgeven dat de betaling succesvol is geïnitieerd. Betalingsinitiatiediensten kunnen overigens ook betrekking hebben op overboekingen, ongeacht of er onderliggende verplichtingen zijn tussen betaler en begunstigde.[21]

Een voorbeeld van een betaalinitiatiedienst die nog niet vergunningplichtig is, maar dit wel zal worden onder PSD II, is het recent geïntroduceerde betalen via iDEAL op www.marktplaats.nl. Verkopers kunnen hierbij betaalverzoeken via iDEAL initiëren en daarmee de financiële afhandeling van een verkoop via de website in eigen hand nemen. Deze dienst wordt aangeboden door een derde partij. Met behulp van deze partij kan een verkoper een betaalverzoek aanmaken. De koper ontvangt vervolgens dit verzoek en wordt met het ingaan op het verzoek direct naar zijn eigen online bankomgeving geleid. De betaling via zijn betaalrekening wordt in die omgeving direct afgehandeld. De derde partij controleert hierbij de identiteit van de verkoper en slaat diens gegevens en IBAN-nummer op.

4.2 Rekeninginformatiediensten

De tweede nieuwe, innovatieve betaaldienst die PSD II zal reguleren, is de 'rekeninginformatiedienst'. Dit is een online dienst voor het verstrekken van geconsolideerde informatie over één of meer betaalrekeningen die de betaaldienstgebruiker bij één of meer banken aanhoudt. Door het online geconsolideerd verstrekken van informatie kan een betaaldienstgebruiker een overzicht van zijn financiële situatie krijgen. De aanbieders van rekeninginformatiediensten kunnen uitgaven categoriseren, waardoor de betaaldienstgebruiker beter inzicht in zijn uitgavenpatroon kan krijgen.

Een rekeninginformatiedienst kan leiden tot een soort elektronisch huishoudboekje. Voorbeelden hiervan zijn de smartphoneapps GRIP van ABN AMRO en (in Engeland) Yolt van ING. Met deze apps bieden de banken (als betaaldienstverleners) een geconsolideerd overzicht van de financiële situatie van de betaaldienstgebruiker op één of meer van zijn betaalrekeningen. De betaaldienstgebruiker kan met de app uitgaven categoriseren en op andere manieren inzichtelijk maken, maar bijvoorbeeld ook budgetten instellen om een melding te krijgen wanneer een budget voor een bepaalde categorie uitgaven is bereikt.

20 MvT Implementatiewet, p. 4.
21 Open Boek Toezicht DNB, Q&A 22 september 2017, 02146.01.

Onderneming en Financiering 2017 (25) 4
doi: 10.5553/OenF/157012472017025004002

Dit artikel uit Onderneming en Financiering is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

5 Toegang tot betaalsystemen en betaalrekeningen

5.1 Toegang bezien vanuit third party providers

Aanbieders van betaalinitiatie- en rekeninginformatiediensten (voor zover zij geen betaalrekeningen aanbieden) worden ook wel '*third party providers*' (TPP's) genoemd.[22] TPP's bieden aan gebruikers toegang tot de technische infrastructuren (of diensten in verband daarmee) van banken. Dit is de kern van hun dienstverlening. Het is voor TPP's dus noodzakelijk dat de banken deze toegang daadwerkelijk verschaffen. Op grond van PSD II is de bank gehouden hieraan medewerking te verlenen, zodat het recht van de betaler om gebruik te kunnen maken van een betaalinitiatiedienstverlener of rekeninginformatiedienstverlener is gewaarborgd. Aan deze verplichting zijn wel bepaalde voorwaarden verbonden. Zo heeft de toegang alleen betrekking op betaalrekeningen die online raadpleegbaar zijn. Verder dient het verzoek om informatie door de TPP's aan de rekeninghoudende betaaldienstverlener overeen te komen met de informatie die door de betaaldienstgebruiker expliciet is gevraagd. De reikwijdte van de toegang en van de informatie die mag worden verkregen, wordt dus steeds bepaald door, en is steeds afhankelijk van, (de inhoud van) de toestemming. Als de betaaldienstgebruiker bepaalde informatie niet opvraagt, kan de TPP geen toegang krijgen tot deze informatie. Als de betaaldienstgebruiker echter expliciet toestemming heeft verleend, legt PSD II geen (verdere) beperkingen op aan de hoeveelheid informatie die door een TPP mag worden verkregen. Zoals wij hierna nader uiteenzetten, kunnen deze beperkingen wel bestaan op grond van de algemeen geldende Europese privacyregels. Op grond van PSD II mag een bank de toegang tot de betaalrekening verder alleen weigeren wanneer er een objectief vermoeden is van een niet-toegestane betalingstransactie of fraude.[23]

