De tweede Europese betaaldienstenrichtlijn (PSD2) en de risico's op fraude en witwassen

Versie 1.1
Oktober, 2017

Auteurs:
I. Lammerts MSc CFE (ABN AMRO)
D. Ma MSc (ABN AMRO)
N. Ploeger MSc (ANTI MONEY LAUNDERING CENTRE)
mr. B.A. Deutekom (BETAALVERENIGING NEDERLAND)
S.J. van Eerten MSc EMoC (DELOITTE)
N. Vink MSc (DE VOLKSBANK)
T.N. Wagemakers (FINANCIAL INTELLIGENCE UNIT)
K.I.M. Sanders MSc MA (KPMG)
C.L.S. Visser MSc (NATIONALE POLITIE / KNOOPPUNT FINEC)
R.B. Schaap MSc (NATIONALE POLITIE / TEAM HIGH TECH CRIME)

Disclaimer

Dit document is bedoeld als introductie van de herziene Europese betaaldienstenrichtlijn (PSD2) en gerelateerde risico's op het gebied van fraude en witwassen. Het is gebaseerd op de inbreng van de individuele auteurs, op persoonlijke titel geschreven en vertegenwoordigt op geen enkele wijze standpunten en/of beleid van de organisaties waaraan zij zijn verbonden. Hoewel de auteurs dit document met zorg hebben samengesteld en daarbij gebruik hebben gemaakt van bronnen die zij betrouwbaar achten, kunnen zij niet instaan voor de juistheid, volledigheid en actualiteit van het document.

Inhoudsopgave

1. Inleiding

1.1 Aanleiding

Het Anti Money Laundering Centre (AMLC) heeft in 2017 de thematafel witwassen via internet / new payments opgericht. De thematafel is een samenwerkingsverband tussen partijen afkomstig uit het publieke-, private- en wetenschapsdomein. Binnen de thematafel worden op fenomeenniveau verwachte en reeds onderkende witwasrisico's besproken. Doel hiervan is om te komen tot gemeenschappelijke onderwerpen, die in werkgroepverband met belanghebbende organisaties verder worden uitgewerkt tot concrete samenwerkingsproducten. Het eerste onderwerp dat in de thematafel is geselecteerd, is de tweede Europese betaaldienstenrichtlijn (PSD2) die in januari 2018 van kracht wordt.

Als gevolg van PSD2 moeten banken hun infrastructuur openen voor externe dienstverleners (TPP)[1], een proces dat ook wel toegang tot de betaalrekening (XS2A)[2] wordt genoemd. Hoewel innovatie in het betalingsverkeer wordt toegejuicht, bestaat de zorg dat criminelen hierdoor mogelijkheden krijgen om te frauderen en geld wit te wassen. Daarnaast kan PSD2 ook de nodige implicaties hebben voor de opsporing. Vanuit de thematafel is om die reden een zogenaamde PSD2-werkgroep opgericht om over dit onderwerp een gezamenlijk kennisdocument op te stellen. Deelnemers aan de werkgroep zijn ABN AMRO, AMLC, Betaalvereniging Nederland (BVN), Deloitte, Financial Intelligence Unit (FIU), ING Bank, KPMG, de Nationale Politie (Eenheid Amsterdam, Knooppunt FINEC en Team High Tech Crime) en de Volksbank.

1.2 Doelstelling en scope

De centrale vraagstelling waarover de PSD2 werkgroep zich heeft gebogen, is tweeledig; wat zijn *vanuit Nederlands perspectief* in hoofdlijnen de mogelijke veranderingen in het betaallandschap ten gevolge van de PSD2 en wat zijn de mogelijke risico's op fraude en witwassen met de invoering van de PSD2?

Dit gezamenlijke kennisdocument is opgesteld om de deelnemende organisaties aan de PSD2-werkgroep intern voor te lichten over de naderende veranderingen en de (mogelijke) risico's die hiermee gepaard gaan. Daarnaast zal het kennisdocument met haar conclusies en aanbevelingen worden aangeboden aan de relevante toezichthouders en partijen die een rol spelen bij de implementatie. Overigens is terrorismefinanciering bewust buiten de scope van dit document gehouden, omdat dit niet tot de focus van de thematafel behoort.

De inhoud van dit rapport is gebaseerd op ontwikkelingen tot 1 september 2017.

1.3 Onderzoeksvragen

Om de centrale vraagstelling te kunnen beantwoorden, zijn door de PSD2-werkgroep de volgende onderzoeksvragen geformuleerd:

1. Wat is het doel van de PSD2?
2. Wanneer en op welke wijze dient de PSD2 geïmplementeerd te worden?
3. Welke nieuwe (betaal)diensten worden er in de PSD2 geïntroduceerd?
4. Welk soort nieuwe (betaal)dienstverleners worden er in de PSD2 geïntroduceerd?
5. Welke verplichtingen hebben deze nieuwe (betaal)dienstverleners?

[1] TPP staat voor: third party payment service provider
[2] XS2A staat voor: access to the account.

6. Welke verplichtingen hebben bestaande betaaldienstverleners, zodra de nieuwe (betaal)dienstverleners actief worden?
7. Welke (risico)aspecten van de PSD2 zijn (nog) niet volledig uitgewerkt en onderhevig aan (nationale) interpretatie?
8. Wat zijn de fraude- en witwasrisico's voor banken en de betalingsdienstgebruikers zodra de PSD2 in werking treedt?
9. Welke gevolgen heeft de PSD2 voor de opsporing bij de bestrijding van fraude en witwassen?
10. Welke gevolgen heeft de PSD2 voor toezicht bij het voorkomen van fraude en witwassen?
11. Welke kansen biedt de PSD2 banken, consumenten, opsporing en toezicht om fraude en witwassen tegen te gaan?

1.4 Onderzoeksmethoden

Om antwoord te krijgen op de verschillende onderzoeksvragen, hebben leden van de PSD2-werkgroep literatuuronderzoek verricht en diverse partijen benaderd en bereid gevonden om over het onderwerp te praten. Zo zijn er gesprekken gevoerd met de Autoriteit Consument en Markt (ACM), de Autoriteit Financiële Markten, De Nederlandsche Bank (DNB) en de Nederlandse Vereniging van Banken (NVB). Ook is over het onderwerp informatie verkregen van International Cards Services (ICS) en het Ministerie van Financiën (MinFin). Door een aantal werkgroepleden is op 4 april 2017 deelgenomen aan een evenement georganiseerd door de Betaalvereniging Nederland en Holland FinTech over de PSD2. Om de voortgang te bespreken, taken te verdelen en te discussiëren over de inhoud van het kennisdocument, is de werkgroep een aantal keren bij elkaar gekomen.

N.b. Indien in het rapport verwezen wordt naar "de opsporingspraktijk", heeft dit betrekking op de kennis en ervaring van leden van de PSD2-werkgroep die werkzaam zijn binnen de opsporing.

1.5 Opbouw

Na dit inleidende hoofdstuk worden in hoofdstuk 2 de PSD2 en de (beoogde) veranderingen besproken. Vervolgens wordt ingegaan op de onderdelen van de PSD2 die een rol spelen bij het bespreken van de risico's op fraude en witwassen. Deze risico's komen aan bod in het derde hoofdstuk. Hoofdstuk 4 sluit het kennisdocument af met conclusies en aanbevelingen.

2. PSD2

2.1 Inleiding

In dit hoofdstuk wordt allereerst aandacht besteed aan de doelstellingen, reikwijdte en implementatie van de PSD2. Vervolgens worden de nieuwe betaaldiensten die in de PSD2 worden geïntroduceerd en de mate waarin de aanbieders van deze diensten onder toezicht en antiwitwaswetgeving vallen, besproken. Tot slot wordt ingegaan op onderdelen van de PSD2, waarover nog onduidelijkheid bestaat en die aan interpretatie onderhevig zijn, maar wel relevant zijn bij het bespreken van de risico's op fraude en witwassen in hoofdstuk 3.

2.2 Doelstellingen PSD2

De PSD2 kent een aantal doelstellingen: *"Ten eerste het versterken van een interne markt voor kaartbetalingen, internetbetalingen en mobiele betalingen. Ten tweede het stimuleren en faciliteren van innovaties, onder meer door het reguleren van verschillende betaaldiensten die zijn ontstaan na de publicatie van PSD I, zoals de genoemde betaalinitiatiediensten en rekeninginformatiediensten. Tot slot beoogt PSD II gesignaleerde problemen van PSD I, zoals achterhaalde of vage begrippen, te verhelpen. In het algemeen geldt dat is gezocht naar een balans tussen het stimuleren van innovatie enerzijds en veiligheid en consumentenbescherming anderzijds*"[3].

