Risicoanalyse Europese betaalrichtlijn PSD2

Samenvatting voor dummies, door Dorine Stahlie en Niels Ploeger (AMLC)

Inleiding

In het voorjaar van 2018 zal de tweede Europese betaaldienstenrichtlijn (payment service directive, verder: PSD2) in de Nederlandse regelgeving[1] worden geïmplementeerd.[2] Deze richtlijn is een vervolg op PSD1 uit 2007, die tot doel heeft het grensoverschrijdend betaalverkeer makkelijker te maken en de markt heeft opengesteld voor nieuwe betaalinstellingen zoals Adyen en Mollie. Ontwikkelingen in de betaalsector gaan razendsnel en inmiddels is de PSD1 door nieuwe vormen van betaaldienstverlening alweer achterhaald, waardoor nieuwe Europese wetgeving noodzakelijk is. PSD2 heeft vooral tot doel om innovatie te stimuleren.

PSD2 introduceert onder meer twee nieuwe betaaldiensten, te weten de betaalinitiatiedienst (payment initiation service provider, **PISP**) en de rekeninginformatiedienst (account information service provider, **AISP**). Banken worden verplicht om hun infrastructuur te openen voor deze nieuwe dienstverleners; zij moeten de PISP's en AISP's toegang verlenen tot de betaalrekening van hun klanten. Dit brengt kansen maar ook risico's met zich mee. Onder meer op het gebied van fraude en witwassen.

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. Het eerste onderwerp dat in de thematafel is geselecteerd, is PSD2. Vanuit deze thematafel is een gezamenlijk kennisdocument opgesteld waarin de wijzigingen en risico's van PSD2 vanuit Nederlands perspectief in kaart zijn gebracht. Het uitgebreide kennisdocument is wellicht wat lastig leesbaar voor wie niet dagelijks met (new) payment-ontwikkelingen te maken heeft. Deze samenvatting geeft dan ook een aantal hoofdlijnen weer waarbij technische termen zoveel mogelijk zijn omzeild. Deze samenvatting is met name gericht op de risico's van toegang tot rekening door derde partijen.[3]

Het volledige kennisdocument is op te vragen bij het AMLC en te vinden op onze website.[4]

---

[1] Implementatie in Burgerlijk Wetboek en Wet op het financieel toezicht

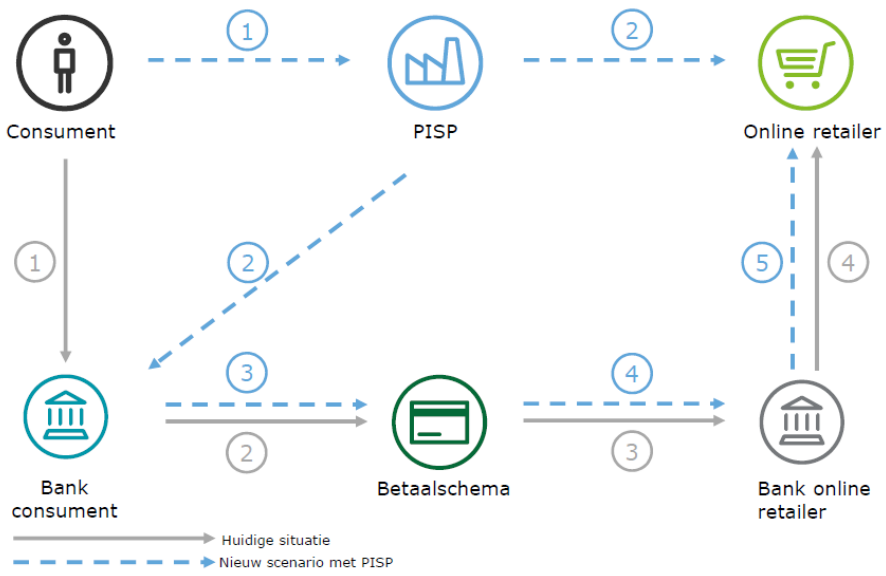
[2] https://www.rijksoverheid.nl/documenten/kamerstukken/2017/09/22/kamerbrief-voortgang-implementatie-herziene-betaaldienstenrichtlijn-psd2

[3] Het uitgebreide kennisdocument *'De tweede Europese betaaldienstenrichtlijn (PSD2) en de risico's op fraude en witwassen'* is opgesteld vanuit een werkgroep met als deelnemers: 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. Deze samenvatting is opgesteld door het AMLC, zonder afstemming met de andere partijen.