Zoals uit het voorbeeld van ABN AMRO en ING (Grip en Yolt) blijkt, kunnen banken zelf ook betaalinitiatie- en rekeninginformatiediensten aanbieden. Onder PSD II zal dat niet veranderen. Hierbij geldt dat een bank uiteraard al toegang heeft tot zijn eigen betaalrekeningen, maar door PSD II ook toegang kan krijgen tot betaalrekeningen aangehouden bij andere banken. Dit kan uiteraard commercieel interessant zijn. Dan kunnen banken dus (ook) gebruik maken van betaalrekeningdata van hun (Europese) concurrenten en de betaalrekeningen van de betaaldienstgebruikers bij die concurrenten meenemen in hun betaalinitiatie- en rekeninginformatiediensten.

22 Om actief te mogen zijn als betaalinstelling, dienen TPP's te voldoen aan een aantal voorwaarden. Zo mogen zij geen tegoeden van betaaldienstgebruikers onder zich houden, hetgeen bepaalde prudentiële voordelen heeft. Ook moeten zij beschikken over een beroepsaansprakelijkheidsverzekering of een andere vergelijkbare waarborg tegen aansprakelijkheid. Daarnaast worden er voorwaarden gesteld aan de bedrijfsvoering, in het bijzonder met betrekking tot gegevensverwerking, veiligheid en consumentenbescherming. Vgl. art. I onder D en H en art. II onder D Wijzigingsbesluit.

23 Art. II onder I Implementatiewet, geïmplementeerd in art. 7:523 lid 5 BW.

Dit artikel uit Onderneming en Financiering is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

5.2 Van screen scraping naar API's

Op dit moment is het mogelijk dat TPP's, die momenteel dus nog niet over een vergunning als betaalinstelling hoeven te beschikken, via de online bankomgeving van een betaaldienstgebruiker toegang verkrijgen tot de betaalrekening van de betaaldienstgebruiker, zonder dat dit voor de bank zichtbaar is. De TPP doet zich bijvoorbeeld (digitaal) voor als de betaaldienstgebruiker en vult namens de betaaldienstgebruiker diens gegevens in bij de bank om een betaling te initiëren. Deze manier van toegang krijgen heet '*screen scraping*'.

De EBA heeft met de RTS de wijze waarop TPP's toegang wordt verleend tot betaalrekeningen van betaaldienstgebruikers verder ingevuld. Om er zorg voor te dragen dat betalingstransacties op een veilige manier kunnen verlopen, is *screen scraping* hierbij vooralsnog in de ban gedaan. De gedachte daarbij is dat banken TPP's toegang verlenen tot de betaalrekening via platforms waarop TPP's de door betaaldienstgebruikers gevraagde diensten kunnen verlenen, met alleen die informatie die voor een specifieke transactie of reeks transacties nodig is. Zo'n platform heeft vaak de vorm van een '*application programming interface*' (API). Een API definieert de toegang tot de functionaliteit die er achter schuil gaat (bijvoorbeeld een banksysteem voor het verrichten van betalingen) en definieert afspraken bij deze toegang. Software (waaronder begrepen een smartphoneapp) kan met de API communiceren. Wanneer aan de ene kant software toegang tot een platform en een set afspraken aanbiedt, kan aan de andere kant andere software deze toegang en afspraken gebruiken om informatie en instructies uit te wisselen met het platform. Op deze manier kent de TPP geen details van de achterliggende functionaliteit, maar kan het dankzij de API deze functionaliteit wel gebruiken.

Veel websites en smartphoneapps maken gebruik van API's. Deze zijn er meestal op gericht om informatie of functionaliteit beschikbaar te stellen aan derden, of andere applicaties de mogelijkheid te geven informatie toe te voegen. Denk bijvoorbeeld aan het plaatsen van een Google Maps-kaart op een website als airbnb.com of in een app als Uber, of het plaatsen van rekentools voor bijvoorbeeld maandlasten of belastingteruggave op websites.