2.3 RTS over SCA

In de *Regulatory Technical Standards on strong customer authentication and secure communication under PSD2* (RTS over SCA) zijn bepalingen opgenomen, die zien op het proces rond authenticatie bij transacties en het beveiligen van het communicatiekanaal[4]. De RTS over SCA kunnen gezien worden als het technische raamwerk van de PSD2 en zijn opgesteld door de *European Banking Authority* (EBA)[5]. Ten tijde van het schrijven van dit kennisdocument, bevindt de RTS over SCA zich in conceptfase en moet de Europese Commissie nog een definitieve versie indienen bij het Europees Parlement en de Europese Raad ter goedkeuring. Op politiek niveau is nog geen consensus over of de toegang ten gevolge van de RTS over SCA enkel via een *Application Programming Interface* (API) mag geschieden, zoals de draft nu voorschrijft, of dat *direct access* ook door aanbieders van betaalrekeningen (ASPSP[6]), met name banken, moet worden toegestaan als terugvaloptie, indien de API niet werkt. Bij *direct access* logt de betalingsdienstgebruiker zelf handmatig in via het online portaal van zijn betaalrekening, een werkwijze dat ook wel *screenscraping* wordt genoemd. In het kader van PSD2 zijn dit alleen geen synoniemen van elkaar. De PSD2 schrijft namelijk voor dat de TPP zich bij iedere transactie dient te identificeren bij de ASPSP, onder meer genoemd in artikel 66 lid 3 onder d. Het onder de naam van een betalingsdienstgebruiker inloggen door een TPP zoals bij *screenscraping* het geval is, is onder de PSD2 niet toegestaan. De inhoud van de RTS over SCA kan de komende tijd op een aantal onderdelen dus nog wijzigen. Na goedkeuring door het Europees Parlement en de Europese Raad zal het nog 18 maanden duren, voordat de regels van de RTS over SCA van kracht worden.

---

[3] Ministerie van Financiën & Ministerie van Veiligheid en Justitie (2016). *Memorie van toelichting op de implementatiewet herziene richtlijn betaaldiensten*. Den Haag.

[4] Deze onderwerpen worden verder behandeld in paragraaf 2.8 en paragraaf 2.9 van dit kennisdocument.

[5] Door EBA worden in het kader van PSD2 In totaal vijf RTS en vijf *guidelines* opgesteld.

[6] ASPSP staat voor account servicing payment service provider.

2.4 Reikwijdte

De reikwijdte van de PSD2 wordt ten opzichte van haar voorganger op een tweetal punten uitgebreid. De eerste Europese Betaaldienstenrichtlijn (PSD1) introduceerde toezicht op betaaldienstverleners voor zover de bij de betaaltransactie betrokken betaaldienstverleners beiden zijn gevestigd in een EU lidstaat en voor zover de betaaldienstverleners transacties verrichten in een valuta van een lidstaat. Betaaldienstverleners die onder de PSD2 vallen, hebben een vergunning nodig als betaalinstelling indien de betaaldiensten worden verricht in de uitoefening van beroep of bedrijf. De volgende situaties vallen binnen het bereik van de PSD2:

- Transacties waarbij slechts één van de twee betaaldienstverleners in een EU-lidstaat is gevestigd; en
- Betaaldiensten in elke valuta voor zover deze binnen de EU plaatsvindt[7].

Er zijn ook uitzonderingen op de reikwijdte van de richtlijn, die worden genoemd in artikel 3 van de richtlijn (2015/2366). In de Memorie van Toelichting die ziet op de implementatie van de PSD2 in de Nederlandse wet, worden de drie belangrijke uitzonderingen uiteengezet[8]:

1. Kleine, beperkte netwerken vallen buiten de reikwijdte van de PSD2. Van een beperkt netwerk is sprake indien een betaaldienst alleen in bepaalde, in de preambule van de richtlijn genoemde, omstandigheden kan worden gebruikt. Beperkte netwerken die gebruik maken van de vrijstelling zijn verplicht dit te melden aan DNB[9].
2. De beperking met betrekking tot betaaldiensten die worden verricht via telecomapparatuur of –netwerken, wordt strikter gedefinieerd[10]. Betalingstransacties die verband houden met het inzamelen van giften voor liefdadigheidsinstellingen en betalingstransacties onder een wettelijk bepaalde drempel, worden uitgezonderd van de reikwijdte van de PSD2[11]. Indien gebruik wordt gemaakt van de genoemde uitzonderingen, dient dit te worden gemeld aan DNB.
3. De beperking met betrekking tot handelsagenten wordt aangepast. Agenten die alleen voor rekening de betaler dan wel de begunstigde handelen, worden uitgezonderd van de PSD2, ongeacht of zij in het bezit zijn van de geldmiddelen van hun cliënten. Agenten die voor rekening van zowel de betaler als de begunstigde handelen, worden alleen uitgezonderd indien zij op geen enkel moment in het bezit zijn van of controle hebben over de geldmiddelen van hun cliënten[12] [13].

2.5 Implementatie

De richtlijn gaat uit van volledige harmonisatie, hetgeen betekent dat lidstaten niet mogen afwijken van datgene dat is voorgeschreven in de richtlijn. Er mogen door lidstaten dus ook geen strengere eisen worden gesteld. Landen in de Europese Economische Ruimte (EER) zijn verplicht om uiterlijk op 13 januari 2018 de richtlijn te hebben geïmplementeerd in de lokale wetgeving. In Nederland zal implementatie plaatsvinden via de Wet op het financieel toezicht (Wft) en boek 7 van het Burgerlijk

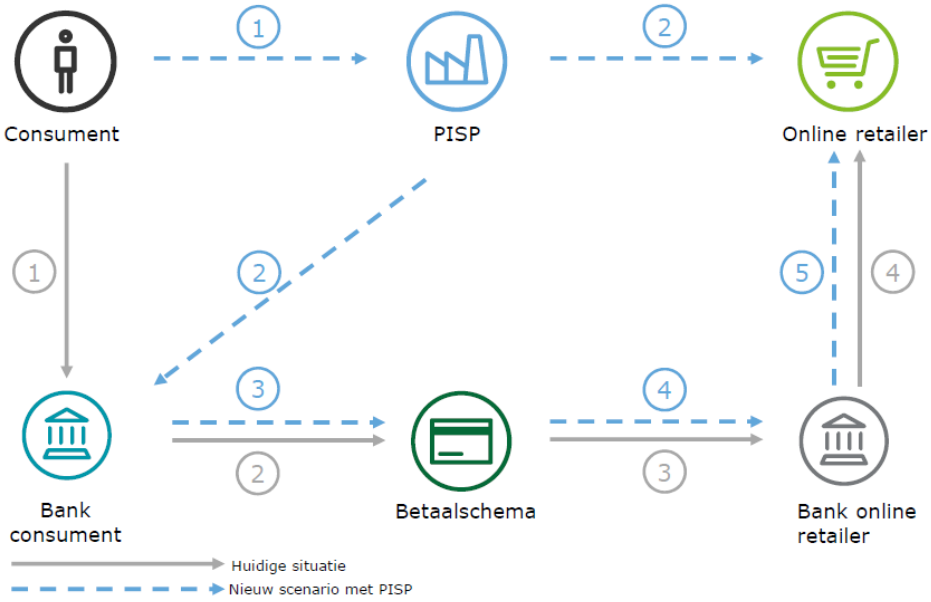
[7] Artikel 2 van de PSD2.
[8] Ministerie van Financiën & Ministerie van Veiligheid en Justitie (2016). *Memorie van toelichting op de implementatiewet herziene richtlijn betaaldiensten*. Den Haag.
[9] Overweging 13 van de PSD2.
[10] Overweging 16 van de PSD2.
[11] Overweging 16 van de PSD2.
[12] Overweging 11 van de PSD2.
[13] Ministerie van Financiën & Ministerie van Veiligheid en Justitie (2016). *Memorie van toelichting op de implementatiewet herziene richtlijn betaaldiensten*. Den Haag.

Wetboek. Ten gevolge van de PSD1 zijn in deel 7B van boek 7 wetsartikelen opgenomen over onder meer de uitvoering, instemming en aansprakelijkheid bij een betalingstransactie[14]. De officiële consultatieronde is inmiddels gesloten, maar het wetsvoorstel dient in Nederland nog voorgelegd en goedgekeurd te worden door het parlement. Zoals opgemerkt, laat de inwerkingtreding van de RTS over SCA door het Europees Parlement en de Europese Raad – na goedkeuring – nog minimaal 18 maanden op zich wachten. De PSD2 kent een aantal nieuwe vergunningsvereisten voor betaalinstellingen, die in Nederland worden uitgewerkt bij algemene maatregel van bestuur. In de praktijk moeten banken in beginsel al vanaf 18 januari 2018 derde partijen - zoveel mogelijk in de geest van de RTS over SCA - toegang verlenen tot de betaalrekeningen van hun klanten, indien de klant hier uitdrukkelijke toestemming voor geeft. DNB zal in deze periode toezicht houden of derde partijen die toegang willen, procedures rond authenticatie en beveiliging op orde hebben. Op het moment van schrijven is niet bekend hoe DNB banken zal informeren over de uitkomsten.

2.6 Nieuwe betaaldiensten

2.6.1 AISP & PISP

De PSD2 introduceert twee nieuwe soorten betaaldiensten en betaaldienstverleners (PSP)[15]; namelijk de betaalinitiatiedienstverlener (PISP[16]) en de rekeninginformatiedienstverlener (AISP[17])[18].