[4] https://www.amlc.nl/nl/documenten/

De betaalinitiatiedienst (PISP)

Een PISP kan in opdracht van een gebruiker een betaling verrichten, zoals voor de aankoop van een product in een webwinkel. De gebruiker kan hiertoe een PISP toestemming verlenen voor het verkrijgen van toegang tot zijn betaalrekening bij een *andere* betaaldienstverlener, zoals een bank. 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. Of een grote webshop die niet langer gebruik wil maken van iDEAL, maar een zelf ontwikkeld (en dus goedkoper) alternatief wil aanbieden met een eigen inlogportaal en eigen uiterlijk.



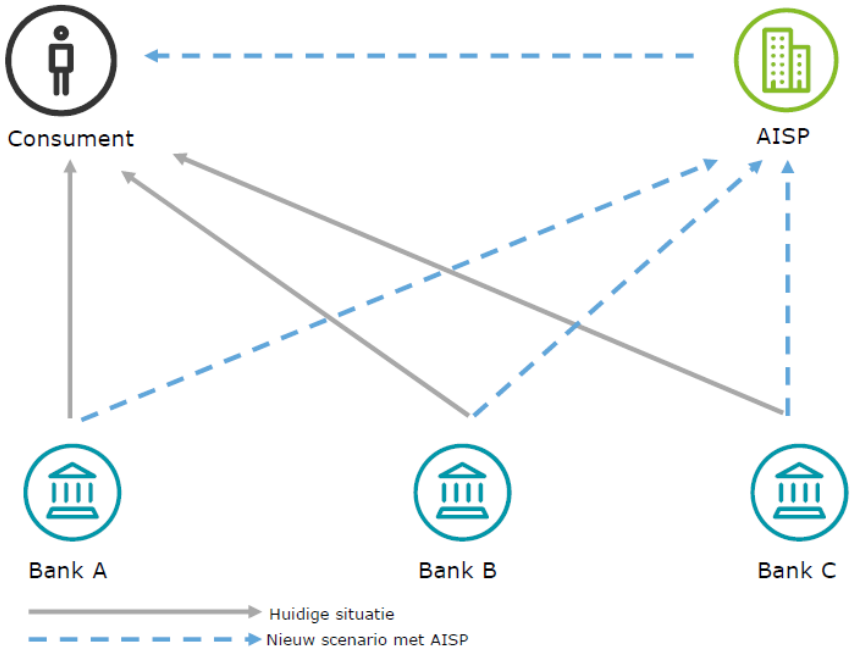
Figuur 1. Betaaldienst PISP schematisch weergegeven.

Een PISP mag niet op enig moment in het bezit komen van de geldmiddelen van de betalingsdienstgebruiker/consument. Ook mogen geen gevoelige betaalgegevens worden opgeslagen. Er is dus geen volledige toegang voor de PISP tot een rekening van een klant bij de bank. Een bank mag de toegang tot de betaalrekening ontzeggen als er een objectief vermoeden is van frauduleuze toegang tot de betaalrekening.

De rekeninginformatiedienst (AISP)

Een AISP kan in opdracht van een gebruiker op een voor de consument overzichtelijke manier informatie verstrekken, afkomstig van een of meerdere betaalrekeningen bij een of meerdere banken. Hiermee kan ieder bedrijf en iedere particulier alle transacties en saldi van al zijn bankrelaties en creditcards verzamelen in één overzicht. Een AISP mag echter geen gevoelige betaalgegevens opvragen; dit zijn gegevens waarmee fraude kan worden gepleegd, waaronder persoonlijke beveiligingsgegevens.

Een voorloper van een AISP is AFAS Personal, een online huishoudboekje waarmee onder meer (grafisch) inzicht kan worden verkregen in uitgaven, en budgetten en begrotingen kunnen worden opgesteld.
Het geven van financieel advies valt overigens niet onder de vergunning van een rekeninginformatiedienst.



Figuur 2. Betaaldienst AISP schematisch weergegeven.