Na de presentatie van de RTS begonnen FinTechs een lobby om *screen scraping* als alternatief naast API's te handhaven. Fintechs stellen dat banken bij het gebruik van API's zelf kunnen bepalen welke data zij beschikbaar stellen aan derde partijen. Zij stellen te vrezen dat de banken mogelijk minder data zullen delen dan betaaldienstgebruikers zouden willen, of data via de API's slechts met vertraging ter beschikking zullen stellen. Daarop heeft de EC bij de EBA het voorstel gedaan om de ban op *screen scraping* op te heffen. Dit voorstel heeft de EBA echter niet overgenomen. De banken stellen op hun beurt dat zij zich zorgen maken om de privacy en veiligheid. Zij stellen dat bij *screen scraping* klantgegevens makkelijk kunnen worden misbruikt. Ook wijzen de banken erop dat ze wel degelijk aan

Dit artikel uit Onderneming en Financiering is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

PSD II willen voldoen, maar dat ze eerst volledige zekerheid willen hebben over de veiligheid van de (klant)gegevens voordat ze toegang geven tot hun systemen.[24]

5.3 Toegang bezien uit gebruikersperspectief: sterke(re) cliëntauthenticatie

Een middel om die veiligheid van het betalingsverkeer te waarborgen is het verifieren – of 'authenticeren' – van de identiteit van de betaaldienstgebruiker. Voor de bescherming van de vertrouwelijkheid en integriteit van persoonlijke beveiligingsgegevens dient de betaaldienstverlener gebruik te maken van authenticatieprocedures. Als gevolg van de implementatie van PSD is het begrip 'authenticeren' al in het BW verankerd. Het gaat hierbij echter alleen om het verifiëren van het gebruik van een *betaalinstrument*, niet om het verifiëren van de identiteit van de *betaaldienstgebruiker*. Onder PSD II heeft het begrip 'sterke cliëntauthenticatie' een bredere strekking. Op grond van PSD II dient een betaaldienstverlener te voorzien in sterke cliëntauthenticatie wanneer (1) een betaler online toegang wil krijgen tot zijn betaalrekening, (2) een betaler een elektronische betalingstransactie initieert, zoals pinnen, (3) een betaler een communicatiemiddel op afstand gebruikt dat een risico op fraude of ander misbruik met zich brengt, zoals een gsm of tablet, (4) een betaling via een betaalinitiatiedienstverlener wordt geïnitieerd of (5) informatie via een rekeninginformatiedienstverlener wordt opgevraagd.[25] Hierbij geldt dat als de betaaldienstgebruiker gebruikt maakt van een TPP deze laatste zich mag baseren op authenticatieprocedures die een bank toepast.[26]

PSD II koppelt sterke cliëntauthenticatie aan de factoren *kennis* (iets wat alleen de gebruiker weet), *bezit* (iets wat alleen de gebruiker heeft) en *inherente eigenschap* (iets wat de gebruiker is). Sterke cliëntauthenticatie is een authenticatieprocedure waarbij een hoog beveiligingsniveau wordt gegarandeerd omdat er ten minste twee verschillende van de hiervoor genoemde elementen worden gecombineerd. Een voorbeeld van sterke cliëntauthenticatie, die overigens in Nederland al enige tijd in zwang is, is het invoeren van de pincode (kennis) voor de betaalpas in een apparaat voor internetbankieren (bezit) en het voor elke betalingstransactie genereren van een unieke code, zoals met de e.dentifier bij ABN AMRO. Een meer eigentijds voorbeeld is het betalen via een smartphoneapp door middel van een pincode (wederom kennis) of een vingerscan (wederom bezit), zoals bij Knab.

Op grond van de RTS wordt bij sterke cliëntauthenticatie een unieke authenticatiecode gegenereerd, die de betaaldienstverlener vervolgens eenmalig accepteert. Daarna kan de betaaldienstgebruiker met behulp van de unieke code toegang krijgen tot zijn online betaalrekening om bijvoorbeeld een elektronische betaling te

24 Zie fd.nl/ondernemen/1203489/europese-betaalrichtlijn-leidt-tot-ruzie-tussen-banken-en-FinTechs.

25 Uitzonderingen op de verplichting om te voorzien in sterke cliëntauthenticatie worden nader uitgewerkt in de RTS. De RTS zijn bindend voor alle betaaldienstverleners. Wel kan een betaaldienstverlener, indien aan de criteria voor uitzondering wordt voldaan, besluiten om niet van deze uitzondering gebruik te maken als hij meent dat het risico (te) hoog is.