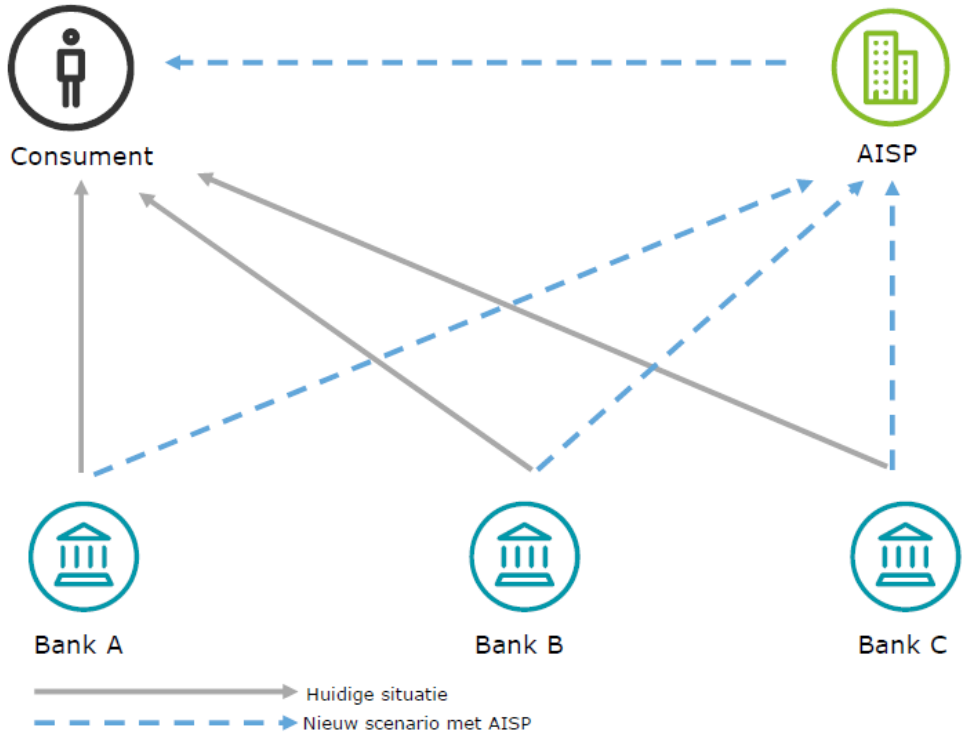


Figuur 1. Betaaldienst PISP schematisch weergegeven.

Een PISP kan in opdracht van een gebruiker een betaling verrichten, zoals voor de aankoop van een product in een webwinkel. De gebruiker kan een PISP hiervoor toestemming verlenen voor het verkrijgen van toegang tot zijn betaalrekening bij een *andere* betaaldienstverlener, zoals een bank. Het

[14] Wet van 15 oktober2009 tot wijziging van de Wet op het financieel toezicht, het Burgerlijk Wetboek en de Wet inzake geldtransactiekantoren en intrekking van de Wet op het grens overschrijdend betalingsverkeer ter implementatie van richtlijn nr.2007/64/EG van het Europees Parlementen de Raad betreffende betalingsdiensten in de interne markt en tot wijziging van de Richtlijnen 97/7/EG, 2002/65/EG, 2005/60/EG en 2006/48/EG, en tot intrekking van Richtlijn97/5/EG(PbEUL319).
[15] PSP staat voor payment service provider.
[16] PISP staat voor payment initiation service provider.
[17] AISP staat voor account information service provider.
[18] Artikel 4 van de PSD2.

onderwerp toegang tot betaalrekeningen wordt behandeld in paragraaf 2.7. Een PISP mag niet op enig moment in het bezit komen van de geldmiddelen van de betalingsdienstgebruiker[19]. Bedrijven die producten en of diensten aanbieden aan consumenten, krijgen door de PSD2 de mogelijkheid om het betalen te integreren in de complete gebruikerservaring. Denk bijvoorbeeld aan een klantenpas of mobiele app van een winkel, waarin betaalgegevens, kortingen en spaarpunten gecombineerd worden en de klant automatisch draadloos kan afrekenen bij het verlaten van de winkel.



Figuur 2. Betaaldienst AISP schematisch weergegeven.

Een voorloper van een rekeninginformatiedienst is AFAS Personal, een online huishoudboekje waarmee onder meer (grafisch) inzicht kan worden verkregen in uitgaven, en budgetten en begrotingen kunnen worden opgesteld. Een AISP kan in opdracht van een gebruiker geconsolideerde informatie verstrekken, afkomstig van een of meerdere betaalrekeningen bij een of meerdere ASPSP's. Een AISP mag echter geen gevoelige betaalgegevens opvragen[20]; dit zijn gegevens waarmee fraude kan worden gepleegd, waaronder persoonlijke beveiligingsgegevens[21]. Het geven van financieel advies valt overigens niet onder de vergunning van een rekeninginformatiedienst.

2.6.2 Markttoegang en toezicht

PISP's zijn als betaalinstellingen vergunningplichtig en vallen onder het *risk based* integriteitstoezicht van DNB. Daarnaast kunnen PISP's ook gebruik maken van het zogenaamde EU Paspoort, waarmee het mogelijk is om, in geval van een verleende vergunning in een lidstaat, de dienstverlening ook in andere lidstaten aan te bieden. Hoewel AISP's ook onder de categorie betaalinstellingen vallen en gebruik kunnen maken van een EU Paspoort, worden zij vrijgesteld van een deel van de verplichtingen[22]. Ook zal sprake zijn van een mildere vorm van integriteitstoezicht door DNB.

[19] Artikel 66 lid 3 onder a van de PSD2.
[20] Artikel 67 lid 2 onder e van de PSD2.
[21] Artikel 4 lid 1 onder 32 van de PSD2.
[22] Artikel 33 lid 2 van de PSD2.

Bij de aanvraag voor een vergunning als betaalinstelling wordt een aantal eisen gesteld, waaronder beschrijvingen van:

- een bedrijfsplan met budgetprognose voor de eerste drie boekjaren;
- een bewijs van aanvangskapitaal;
- een waarborg of verzekering ter dekking van de geldmiddelen van haar gebruikers;
- processen om klachten en veiligheidsincidenten af te halen;
- een beveiligingsbeleid onder andere voor de bescherming van haar gebruikers tegen fraude en illegaal gebruik van (persoonlijke) data;
- (indien van toepassing) interne controlemechanismen om te voldoen aan verplichtingen die voortvloeien uit Europese antiwitwaswetgeving;
- de identiteit van managers en bestuurders, alsmede een bewijs dat zij betrouwbaar en bekwaam zijn[23].

In tegenstelling tot de PSD1 heeft de PSD2 als extra *vergunningseis* dat betaalinstellingen zich in een lidstaat mogen vestigen als ten minste een substantieel deel van de werkzaamheden ook daadwerkelijk in deze lidstaat plaatsvindt[24]. Deze zogenaamde *substance* eis is in de PSD2 niet nader geconcretiseerd. Bestuurders worden door DNB bij de aanvraag van een vergunning gescreend op betrouwbaarheid[25] en geschiktheid[26]. Bestuurders hoeven niet de nationaliteit te bezitten van het land van vestiging. Ten opzichte van de PSD1 verruimt de PSD2 de mogelijkheden om een vergunning weer in te trekken; namelijk in geval het vertrouwen in het betaalverkeer in het geding is of als de toezichthouder niet geïnformeerd is over belangrijke ontwikkelingen die te maken hebben met de voorwaarden van de vergunning[27].

In Nederland spelen behalve DNB[28] ook andere toezichthouders een rol bij het toezicht op de betaalinstellingen, namelijk de ACM[29], de AFM[30] en de Autoriteit Persoonsgegevens[31]. De ACM heeft naast het mededingingstoezicht ook toezicht op onder meer toegang tot betalingssystemen en de toegang van TPP's tot betaalrekeningdiensten van kredietinstellingen[32]. Het gedragstoezicht van de AFM is gericht op eerlijke en transparante financiële marktprocessen, zuivere verhoudingen tussen marktpartijen en de zorgvuldige behandeling van zowel betaaldienstverleners als betalingsdienstgebruikers. Er lijkt rond de onderwerpen markttoegang, het gedrag van betaaldienstverleners naar de betalingsdienstgebruiker en fraude-incidenten overlap te zijn in de toezichttaken van ACM, AFM en DNB. Bij incidenten rond witwassen, zal DNB de aangewezen toezichthouder zijn. De Autoriteit Persoonsgegevens houdt toezicht op het gebruik en verwerken van persoonsgegevens. DNB houdt hiernaast toezicht op de in PSD2 opgenomen regels ten aanzien van

[23] Artikel 5 lid 1 van de PSD2.
[24] Artikel 11 lid 3 van de PSD2.
[25] Artikel 5 lid 1 onder n van de PSD2.
[26] Artikel 5 lid 1 onder m van de PSD2.
[27] Artikel13 lid 1 onder c en d van de PSD2.
[28] Artikel 1:24 lid 2 van de Wft.
[29] Artikel 1:25a van de Wft.
[30] Artikel 1:25 lid 2 van de Wft.
[31] Nu nog op grond van de Wet bescherming persoonsgegevens (WBP), per 25 mei 2018 op grond van de Algemene Verordening Gegevensbescherming (AVG) en Uitvoeringswet Algemene verordening gegevensbescherming artikel 6 lid 2.
[32] Artikel 36 van de PSD2.

gegevensbescherming in het kader van vergunningverlening en het doorlopend toezicht[33]. Op Europees niveau is EBA de toezichthouder op de naleving van de PSD2.