De AISP's verrichten diensten waar de consument uitdrukkelijk toestemming voor geeft en heeft alleen toegang tot de informatie van de door de consument aangewezen betaalrekeningen en de betrokken betalingstransacties. 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.

Toegang tot de rekeninggegevens

Om PISP's en AISP's hun werk te kunnen laten doen, moeten banken hen toegang verlenen tot transactiegegevens, mits de consument daar toestemming voor heeft gegeven. Bij de totstandkoming van de richtlijn en de bijbehorende technische standaard, is er discussie geweest over de vraag hóe banken die toegang moeten gaan verlenen. Er moest gekozen worden tussen enerzijds een door de bank ontworpen digitale toegangspoort waarin de bank bepaalt op welke momenten ze data doorgeven via de poortjes en hoe nieuw of oud die informatie is, en anderzijds een technische mogelijkheid waarbij externe betaaldienstverleners potentieel toegang zouden hebben tot veel meer klantdata die bovendien altijd tot het allerlaatste moment zou zijn bijgewerkt. De Europese Commissie heeft recent

gekozen voor de eerste optie, waarin de banken in de lead zijn[5]. De Europese Raad heeft echter nog tot eind februari 2018 de tijd om aanpassingen te doen.

Overigens geldt voor de toestemming van de consument: hoewel expliciete toestemming voor toegang tot de rekening 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.

Risico's fraude en witwassen

Bij beschrijving van de risico's moet bedacht worden dat:

- op dit moment de interpretatie van de PSD2 en de implementatie daarvan in nationale regelgeving nog niet volledig duidelijk is
- op dit moment nog niet bekend is welke (nieuwe) maatregelen door betaalinstellingen geïntroduceerd zullen worden
- op dit moment nog niet bekend is welk positief effect toezicht zal hebben op het beperken van de risico's
- 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.

Dit gezegd hebbende, ziet de werkgroep o.a. de volgende risico's.

Onbetrouwbare en criminele betaaldienstverleners

De komst van PSD2 zal naar verwachting leiden tot een toename van nieuwe (buitenlandse) betaaldienstverleners en betaalopties op de Nederlandse betaalmarkt.

Aangenomen wordt, dat het merendeel van de aanbieders 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 betaaldienstverleners. Daarnaast kunnen integere betaaldienstverleners misbruikt worden door criminelen, bijvoorbeeld door infectie met *malware*.

Banken worden verplicht om, bij uitdrukkelijke toestemming van de consument, externe betaaldienstverleners toegang te verlenen tot de betaalrekening. De vraag is echter of banken en consumenten de betrouwbaarheid van betaaldienstverleners en de aangeboden betaalinfrastructuur voldoende kunnen beoordelen.

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 transacties *geautomatiseerd* uitvoeren, waarbij meerdere betaalrekeningen bij verschillende banken worden gebruikt (zie figuur 3, situatie A). Een voorbeeld:

Crimineel Jansen met een Nederlandse betaalrekening (A) wil geld overmaken naar crimineel Visser met een Zwitserse betaalrekening (D); dit is een poortwachter die

[5] https://fd.nl/ondernemen/1229812/banken-houden-controle-over-het-nieuwe-betalingsverkeer?utm_source=nieuwsbrief&utm_campaign=fd-ochtendnieuwsbrief&utm_medium=email&utm_content=20171129&s_cid=671