26 Vgl. art. 97 PSD II en artikel I, onder D Wijzigingsbesluit, dat voorziet in een nieuw artikel 26h Bpr.

Dit artikel uit Onderneming en Financiering is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

initiëren. Betaaldienstverleners die online diensten verlenen, moeten aan aanvullende eisen voldoen. De gegenereerde authenticatiecode is in dat geval alleen gekoppeld aan het specifieke bedrag dat bij een betalingstransactie overeen is gekomen via het zogenaamde '*dynamic linking*'.[27] Hiermee wordt voorkomen dat fraudeurs met een onderschepte unieke code een betalingstransactie naar een andere betaalrekening kunnen initiëren.

Bij het gebruik van de hiervoor besproken API's brengt sterke cliëntauthenticatie met zich dat API's (1) TPP's in staat moeten stellen de beheerder van de API (i.e. de bank) de instructie te geven de authenticatie te starten, (2) ervoor zorgen dat de communicatiesessies tussen de TPP's, de beheerder en de betaaldienstgebruiker (rekeninghouder) tot stand komt én blijft via de authenticatie, en (3) er tevens voor zorgen dat de integriteit en vertrouwelijkheid van de persoonlijkheidskenmerken en authenticatiecodes die TPP's doorgegeven, zijn gewaarborgd. Een TPP zal dus betaalopdrachten klaar kunnen zetten in een API, maar het is de betaaldienstgebruiker zelf die uiteindelijk via sterke cliëntauthenticatie de betaalopdracht autoriseert en toestemming geeft voor de toegang. Daarbij geldt, zoals eerder aangegeven, dat de toegang tot de betaalrekeningen voor TPP's, zonder objectief vermoeden van een niet-toegestane betalingstransactie of fraude, door een bank niet mag worden beperkt.

6 Privacyaspecten PSD II

6.1 Toegang bezien vanuit het privacyperspectief

PSD II zal het mogelijk maken dat naast de bank van een betaaldienstgebruiker ook andere betaaldienstverleners toegang krijgen tot (gegevens met betrekking tot) de betaalrekening van de betaaldienstgebruiker. Het verkrijgen van toegang tot de betaalrekening van de betaaldienstgebruiker is voor zowel de betaalinitiatie- als de rekeninginformatiedienstverleners immers noodzakelijk om hun diensten te kunnen verrichten.

Om privacyschendingen te voorkomen zullen betaaldienstverleners op grond van PSD II alleen toegang mogen krijgen tot de financiële gegevens van de betaaldienstgebruiker indien zij een vergunning als betaalinstelling hebben verkregen. Daarnaast bepaalt art. 94 lid 1 PSD II dat de privacyrichtlijn[28] en de implementatiewetgeving daarvan (in Nederland is dit de Wet bescherming persoonsgegevens (Wbp)) van toepassing zijn op de verwerking van persoonsgegevens. De privacyrichtlijn zal op 25 mei 2018 worden vervangen door de Algemene verordening gegevensbescherming (AVG).[29] Hierdoor zal de Wbp worden ingetrokken. De

27 Artikel 5 RTS.

28 Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens.

29 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 mei 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG.

doi: 10.5553/OenF/157012472017025004002

Dit artikel uit Onderneming en Financiering is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

AVG brengt aanzienlijke en substantiële veranderingen mee voor het verwerken van persoonsgegevens en introduceert meerdere nieuwe concepten. Het gaat het bestek van deze bijdrage echter te buiten om de vereisten van de AVG te behandelen.

6.2 Verwerkingsgrondslag PSD II

Duidelijk is wel dat, gelet op de gegevens die in het kader van betaaldiensten worden verwerkt, waaronder de klantnaam, het bankrekeningnummer en financiële gegevens, er bij het verlenen van betaaldiensten vrijwel altijd sprake zal zijn van een vorm van verwerking van persoonsgegevens. Op grond van de AVG (en de Wbp) mogen persoonsgegevens alleen worden verwerkt als een van de zes limitatieve grondslagen voor verwerking van toepassing is.[30] In afwijking hiervan bepaalt art. 94 lid 2 PSD II dat een bank alléén toegang tot de persoonsgegevens van de betaaldienstgebruiker mag verstrekken aan betaaldienstverleners met de uitdrukkelijke toestemming van de betaaldienstgebruiker.[31] Dit om betaaldienstgebruikers (nog) meer bescherming te bieden. De betaaldienstgebruiker heeft het recht zijn toestemming op elk moment in te trekken. Nadat dit is gebeurd, mag de betaaldienstverlener de persoonsgegevens in beginsel niet langer verwerken. Hierop gelden enkele uitzonderingen, bijvoorbeeld indien de verdere verwerking noodzakelijk is in verband met een wettelijke verplichting.