2.7 Definitie betaalrekening

In de PSD2 wordt geen afgebakende definitie van het begrip betaalrekening gegeven. De betaalrekening dient wel online raadpleegbaar te zijn om benaderd te kunnen worden door AISP's en PISP's[34]. Vooralsnog gaat het om rekeningen in wettelijk erkende valuta, waarvan het tegoed vrij besteedbaar is: *"een op naam van een of meer betalingsdienstgebruikers aangehouden rekening die voor de uitvoering van betalingstransacties wordt gebruikt"*[35]. De reikwijdte van het begrip betaalrekening die in de PSD2 gehanteerd wordt, lijkt overeenkomstig met de definitie zoals deze is gegeven in Europese richtlijn ten aanzien van betaalrekeningen die in 2014 werd gepubliceerd (2014/92/EU):

> *"betaalrekeningen waarmee consumenten ten minste:*
> *a) geldmiddelen op een betaalrekening kunnen plaatsen;*
> *b) contanten van een betaalrekening kunnen opnemen;*
> *c) betalingstransacties, met inbegrip van overmakingen van en naar derden, kunnen ontvangen, respectievelijk uitvoeren.*
> *De lidstaten kunnen besluiten alle bepalingen van deze richtlijn of een deel ervan toe te passen op andere betaalrekeningen dan in de eerste alinea bedoelde."*

Hoewel in eerste instantie gedacht wordt aan betaal- en (sommige) spaarrekeningen bij banken, biedt de definitie ruimte aan betaalrekeningen die beheerd worden bij andere instellingen, zoals aanbieders van (prepaid)creditcards en e-money accounts die aangewend kunnen worden voor betalingen aan derden. Onduidelijk is het standpunt van de Europese Commissie hieromtrent.

2.8 Toegang tot betaalrekeningen

Zoals opgemerkt, introduceert de PSD2 de toegang tot betaalrekeningen voor AISP's en PISP's. De AISP verrichten diensten waarvoor de betalingsdienstgebruiker uitdrukkelijk toestemming voor geeft[36] en heeft alleen toegang tot de informatie van de aangewezen betaalrekeningen en de betrokken betalingstransacties[37]. PSD2 stelt geen regels over welke gegevens moeten worden gedeeld en of historische gegevens hier ook onder vallen. Duidelijkheid hierover bepaalt de mogelijkheden van de toekomstige dienstverlening. De PSD2 regelt de mogelijkheden voor PISP's om betalingen te initiëren op verzoek van de rekeninghouder[38]. Een PISP mag niet in het bezit komen van de geldmiddelen van de betalingsdienstgebruiker[39]. Ook mogen geen gevoelige betaalgegevens worden opgeslagen[40]. Er is geen volledige toegang tot een rekening van een klant bij de ASPSP.

---

[33] Ministerie van Financiën & Ministerie van Veiligheid en Justitie (2016). *Memorie van toelichting op de implementatiewet herziene richtlijn betaaldiensten*. Den Haag, p.8.
[34] Artikel 66 lid 1 en artikel 67 lid 1 van de PSD2.
[35] Artikel 4 onder 12 van de PSD2.
[36] Artikel 67 lid 2 onder a van de PSD2.
[37] Artikel 67 lid 2 onder d van de PSD2.
[38] Artikel 66 lid 1 van de PSD2.
[39] Artikel 66 lid 3 onder a van de PSD2.
[40] Artikel 66 lid 3 onder e van de PSD2.

Een ASPSP mag de toegang tot de betaalrekening ontzeggen als er een objectief vermoeden is van frauduleuze toegang tot de betaalrekening[41]. De toegang tot de betaalrekening moet volgens de concept RTS over SCA via een API tot stand komen. De betrokken betaaldienstverleners dienen dit te faciliteren. Er zijn geen regels omtrent één uniforme API, bijvoorbeeld niet hoe deze ontwikkeld of geïmplementeerd moet worden. Iedere ASPSP dient dit zelf in te regelen. Wel bestaat de eis dat de API hetzelfde niveau van beschikbaarheid en performance moeten bieden als de omgeving die de betaalrekeninghouder gebruikt[42]. Er rust wel een onderzoeksplicht op ASPSP's, voordat aan een TPP toegang tot de API wordt verleend. XS2A is een recht van de betaalrekeninghouder en betreft een overeenkomst tussen de betaalrekeninghouder en de TPP. Het aanbieden van betaalinitiatiediensten en rekeninginformatiediensten mag niet afhankelijk zijn van overeenkomsten tussen ASPSP's en TPP's[43]. Bij geschillen hieromtrent is AFM vanuit gedragstoezicht de aangewezen toezichthouder. Zoals opgemerkt in paragraaf 2.3 over de RTS over SCA, vindt op Europees niveau momenteel een discussie plaats of en onder welke omstandigheden *direct access*, als terugvaloptie indien de API niet werkt, wordt toegestaan.

2.9 Sterke klantauthenticatie

Hoewel de RTS over SCA op 13 januari 2018 nog niet van kracht zijn, zijn betaaldienstverleners vanaf dat moment wel al verplicht om SCA toe te passen krachtens artikel 97 van de PSD2. De authenticatie van een betaalopdracht dient daarnaast elementen te bevatten die, in geval van een transactie, de transactie dynamisch linken aan een specifiek bedrag en een specifieke begunstigde. Tot het moment dat de RTS over SCA in werking is getreden, 18 maanden na goedkeuring door het Europees Parlement en de Europese Raad, zal SCA zoveel mogelijk in de geest van de RTS over SCA dienen te worden toegepast. Authenticatie wordt omgeschreven als een procedure waarmee een betaaldienstverlener de identiteit van een betalingsdienstgebruiker dan wel de validiteit van het gebruik van een specifiek betaalinstrument kan verifiëren. Het gebruik van de persoonlijke beveiligingsgegevens van de betalingsdienstgebruiker is hierbij inbegrepen[44]. Deze verificatie vindt plaats door de zogeheten SCA. Sterke authenticatie maakt gebruik van minimaal twee van de volgende factoren:

1. Kennis (iets wat alleen de gebruiker weet)
2. Bezit (iets wat alleen de gebruiker heeft)
3. Inherente eigenschap (iets wat de gebruiker is)[45].

Deze factoren moeten onderling onafhankelijk zijn, zodat compromittering van één van deze factoren geen afbreuk doet aan de betrouwbaarheid van de andere factoren en de vertrouwelijkheid van de authenticatiegegevens wordt beschermd[46]. Voorbeelden van kennis zijn wachtwoorden, pincodes of het tekenen van patronen (zoals bij het ontgrendelen van een mobiele telefoon). Met bezit wordt bedoeld iets waarmee een code gegenereerd kan worden. Dit kan bijvoorbeeld een telefoon zijn waarop via sms of via een mobiele applicatie een authenticatiecode wordt ontvangen. Het kan ook een apparaat zijn waarop een code verschijnt via een druk op een knop. Een code kan ook gebaseerd zijn op tijd waarbij een apparaat om de dertig of zestig seconden een nieuwe code genereert, omdat

[41] Artikel 68 lid 5 van de PSD2.
[42] Artikel 32 lid 1 van de concept RTS over de SCA (EBA/RTS/2017/02).
[43] Artikel 66 lid 5 en artikel 66 lid 5 van de PSD2.
[44] Artikel 4, lid 29. RICHTLIJN (EU) 2015/2366 VAN HET EUROPEES PARLEMENT EN DE RAAD van 25 november 2015 betreffende betalingsdiensten in de interne markt (PbEU 2015, L337/58)
[45] Artikel 4 lid 1 van de concept RTS over SCA (EBA/RTS/2017/02).
[46] Artikel 4 lid 30 van de PSD2.

de vorige niet meer geldig is. Tot slot kan een apparaat ook een geïntegreerd toetsenbord hebben waarop de gebruiker eerst een code moet invoeren voor het apparaat een nieuwe code genereert; het gaat hierbij om een combinatie van bezit en kennis in één code. Voorbeelden van inherente eigenschappen tenslotte zijn een vingerafdruk, irisscan, stemopname en gezichtsherkenning. Hiervoor is eventueel extra hardware vereist.

Bij de vraag wie de SCA zal toepassen, zijn twee scenario's mogelijk. Het eerste scenario is dat de SCA door de PISP wordt overgelaten aan de ASPSP en hierbij gebruik wordt gemaakt van de door de ASPSP uitgegeven *credentials*. De PISP kan er ook voor kiezen om zelf *credentials* uit te geven en SCA toe te passen. Wanneer een betalingsdienstgebruiker ontkent dat hij of zij een uitgevoerde betalingstransactie heeft toegestaan of aanvoert dat deze niet correct is uitgevoerd, moet de betalingsdienstaanbieder het bewijs leveren dat de betalingstransactie geauthentiseerd, juist geregistreerd en geboekt was en dat geen technische storing of ander falen van de door betalingsdienstaanbieder aangeboden dienst plaatsvond[47]. In principe zal de betalingsdienstgebruiker bij een incident als eerste contact opnemen met de ASPSP van zijn betaalrekening. Daarnaast maakt de betalingsdienstgebruiker aanspraak op financiële compensatie wanneer de betalingsdienstaanbieder van deze betalingsdienstgebruiker geen sterke cliëntauthenticatie vereist (tenzij er sprake is van frauduleus handelen)[48]. Wanneer de aansprakelijkheid van een ASPSP kan worden toegerekend aan een andere betalingsdienstaanbieder of aan een intermediair, dan vergoedt de TPP of intermediair de ASPSP voor alle geleden verliezen, inclusief compensatie wanneer een van de betalingsdienstaanbieders geen sterke cliënt authenticatie toepast[49]. Het is tenslotte aan de nationale toezichthouders om ervoor te zorgen dat betalingsdienstaanbieders voorzien in sterke cliëntauthenticatie wanneer een betalingsdienstgebruiker zich online toegang tot zijn betaalrekening verschaft, een elektronische betalingstransactie initieert of via een communicatiemiddel op afstand een handeling uitvoert die een risico op betalingsfraude of andere vormen van misbruik met zich meebrengt[50].