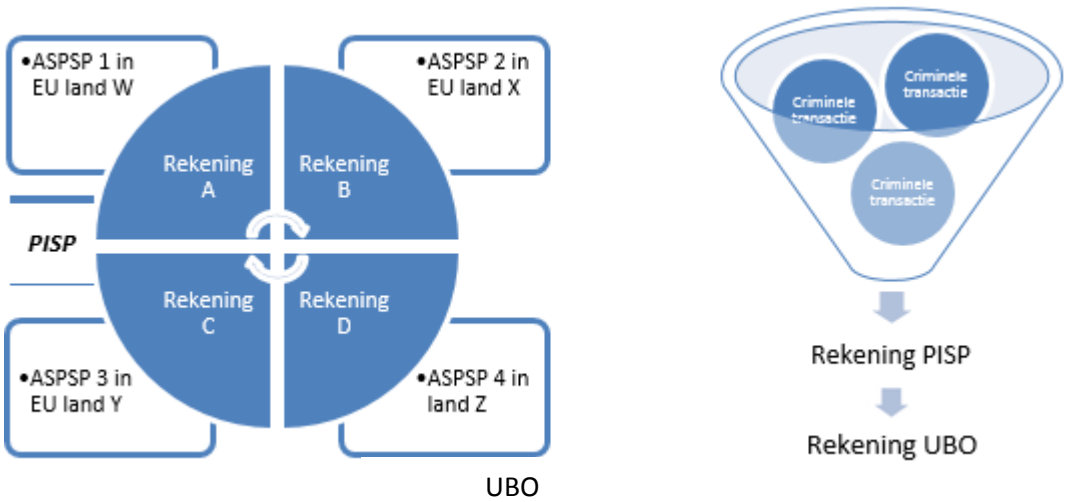
actief is in de bovenwereld. De PISP maakt net als Jansen onderdeel uit van de criminele organisatie, is in Malta gevestigd en heeft aldaar rechtmatig een licentie verkregen om betalingen te kunnen initiëren. De PISP is via een technische verbinding aangesloten op alle banken die in dit voorbeeld worden genoemd.

De PISP stuurt via de technische verbinding een betalingsopdracht naar de bank van Jansen, waarbij aangegeven wordt dat de klant zich bij de PISP heeft geauthentiseerd. Hierbij wordt niet de betaalrekening van Visser opgegeven, maar een betaalrekening (B) bij een Italiaanse bank op naam van een Italiaans bedrijf, dat ook onderdeel uitmaakt van de criminele organisatie.

Na ontvangst van de gelden op de Italiaanse betaalrekening, stuurt de PISP een betalingsopdracht naar de Italiaanse bank om hetzelfde bedrag over te maken naar een Belgische betaalrekening (C) op naam van een Belgisch bedrijf, dat ook onderdeel uitmaakt van de criminele organisatie.

Vervolgens stuurt de PISP eenzelfde opdracht naar de Belgische bank om het geld over te maken naar de Zwitserse betaalrekening van Jansen, de uiteindelijke belanghebbende.

In dit voorbeeld worden 'slechts' twee tussenrekeningen gebruikt, maar in de praktijk zouden dit er veel meer kunnen zijn, zonder dat dit al teveel moeite kost. Aangenomen wordt, dat transacties die via een PISP lopen, door de betreffende banken anders worden gemonitord dan handmatige overboekingen. 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.



Figuur 3. Geautomatiseerde betalingen via betaalrekeningen (situatie A) & verhullen UBO door PISP (situatie B). Een ASPSP is de financiële instelling die betaalrekeningen beheert, zoals een bank. Een UBO is een uiteindelijk belanghebbende.

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 prepaid kaarten aangesloten op het MasterCard- of Visa netwerk, 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 niet in het bezit mag komen van de geldmiddelen van de consument. De bank 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 bank kan vermoedelijk niet vaststellen dat het een eigen betaalrekening van de PISP betreft en zal daarom de transactie gewoon uitvoeren. In dit voorbeeld werken de criminele onderneming en de criminele PISP dus samen.

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.

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*[6] in het buitenland aan te wenden voor betalingen in Nederland. PISP's met complexe internationale geldstromen, 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 niet alle ongebruikelijke transacties onderkend en/of gemeld worden.

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 externe betaaldienstverleners ten behoeve van het vaststellen van risico-indicatoren kan voor banken 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 het geval dat voor een bank niet geheel duidelijk is wat voor soort dienstverlening een PISP aanbiedt, kan dit mogelijk voor problemen zorgen.

[6] Vermogen dat niet fiscaal is aangegeven en/of van criminele herkomst is en dat verborgen wordt gehouden voor de overheid.

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 betaaldienstverleners.

Tot slot

In het uitgebreidere kennisdocument worden behalve relevante wettelijke bepalingen ook de gevolgen voor het toezicht en de risico's op fraude beschreven. Voor de opsporing zal de PSD2 enerzijds een uitdaging betekenen. Nu al is het volgen van internationale geldstromen arbeidsintensief, complex en tijdrovend en dit zal door de PSD2 toenemen. Maar de toetreding van externe betaaldienstverleners, AISP's in het bijzonder, kunnen ook voordelen 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.

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.