In de systematiek van PSD II geeft de betaaldienstgebruiker uitdrukkelijke toestemming aan de TPP. De bank staat hier buiten en kan dus ook geen beperkingen opleggen aan de vorm of inhoud van de gegeven toestemming. Hierbij moet het voor de betaaldienstgebruiker steeds duidelijk zijn dat het verlenen van de betaaldienst waarvoor hij toestemming geeft, wordt verleend door de TPP en niet door de bank.

Zoals ook in de memorie van toelichting bij de Implementatiewet wordt benadrukt, komt in PSD II aan het begrip 'uitdrukkelijke toestemming' een '*PSD II-specifieke betekenis toe*'.[32] Dit betekent dat het niet hetzelfde inhoudt als hetzelfde begrip in de AVG, dat veronderstelt dat de gebruiker voldoende moet zijn geïnformeerd en door middel van een verklaring of duidelijke actieve handeling uitdrukking moet hebben gegeven aan zijn wil om toestemming te verlenen voor het verwerken van zijn persoonsgegevens. Volgens de minister van Financiën heeft '*gezien het lex specialis karakter van deze bepaling de betekenis die aan dit begrip wordt*

30 Dit hangt samen met het beginsel uit de algemeen geldende Europese privacyregels op grond van de AVG; volgens het beginsel van 'minimale gegevensverwerking' of 'dataminimalisatie' mag gegevensverwerking niet excessief zijn en moet de verwerking worden beperkt tot wat noodzakelijk is voor de doeleinden waarvoor persoonsgegevens worden verwerkt (zie par. 4.2.1 MvT bij de Regels ter uitvoering van Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119) (Uitvoeringswet Algemene verordening gegevensbescherming).

31 Art. II onder C Implementatiewet, geïmplementeerd in een nieuw in te voeren art. 7:515a BW.

32 MvT Implementatiewet, p. 26.

Dit artikel uit Onderneming en Financiering is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

gegeven op grond van PSD 2 voorrang ten opzichte van de betekenis op grond van de AVG'.

6.3 Toezicht

Vanwege de PSD II-specifieke betekenis dient DNB volgens de minister de inhoud van het begrip en de vormgeving van de uitdrukkelijke toestemming in te vullen en toe te passen.[33] De Autoriteit Persoonsgegevens (AP) heeft echter op eigen initiatief aan de minister van Financiën te kennen gegeven de verhouding van de Implementatiewet tot de AVG 'verwarrend' te vinden. Zo blijkt volgens de AP uit de Implementatiewet niet dat bij strijdigheid tussen de bepalingen van PSD II en de AVG voorrang toekomt aan de AVG. Gelet hierop acht de AP zich ook niet gebonden aan een rechtsoordeel van DNB over de naleving van de AVG.[34]

Inderdaad is er een zekere overlap tussen de eisen van de AVG en PSD II. Dit geldt ook voor het toezicht op de betaaldienstverleners voor wat betreft het verwerken van persoonsgegevens. Een betaaldienstverlener met vergunning van DNB die persoonsgegevens verwerkt, kan worden geconfronteerd met het toezicht van DNB op grond van de Implementatiewet en de AP op grond van de AVG. Immers, de AVG bepaalt dat elke verwerking van persoonsgegevens dient te geschieden overeenkomstig de AVG. Op grond van de AVG is de AP bevoegd om hierop toezicht te houden. Deze bevoegdheid bestaat náást de bevoegdheid van DNB op grond van PSD II, waarin onder andere is bepaald dat een betaalinstelling over een beveiligingsbeleid dient te beschikken om betaaldienstgebruikers te beschermen tegen beveiligingsrisico's, zoals fraude en illegaal gebruik van gevoelige betaalgegevens en persoonsgegevens.

De minister van Financiën heeft opgemerkt dat nu deze bevoegdheden van DNB en de AP naast elkaar bestaan, het wenselijk is dat de toezichthouders, voor zover mogelijk, samenwerken en hun toezicht op elkaar afstemmen.[35] Hoe dit handen en voeten moet krijgen, is op dit moment niet duidelijk. Wat inmiddels wel duidelijk is, is dat de AP kritisch meekijkt.