Slechts onder stringente voorwaarden mag de SCA achterwege worden gelaten bij PSP's. Een concept dat hierbij een rol speelt, is transactie risicoanalyse (TRA)[51]. Als PSP's zich willen beroepen op het hanteren voor flexibelere authenticatiemethode bij transacties die als laag risico worden beoordeeld, dan moeten zij zich aan een aantal voorwaarden houden:

- Bij transacties met bedragen hoger dan 500 euro dient in elk geval, ongeachte de frauderatio, gebruik te worden gemaakt van SCA;
- in de meeste gevallen is het maximum bedrag lager, afhankelijk van het specifieke instrument dat wordt gebruikt. De EBA heeft voor elk instrument nu fraude ratio's gedefinieerd, en alleen in het geval dat de fraude ratio's lager liggen voor een bepaald instrument dan de door de EBA gezette *benchmark* fraude ratio's, mag een transactie zonder SCA worden uitgevoerd;
- dit betekent dat alle PSP's fraude ratio's moeten gaan bijhouden als ook het transparant maken van de TRA, die periodiek moet worden *ge-audit*.

[47] Artikel 72 lid 1 van de PSD2.

[48] Artikel 74 lid 2 van de PSD2.

[49] Artikel 92 lid 1 en artikel 74 lid 2 van de PSD2.

[50] Artikel 97 lid 1 en artikel 74 lid 2 van de PSD2.

[51] TRA staat voor transaction risk analysis.

2.10 Verwerken (persoons)gegevens

In artikel 94 lid 1 van de PSD2 wordt aangegeven dat persoonsgegevens door betaaldienstverleners mogen worden verwerkt in het kader van de voorkoming van, het onderzoek naar en de opsporing van betalingsfraude. Verder dienen natuurlijke personen op de hoogte te worden gesteld van deze verwerking conform de databeschermingsrichtlijn (Richtlijn 95/46/EG), welke in Nederland is omgezet in de Wet bescherming Persoonsgegevens (Wbp). Op 25 mei 2018 zal echter deze richtlijn worden ingetrokken. Daarvoor in de plaats zal de *General Data Protection Regulation* (GDPR) - in Nederland de Algemene Verordening Gegevensbescherming (AVG) genoemd - in werking treden, die een directe Europese werking kent en zodoende niet apart hoeft te worden geïmplementeerd in Nederlandse wetgeving.

In artikel 94, lid 2 van de PSD2 wordt voorts gesteld dat betalingsdienstaanbieders alleen met de uitdrukkelijke toestemming van de betalingsdienstgebruiker toegang mogen krijgen tot persoonsgegevens die noodzakelijk zijn voor het aanbieden van hun betalingsdiensten, deze gegevens mogen verwerken en bewaren. Hoewel expliciete toestemming vereist is, wordt zowel in de PSD2 zelf als in de zogeheten *explanatory notes*, geen verdere uitleg gegeven over hoe deze expliciete toestemming moet worden gegeven of vastgelegd[52].

[52] Voerman, A. (2017). *The implementation of PSD2 in the Netherlands*. Payments & Fintech Lawyer, p.11.

3. Risico's fraude en witwassen

3.1 Inleiding

Het uitgangspunt van de PSD2 waarbij aan een derde partij toegang tot de betaalrekening wordt verschaft, heeft implicaties voor de bescherming van klantdata, de veiligheid van het betalen en de integriteit van het betalingsverkeer. Aan de komst van de PSD2 zijn hierdoor enkele risico's verbonden, welke in dit hoofdstuk worden behandeld. Hoewel sprake is van overlap, zijn de risico's zoveel mogelijk onderverdeeld in:

- risico's op fraude;
- risico's op witwassen;
- risico's toezicht en opsporing.

Hierbij dient vooraf een aantal kanttekeningen geplaatst te worden. Ten eerste is de interpretatie van de PSD2 en de implementatie daarvan in nationale regelgeving nog niet volledig duidelijk. Daarnaast is nog niet bekend welke (nieuwe) mitigerende maatregelen door betaalinstellingen geïntroduceerd zullen worden en welk positief effect toezicht zal hebben op het beperken van de risico's. Dit betekent dat de hieronder beschreven risico's in eerste instantie *theoretisch* van aard zijn en dat op voorhand niets gezegd kan worden over de mate waarin deze risico's daadwerkelijk zullen plaatsvinden.

3.2 PDS2 en risico's op fraude

3.2.1 Onbetrouwbare en criminele TPP's

De inwerkingtreding van de PSD2 kan leiden tot een toename van (buitenlandse) TPP's die actief zijn op de Nederlandse betaalmarkt. Aangenomen wordt, dat het merendeel hiervan te goeder trouw zal zijn en conform de regels zal opereren. Een scenario waarmee rekening dient te worden gehouden, is dat de betaalsector ook geconfronteerd kan worden met onbetrouwbare en criminele TPP's.

ASPSP's wordt verplicht om, bij uitdrukkelijke toestemming van de betalingsdienstgebruiker, TPP's toegang te verlenen tot de betaalrekening. De vraag is echter of ASPSP's en consumenten de betrouwbaarheid van TPP's en de aangeboden betaalinfrastructuur voldoende kunnen beoordelen. Indien *direct access* wordt toegestaan, kan de ASPSP bovendien niet controleren of de TPP de transactie daadwerkelijk conform de wens van de betalingsdienstgebruiker uitvoert.

Daarnaast zijn ook twee andere risico's te benoemen. Kwaadwillenden die als doel hebben grootschalige (identiteits)fraude te plegen, kunnen hiertoe zelf een TPP opzetten om frauduleuze betalingen te faciliteren en/of toegang te krijgen tot een grote hoeveelheid vertrouwelijke gegevens. Zoals opgemerkt in hoofdstuk 2, krijgen AISP's bovendien te maken met een mildere vorm van integriteitstoezicht. Het opzetten van een 'criminele TPP' lijkt voor kleinschalige fraude een minder aannemelijk scenario, aangezien er eenvoudigere manieren bestaan om te frauderen. Groter is het risico dat door (cyber)criminelen gebruik gemaakt wordt van een bestaande TPP, door deze bijvoorbeeld te infecteren met *malware*.

Consumenten kunnen met deze frauduleuze TPP's in aanraking komen door bijvoorbeeld op nagemaakte websites of mobiele betaalapps hun gegevens in te voeren; een werkwijze die niet (veel) verschilt van *phishing*. De crimineel kan deze gegevens vervolgens misbruiken en met behulp daarvan informatie over de consument inzien en/of betalingen verrichten uit naam van deze consument (zie verder paragraaf 3.2.2). Onduidelijk is welke detectiesystemen er momenteel in staat zijn en/of erop ingericht zijn dit soort fraudepatronen te onderkennen en tegen te gaan (zie verder paragraaf 3.2.3).

Het is aantrekkelijk voor criminelen om te opereren in landen met een mild 'toezichtsklimaat'.

Innovatieve betaalapps worden in toenemende mate gebruikt in het online betalingsverkeer. Een risico is dat criminelen betaalapps ontwikkelen, die als doel hebben frauduleuze transacties mogelijk te maken en/of vertrouwelijke gegevens afhandig te maken.

3.2.2 Misbruik en phishing van gegevens

De risico's in deze subparagraaf worden beschreven, betreffen risico's die ook gelden voor de huidige betaalsector. De PSD2 werkgroep stelt dat de PSD2 de huidige risico's dusdanig beïnvloeden, dat deze risico's om die reden behandeld worden in dit kennisdocument.

In het geval dat *direct access* als *fallback* optie wordt toegestaan, is het mogelijk dat consumenten worden uitgenodigd om onder bepaalde omstandigheden persoonlijke informatie en inloggegevens af te geven aan TPP's. ASPSP's adviseren hun klanten echter sinds jaar en dag om geen vertrouwelijke (login)gegevens aan derde partijen te verstrekken, om te voorkomen dat zij slachtoffer worden van fraude. Voor consumenten wordt het verwarrend in welke gevallen, aan wie en op welke websites of betaalapps nu wel of geen vertrouwelijke (login)gegevens verstrekt kunnen worden; (kwetsbare groepen) consumenten kunnen immers niet toetsen of de API van hun ASPSP daadwerkelijk onvoldoende bereikbaar is en/of de aangeboden betaalinfrastructuur en de TPP betrouwbaar zijn.

Het is ook maar de vraag of consumenten zich bewust zijn van waar ze precies goedkeuring voor geven en wat de gevolgen hiervan kunnen zijn. Daarnaast bestaat het risico dat TPP's die gegevens verwerken van betalingsdienstgebruikers, slachtoffer worden van cyberaanvallen met datalekken tot gevolg. De data kan vervolgens door criminelen worden gebruikt (voor eigen gewin) of worden verkocht aan derden. Hoewel deze problematiek in eerste instantie te maken heeft met de databeveiliging van TPP's, kunnen ASPSP's hierdoor wel reputatieschade oplopen.

Zoals opgemerkt, krijgen AISP's te maken met een mildere vorm van integriteitstoezicht dan andere betaaldienstverleners, hetgeen ook risico's geeft wat betreft misbruik van gegevens. Het is bovendien maar de vraag of betalingsdienstgebruikers zich bewust zijn van welke gegevens TPP's van hen mogen verwerken. Het risico bestaat dat gevoelige gegevens gedeeld worden met kwaadwillende partijen.

De verwachting is dat criminelen daarnaast ook websites of betaalapps bouwen, waarmee ze zich voordoen als een PISP en/of valse schermen introduceren die ogenschijnlijk hetzelfde zijn als die van de inloginterface van de ASPSP of TPP, afhankelijk van wie de SCA uitvoert, om zodoende de beschikking te krijgen over vertrouwelijke gegevens van de betalingsdienstgebruiker. Bij afwezigheid van een echte TPP, zal de ASPSP (of de klant) verantwoordelijk worden gehouden voor de schade.

ASPSP's dienen hun klanten twee maanden voor de inwerkingtreding van de PSD2 te informeren over de nieuwe voorwaarden. Een risico is dat criminelen in deze periode *phishingmails* versturen om bij betalingsdienstgebruikers vertrouwelijke gegevens te ontfutselen. Als een frauduleuze TPP consumenten ook Burgerservicenummers ontfutselt, is het risico op (identiteits)fraude groot.

3.2.3 Verminderde fraudedetectie

De PSD2 opent de betaalmarkt voor nieuwe toetreders, die mogelijk nog geen ervaring hebben opgedaan met compliance en fraudedetectie. Ook zal de betaalketen veranderen en wordt door de PSD2-werkgroep een toename van internationale transacties verwacht. Dit kan mogelijk van invloed zijn op de kwaliteit en effectiviteit van fraudedetectie. ASPSP's dienen hun huidige detectiesystemen aan te passen aan de veranderingen in de betaalketen. Het kan tijd vergen om nieuwe detectieregels te schrijven, die voldoende (kunnen) anticiperen op mogelijke ongebruikelijke transacties via PISP's.

Momenteel is ook een ontwikkeling gaande om het betalingsverkeer te versnellen via *instant payments*, waardoor ook een versnelde cash-out mogelijk is. Het belang van adequate fraudedetectie bij ASPSP's neemt daarmee toe. Het risico dat fraudetransacties succesvol worden uitgevoerd, wordt groter. Daarnaast is nog onduidelijk hoe detectiesystemen bij PISP's worden georganiseerd; dit lijkt in de PSD2 nog onvoldoende te zijn beschreven. Zijn PISP's straks in staat om frauduleuze transacties, bijvoorbeeld ten gevolge van *phishing* of *malware*, te detecteren?

Een punt van zorg is in welke mate de informatiepositie van de ASPSP's door de komst van PISP's eventueel wordt ingeperkt. Indien SCA via de PISP loopt, zal de ASPSP mogelijk niet langer beschikken over informatie omtrent locatie en/of het apparaat waarmee wordt ingelogd. Dit zou betekenen dat het niet alleen langer zal duren, alvorens de detectiesystemen aangepast zijn aan de nieuwe betaalketen, maar ook dat deze systemen minder effectief zullen zijn. De ASPSP zal daarentegen wel over extra informatie beschikken, die betrekking heeft op de door de klant geautoriseerde TPP's.

PSP's hoeven onder bepaalde omstandigheden geen SCA toe te passen. Indien SCA niet wordt toegepast, zal het risico op fraude groter zijn. PSP's zijn in dat geval verplicht fraude ratio's bij te houden, alsmede een transparante TRA. Cruciaal hierbij is in hoeverre PSP's hiertoe in staat zijn en in hoeverre audit dan wel toezicht toereikend zal zijn om eventuele tekortkomingen te identificeren. De PSP's zijn zelf verantwoordelijk voor het inregelen van een robuust SCA proces. PSD2 bevat clausules die PSP's aansprakelijk stellen voor onrechtmatige transacties die plaatsvinden als gevolg van gebrekkige authenticatie. In die zin is er een positieve prikkel voor PSP's om authenticatie goed in te regelen. Artikel 73 en 74 van de PSD2 gaan over aansprakelijkheid van de betaaldienstverlener en het eigen risico van de consument voor niet-toegestane transacties. De ASPSP zal de klant onmiddellijk dienen te vergoeden bij niet-toegestane transacties, tenzij er sprake lijkt te zijn van fraude. Deze betaaldienstverlener, bijvoorbeeld de bank, kan zich verhalen op de PISP indien deze verantwoordelijk kan worden gehouden. Dat laatste is het geval als deze zich niet kan verantwoorden voor de sterke cliënt authenticatie (niet uitgevoerd of niet aantoonbaar uitgevoerd) of sprake lijkt te zijn van een technisch mankement. Hoewel de bewijslast hiervoor bij de PISP ligt, zal het risico en de eventuele reputatieschade in de praktijk vooral neerdalen bij de ASPSP. De PSD2 verlaagt het eigen risico van de betalingsdienstgebruiker bij schade ten gevolge van misbruik van €150 naar €50.

De PSD2 betekent echter ook een kans; in gevallen dat voortaan een TPP betrokken is bij een transactie, ontstaat een extra mogelijkheid tot fraudedetectie. De mogelijkheden om fraude te bestrijden zouden hierdoor een impuls kunnen krijgen, mits TPP's voldoende inregelen aan fraudedetectie.

3.3 PDS2 en risico's op witwassen

3.3.1 Inleiding

Betaalinstellingen dienen te voldoen aan de verplichtingen die voortvloeien uit de Wet ter voorkoming van witwassen financieren terrorisme (Wwft). Dit betekent dat ook AISP's en PISP's onder meer processen dienen in te richten ten behoeve van cliëntenonderzoek en het melden van ongebruikelijke transacties. De FIU-Nederland is op basis van de Wwft de organisatie waar diverse meldplichtige instellingen (voorgenomen) ongebruikelijke transacties dienen te melden. De FIU onderzoekt of transacties en geldstromen (mogelijk) gerelateerd zijn aan witwassen, financiering van terrorisme of onderliggende misdrijven. Nadat transacties verdacht zijn verklaard door het hoofd van de FIU-

Nederland, worden deze ter beschikking gesteld aan diverse handhavings- en opsporingsdiensten. De opsporing kan de FIU-Nederland daarnaast bevragen in geval van een verdenking van een strafbaar feit.

In Nederland wordt momenteel de vierde Europese anti-witwasrichtlijn geïmplementeerd, die op 26 juni 2017 in werking is getreden[53]. De belangrijkste wijzigingen voor betaaldienstverleners en betaalinstellingen zijn:

- een uitbreiding van de risicogebaseerde benadering van de verplichtingen van de Wwft, die onder meer tot uitdrukking komt in de verplichting voor instellingen om een risicoanalyse op te stellen;
- wijzigingen in de verplichtingen van het cliëntenonderzoek;
- een uitbreiding van het handhavingsinstrumentarium voor de toezichthouder;
- de introductie van publicatiebevoegdheden voor de toezichthouder, met betrekking tot opgelegde administratieve maatregelen en sancties;
- FIU's krijgen ten gevolge van de richtlijn meer bevoegdheden ter bevordering van de internationale informatie-uitwisseling en samenwerking tussen de FIU's.