7 Tot slot: what's next? Open banking?

Een van de doelstellingen van PSD II is het stimuleren en faciliteren van innovatie door het reguleren van betaaldiensten die zijn ontstaan ná PSD. Dit wordt bereikt door het reguleren van betaalinitiatiediensten en rekeninginformatiediensten. Dit zal uiteraard directe gevolgen hebben voor de wijze waarop TPP's die nu betaalinitiatiediensten en rekeninginformatiediensten aanbieden, opereren. En dit biedt kansen voor nieuwe TPP's.

33 Nota van toelichting bij Implementatiebesluit, p. 17.

34 Zie autoriteitpersoonsgegevens.nl/nl/nieuws/ap-adviseert-over-wetsvoorstel-psd2 en de daarop te downloaden brief van de AP van de minister van 22 augustus 2017.

35 Implementatiebesluit, p. 17.

doi: 10.5553/OenF/157012472017025004002

Dit artikel uit Onderneming en Financiering is gepubliceerd door Boom juridisch en is bestemd voor anonieme bezoeker

Er wordt wel gezegd dat PSD II pas het begin van een veel grotere beweging is, en kansen biedt aan start-ups, FinTechs en andere bedrijven om nieuwe verdienmodellen en producten/diensten te ontwikkelen in een gereguleerde omgeving. In deze omgeving veranderen banken van gesloten systemen naar open platformen en ontstaat er een vorm van 'open banking'. Hierbij is er een belangrijke rol weggelegd voor API's: de digitale toegangspoorten tot de data en diensten van een bedrijf. Via de API's van bestaande banken kunnen betaaldienstverleners toegang krijgen tot betaalgegevens van de klanten van de banken, mits dezen daar toestemming voor geven. Dit is een interessant businessmodel voor zowel de banken als TPP's die toegang krijgen tot de betaalgegevens. Er zijn veel verschillende toepassingen te bedenken voor deze nieuwe, opener omgeving. Denk aan multibank-*wallets*, betalen via social media en automatische verbetering van persoonlijke financiën. Ook voor zakelijke klanten biedt dit kansen. Zo kan bijvoorbeeld boekhoudsoftware autonomer handelen en wordt het makkelijker om liquiditeitsprognoses te doen.

Omdat banken onder PSD II aan derden toegang moeten verlenen tot betaaldata en rekeninginformatie, is er in zekere zin sprake van 'open banking', maar bevinden deze data zich wel nog altijd in min of meer afgesloten systemen van banken. Immers, de beheerders van deze systemen (banken) moeten toegang verlenen aan derden om van die data gebruik te kunnen maken. Uit de in de inleiding van deze bijdrage aangehaalde mediaberichten over de 'strijd' tussen banken en FinTechs blijkt wel dat dit een zeker spanningsveld met zich brengt. De toegang tot betaaldata en rekeninginformatie biedt banken en FinTechs echter ook kansen. Een Londense bankier heeft dit treffend onderschreven:

> '*There's this knee-jerk reaction when you first talk about PSD II to think about banks in one playpen being concerned and the FinTechs in another playpen sharpening their pencils. But whether you're a bank or a FinTech, both groups are going to be able to access more data to create better tech solutions. Nothing is stopping a bank from accessing the data of other banks with those open APIs as well.*'[36]

Met blockchain is al technologie beschikbaar waarmee data volledig gedecentraliseerd worden beheerd. Als gevolg van de hiermee verband houdende ontwikkelingen lijkt het een kwestie van tijd dat financiële ondernemingen de stap zetten van gesloten naar open systemen. Wellicht dat PSD II dus slechts een eerste stap is op weg naar het werkelijke *open banking*: bankieren waar relevante data te allen tijde overal en voor iedereen beschikbaar zijn. Gezien deze ontwikkelingen zal PSD II zeker niet het eindstation zijn, en de komende regulering van betaalinitiatie- en rekeninginformatiediensten slechts een tussenstap om de interne markt voor betalingsverkeer te versterken en innovatie te stimuleren. Zoals wij in deze bijdrage hebben laten zien, hoeven banken en FinTechs daarbij niet tegenover elkaar te staan.

36 Zie ripple.com/insights/psd2-blockchain/.