Daarnaast wordt momenteel onderhandeld over het richtlijnvoorstel tot wijziging van de vierde anti-witwasrichtlijn, dat in de zomer van 2016 door de Europese Commissie is gepubliceerd[54]. Voor betaaldienstverleners en betaalinstellingen die binnen de reikwijdte van PSD2 vallen, is een aantal onderdelen van het richtlijnvoorstel met name relevant. Voorgesteld wordt onder meer om:

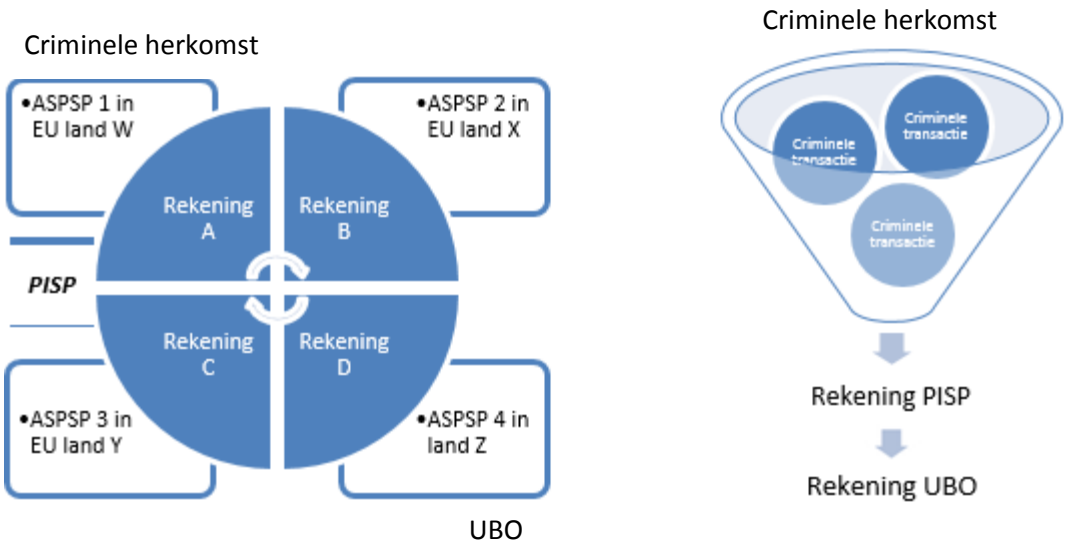
- de reikwijdte van de vierde anti-witwasrichtlijn uit te breiden naar platforms voor het omwisselen van virtuele valuta en wallet providers;
- de verplichtingen inzake cliëntenonderzoek in geval van elektronisch geld uit te breiden;
- de cliëntenonderzoeksmaatregelen in geval van 'hoog risico derde landen' te harmoniseren;
- lidstaten te verplichten een centraal register met informatie van bankrekeninghouders op te zetten.

De wijzigingen waarin dit richtlijnvoorstel voorziet zullen, wanneer de richtlijn eenmaal is vastgesteld, middels een separaat wetgevingstraject in de Nederlandse wet- en regelgeving worden geïmplementeerd.

3.3.2 Onbetrouwbare en criminele TPP's

Zoals opgemerkt in de vorige paragraaf, zal de komst van PSD2 naar verwachting leiden tot een toename van (buitenlandse) TPP's op de Nederlandse betaalmarkt. Met betrekking tot AISP's lijken er op voorhand niet direct witwasrisico's te bestaan; er kunnen immers via deze dienstverleners geen transacties worden verricht. PISP's daarentegen kunnen wel een risico vormen. Zo kan een criminele PISP via API's transacties *geautomatiseerd* uitvoeren, waarbij meerdere betaalrekeningen bij verschillende ASPSP's worden gebruikt (zie figuur 3, situatie A). Naarmate het spoor langer wordt, wordt het ook moeilijker om de daadwerkelijke herkomst van het geld te achterhalen en tijdrovender voor bijvoorbeeld de opsporing om geldstromen te volgen (zie ook paragraaf 3.4).

[53] Zie ook: https://www.internetconsultatie.nl/implementatiewetvierdeantiwitwasrichtlijn , geraadpleegd op 16 augustus 2017.
[54] Zie ook: http://ec.europa.eu/justice/newsroom/criminal/news/160705_en.htm , geraadpleegd op 16 augustus 2017.



Figuur 3. Geautomatiseerde betalingen via betaalrekeningen (situatie A) & verhullen UBO door PISP (situatie B).

Ter legitimering van de geldstroom is, afhankelijk van de bron en de bestemming van het geld, vaak ook een aanvullend middel noodzakelijk, zoals een contract, factuur of andere overeenkomst. Criminelen die bijvoorbeeld beschikken over crimineel vermogen op *open loop* prepaid kaarten[55], kunnen onder meer via een eigen onderneming voor fictieve goederen of diensten afrekenen, waarna het geld via de PISP verplaatst wordt naar één of meerdere betaalrekeningen in het buitenland. In beginsel kan hierbij de begunstigde van deze betalingen door de PISP niet worden verhuld, aangezien een PISP, in tegenstelling tot een collecterende PSP, niet in het bezit mag komen van de geldmiddelen van de betalingsdienstgebruiker. De ASPSP moet bovendien wel weten wat de tegenrekening is, anders kunnen de gelden niet worden overgeboekt. Uitzondering hierop is het geval dat een criminele PISP een 'eigen' rekeningnummer opgeeft, het geld ontvangt en vervolgens overmaakt naar de uiteindelijke begunstigde (zie figuur 3, situatie B). De ASPSP kan vermoedelijk niet vaststellen dat het een eigen betaalrekening van de PISP betreft en zal daarom de transactie gewoon uitvoeren.
Uit de opsporingspraktijk blijkt dat toezicht tot op transactieniveau niet vanzelfsprekend is; in de afgelopen jaren zijn door de FIOD en Nationale Politie verschillende witwasonderzoeken gedaan, waarin een financiële instelling in Nederland over een langere periode (als verdachte) betrokken was bij witwastransacties.

3.3.3 Toename internationale (witwas)transacties en inefficiënte meldketen

De inwerkingtreding van de PSD2 zal vermoedelijk (op termijn) leiden tot een toename van het aantal internationale transacties in het online betalingsverkeer en het aantal internationale betaalmogelijkheden. Hierdoor wordt het makkelijker om *afgeschermd vermogen*[56] in het buitenland aan te wenden voor betalingen in Nederland. PISP's met complexe internationale geldstromen,

[55] Dit zijn kaarten aangesloten op het MasterCard of VISA netwerk. Aan een prepaid kaart is een account gekoppeld, waarop vooraf eerst geld moet worden gestort. Afhankelijk van de aanbieder kan dit bijvoorbeeld met contant of giraal geld, maar ook via allerlei andere betaalmethoden die op internet te gebruiken zijn.
[56] Vermogen dat niet fiscaal is aangegeven en/of van criminele herkomst is en dat verborgen wordt gehouden voor de overheid.

kunnen bovendien bedoeld (in geval van een criminele PISP) of onbedoeld witwassen faciliteren. De meldketen is derhalve niet alleen versnipperd over verschillende partijen, maar ook over verschillende landen. De ervaring leert dat instellingen en bedrijven die meldplichtig zijn, het soms lastig vinden om mogelijke witwastransacties te onderkennen; uit opsporingsonderzoeken blijkt dat transacties die gemeld hadden moeten worden, niet waren gemeld.
Doordat klantcontact bovendien steeds digitaler wordt en direct klantcontact (face-to-face) vermindert, veranderen ook de 'ken je klant' processen voor banken en dienen betrokken partijen hun witwas-detectiesystemen hierop aan te passen.

Het classificeren van TPP's ten behoeve van het vaststellen van risico-indicatoren kan voor ASPSP's een uitdaging betekenen. Grote bekende (online) winkels die bijvoorbeeld een vergunning hebben als PISP, zullen niet snel een verhoogd risico met zich meebrengen, maar een (buitenlands) bedrijf dat in virtuele valuta handelt, mogelijk wel. In geval voor een ASPSP niet geheel duidelijk is wat voor soort dienstverlening een PISP aanbiedt, kan dit mogelijk voor problemen zorgen.

Meldingen van ongebruikelijke dan wel verdachte transacties worden door betaaldienstverleners in het land van vestiging gedaan. Ongebruikelijke transacties worden echter niet automatisch gedeeld met FIU's van andere landen. Verdachte transacties worden pas met de FIU van een ander land gedeeld, indien sprake is van een *hit* met een subject uit een strafrechtelijke onderzoek. Vervolgens is een rechtshulpverzoek noodzakelijk om de gegevens te kunnen gebruiken in een strafrechtelijk onderzoek. De vierde anti-witwasrichtlijn biedt meer mogelijkheden voor internationale samenwerking en uitwisseling van gegevens tussen FIU's. De praktijk zal leren of dit voldoende zal zijn om zicht te krijgen op dubieuze internationale transacties van Nederlandse ingezetenen via buitenlandse TPP's.

Opgemerkt dient te worden dat de toetreding van TPP's, AISP's in het bijzonder, ook voordelen kunnen bieden bij de bestrijding van witwassen. Zo kunnen AISP's over waardevolle gegevens beschikken ten aanzien van zicht op (onverklaarbaar) vermogen en het melden van ongebruikelijke transacties.

3.4 Risico's toezicht en opsporing

Bij het toezicht op de betaaldienstverleners zijn verschillende toezichthouders betrokken; in Nederland zijn dit de AP, de ACM, de AFM en DNB. De toezichthouders dienen nationaal samen te werken om de implementatie en de uitvoering van PSD2 in goeden banen te leiden. Ook vanuit internationaal perspectief zijn er de nodige uitdagingen. Niet-ingezetenen kunnen in Nederland bijvoorbeeld een TPP beginnen. DNB zal in dit geval de bestuurders moeten screenen op *betrouwbaarheid* en *geschiktheid*. Hiervoor is de Nederlandse toezichthouder afhankelijk van informatie die wordt aangeleverd door buitenlandse toezichthouders. Een andere vraag is in hoeverre Europees toezicht geconvergeerd is en of EU landen op uniforme wijze reguleren en handhaven. Zoals gezegd, verwacht de PSD2-werkgroep een toename van internationale transacties via PSP's. Een gevolg kan zijn dat buitenlandse PSP's een grotere rol op de Nederlandse betaalmarkt gaan spelen. De mate waarin toezicht een risico vormt, hangt voor een deel samen met de mate van strengheid en fraudegevoeligheid van het proces waarmee een PSP kan worden opgericht en de mate waarin de bedrijfsvoering wordt gecontroleerd.

Voor entiteiten die vermogen willen verhullen in het buitenland, wordt het eenvoudiger dit vermogen aan te wenden voor reguliere betalingen in Nederland. Door gebruik te maken van buitenlandse PSP's, zullen deze transacties niet snel worden opgemerkt door de fiscus. Het beschikken over een Nederlandse bankrekening lijkt minder belangrijk te worden om deel te kunnen nemen aan het reguliere betalingsverkeer. Hiermee vormt de PSD2 ook een uitdaging vanuit fiscaal perspectief.

Ook voor de opsporing zal de PSD2 een uitdaging betekenen. Nu al is het volgen van internationale geldstromen arbeidsintensief, complex en tijdrovend en dit zal door de PSD2 toenemen. Uit de opsporingspraktijk blijkt dat criminelen zich bedienen van buitenlandse betaalrekeningen, buitenlandse PSP's en complexe witwasstructuren. Zonder aanvullende mogelijkheden voor de opsporing om (snel) gegevens te kunnen vorderen bij buitenlandse partijen, kan de PSD2 tot grote problemen leiden. Denk hierbij ook nog even aan het voorbeeld van de geautomatiseerde transacties via API's. Uit de opsporingspraktijk blijkt dat de afhandeling van een internationale rechtshulpverzoek soms maanden kan duren. De strafbaarstelling van witwassen verschilt bovendien in de Europese landen, hetgeen voor beperkingen kan zorgen in internationale opsporingsonderzoeken. In sommige gevallen kan de komst van TPP's juist een meerwaarde betekenen voor opsporingsonderzoeken; deze partijen kunnen immers een belangrijke bron van informatie zijn betreffende een onderzoekssubject. Ook kan snel inzage worden verkregen bij welke ASPSP eventueel nog vermogen te vinden is en waar beslag op kan worden gelegd.

PSD2 geldt straks voor alle betalingen van en naar de EU. Dat betekent dat betalingen naar landen buiten de EU onder meer toezicht komen te vallen, aangezien de transacties dienen te voldoen aan Europese regelgeving. Ook leidt PSD2 tot een verdere harmonisering van fraudebestrijding en veiligheid van gegevens. Mogelijk dat dit op termijn ook kansen gaat bieden voor de opsporing.

4. Conclusies en aanbevelingen

4.1 Conclusies

Het Europese betaallandschap zal zich ten gevolge van de PSD2 verder ontwikkelen. Ongetwijfeld zullen de nieuwe betaaldiensten op termijn leiden tot een grotere diversiteit aan (nieuwe) aanbieders van betaalproducten. Op Europees niveau vindt momenteel nog discussie plaats over een aantal elementen van de RTS over SCA en moeten bepaalde artikelen van de PSD2 nog geïmplementeerd worden in nationale wetgeving. Dit maakt het lastig om ten aanzien van de risico's op fraude en witwassen op voorhand eenduidige conclusies te trekken.

Voor grote (internationale) bedrijven biedt de PSD2 kans om, middels een vergunning als PISP, het afrekenen voor producten of diensten onderdeel te maken van de complete gebruikerservaring. Ook AISP's kunnen met het ontwikkelen en aanbieden van innovatieve dienstverlening een interessante rol gaan spelen op de betaalmarkt. Het lijkt aannemelijk dat de PSD2 zal leiden tot een verdere toename van internationale transacties, alsmede het aantal buitenlandse partijen die hun betaaldiensten aanbieden aan Nederlandse klanten.

Ook criminelen zullen zich op enigerlei wijze bedienen van de nieuwe betaaldiensten. Een risico zijn onbetrouwbare en criminele TPP's die als doel hebben frauduleuze betalingen en/of misbruik van gegevens mogelijk te maken. Ook kan de betaalinfrastructuur vals of onbetrouwbaar zijn. *Direct access* vormt hierbij een extra risico. Daarnaast zal de PSD2 een aantal uitdagingen tot gevolg hebben voor wat betreft fraudedetectie. Hoewel geen onderdeel van de PDS2, zal het versnellen van transacties middels *instant payments* de fraudedetectie bovendien verder onder druk zetten. De huidige fraudedetectiesystemen van de ASPSP's dienen te worden aangepast en het is maar de vraag wat de kwaliteit is van de fraudedetectie bij nieuwe, onervaren toetreders tot de betaalmarkt.

PISP's kunnen ook bedoeld of onbedoeld een rol spelen bij het witwassen van crimineel vermogen. Logischerwijs vormen criminele PISP's die zelf SCA organiseren hierbij een groot risico, omdat ze met geautomiseerde API's en/of eigen betaalrekeningen verhullende handelingen kunnen verrichten.

Effectief toezicht lijkt noodzakelijk om fraude en witwassen tegen te gaan. De vraag is echter of de veelheid aan verschillende toezichthouders en de vermoedelijke aanwas van buitenlandse partijen op de Nederlandse markt effectief toezicht mogelijk maken.

De PSD2 biedt echter ook een aantal kansen. Met de komst van TPP's komt er voor opsporingsdiensten meer financiële informatie beschikbaar. Vooral AISP's kunnen in dat kader een belangrijke rol gaan spelen. Daarnaast vallen zowel AISP's als PISP's onder de Wwft, waardoor er een toename zou moeten zijn van het aantal meldingen van ongebruikelijke transacties. Buitenlandse TPP's die Nederlandse klanten bedienen, zullen echter hun meldingen doen in het land van vestiging. Hoewel de informatie-uitwisseling tussen FIU's met de vierde antiwitwasrichtlijn wordt uitgebreid, zal de praktijk moeten uitwijzen in hoeverre de meldketen en de opsporing in Nederland hiervan kunnen profiteren.

Hier staat tegenover dat het betalingsverkeer steeds internationaler en complexer wordt, waardoor het volgen van transacties en het achterhalen van vermogen arbeidsintensief en tijdrovend is. Internationale samenwerking wordt, voor zover dat nog niet het geval was, cruciaal. Onderlinge verschillen tussen landen in de strafbaarstelling van witwassen vormen daarbij een obstakel, maar ook de (trage) afhandeling van rechtshulpverzoeken. Het wordt tijd dat in Europa hieromtrent uniforme afspraken worden gemaakt en voor opsporingsdiensten mogelijkheden worden gecreëerd om tijdig informatie te kunnen verkrijgen bij buitenlandse partijen.

4.2 Aanbevelingen

De PSD2-werkgroep doet de volgende aanbevelingen ter voorkoming en de bestrijding van fraude en witwassen:

- voorlichten van betalingsdienstgebruikers over de veranderingen in betaalmogelijkheden ten gevolge van de PSD2 en de mogelijke risico's die hiermee gemoeid zijn;
- voorlichten van betalingsdienstgebruikers over betaalmogelijkheden die gepaard gaan met een hoog frauderisico en (grote) incidenten hieromtrent;
- stimuleren van publiek-private (internationale) samenwerking tussen aanbieders van *appstores*, (nieuwe) betaaldienstverleners, opsporingsdiensten en toezichthouders met als doel informatie te delen over fraudepatronen, -trends en modus operandi van criminelen om fraude en witwassen te bestrijden;
- ontwikkelen en inrichten van werkprocessen en nieuwe fraude- en witwas-detectiesystemen bij betaaldienstverleners om niet-geautoriseerde en/of frauduleuze transacties te detecteren en blokkeren[57];
- toegang verlenen aan betalingsdienstgebruikers tot een online omgeving met een overzicht van de door hen geautoriseerde TPP's, voorzien van de mogelijkheid om autorisaties (tijdelijk) te kunnen blokkeren;
- actueel houden en voor alle betrokken partijen online (geautomatiseerd) toegankelijk maken van het Europese register met ingeschreven, vergunde betaaldienstverleners;
- nader uitwerken van de *Substance* eis op Europees niveau en/of in nationale wetgeving;
- AISP's onderbrengen in het risicogebaseerd integriteitstoezicht van DNB;
- (internationaal) samenwerken van toezichthouders om de effectiviteit van toezicht te vergroten;
- onderwerpen van betaaldienstverleners aan toezicht tot op transactieniveau om mogelijke witwastransacties te kunnen onderkennen;
- voor Nederlandse opsporingsdiensten en toezichthouders raadpleegbaar maken van administratie van buitenlandse betaaldienstverleners die betrekking heeft op Nederlandse klanten en/of betaalrekeningen op zodanige wijze dat het vorderen van gegevens eenvoudiger wordt en/of internationale rechtshulpverzoeken niet nodig zijn, bijvoorbeeld via een vaste vertegenwoordiger in Nederland;
- voor opsporingsdiensten en toezichthouders mogelijk maken om, ter verbetering van de efficiency en effectiviteit van opsporings- en toezichtactiviteiten, dezelfde technische toegangskanalen (zoals API's) te gebruiken, die betaaldienstverleners ter beschikking staan ten gevolge van de PSD2.

[57] Gezien de grote hoeveelheid gegevens die betrokken partijen met de komst van TPP's uitwisselen, zal hierbij een sterke focus op data analytics komen te liggen.