Autoriteit
Consument & Markt

Openbaar

Besluit

Openbaar besluit niet (verder) behandelen verzoek OK IT tot handhaving Mededingingswet

Ons kenmerk : ACM/UIT/551524
Zaaknummer : ACM/20/042562
Datum :

Muzenstraat 41
2511 WB Den Haag
www.acm.nl
070 722 20 00

Besluit

Besluit van de Autoriteit Consument en Markt tot het niet in behandeling nemen van het verzoek van OK IT BV tot handhaving van de Mededingingswet

Ons kenmerk : ACM/UIT/545588
Zaaknummer : ACM/20/042562
Datum : 16 maart 2021

Inhoudsopgave

1 Inleiding en Samenvatting 3

2 Verloop van de procedure 4

3 Verzoeker 4
3.1 Inleiding 4
3.2 OK IT B.V. 4
3.3 OK app (slimme mobiele portemonnee) 5

4 Betrokkenen 6
4.1 Inleiding 6
4.2 ING, Rabobank, Volksbank en ABNAMRO 6
4.3 Payconiq Netherlands B.V. 6
4.4 Payconiq app (omnichannel betaaloplossing) 6

5 Inhoud handhavingsverzoek 7

6 Toetsingskader 9

7 Context 9
7.1 Mobiel contactloos betalen 9
7.2 Revised Payment Services Directive (PSD2) 10
7.3 Vergunningplicht 12
7.4 Sterke Cliënt Authenticatie 13
7.5 De obstakelvrije klantreis 14

8 Beoordeling 16
8.1 Inleiding 16
8.2 PSD2 in het initieel onderzoek 16
8.3 Geen vergunning voor betaalinitiatiediensten 16
8.4 Sterke Cliënt Authenticatie via *redirection* 17
8.5 Conclusie beoordeling 18

9 Besluit 18

1 Inleiding en Samenvatting

1. OK IT B.V. heeft een handhavingsverzoek ingediend bij de Autoriteit Consument en Markt (ACM) dat is gericht tegen ING Bank N.V., Coöperatieve Rabobank U.A., De Volksbank N.V. en ABN AMRO N.V. (hierna gezamenlijk: de banken). Volgens het handhavingsverzoek zouden de banken weigeren toegang te verlenen tot hun betalingssystemen en de betaalrekeningen van hun betaalrekeninghouders aan OK IT B.V. OK IT B.V. wil rechtstreekse toegang verkrijgen tot de betaalrekeningen van haar gebruikers voor het verlenen van betalingsinitiatiediensten via de OK app, die (ten minste) gelijk is aan de toegang die de Payconiq app van enkele banken heeft. Volgens het handhavingsverzoek misbruiken de banken hun economische machtspositie door de door OK IT B.V. gewenste toegang te weigeren tot hun betalingssystemen en de betaalrekeningen. Daarnaast zouden de banken, met name door de samenwerking met en in Payconiq Netherlands B.V., onderling een afspraak hebben gemaakt met als doel of gevolg de mededinging met derde partijen zoals OK IT B.V. te beperken door de toegang tot hun betalingssystemen te belemmeren.

2. De ACM concludeert in dit besluit het verzoek tot handhaving van de Mededingingswet niet (verder) in behandeling te nemen. Tot die conclusie komt de ACM nadat eerst is nagegaan of doeltreffend en doelmatig optreden mogelijk is. Aan de uitvoering van een volledig handhavingsonderzoek komt de ACM niet toe.

3. Het verzoek tot handhaving van de Mededingingswet is ingediend door OK IT B.V. tegen de achtergrond van de PSD2-regelgeving. De PSD2-regelgeving heeft meerdere doelstellingen, waaronder het verhogen van de veiligheid in het betalingsverkeer en het bevorderen van de concurrentie tussen innovatieve betaaloplossingen, iets wat de ACM ondersteunt. OK IT B.V. wenst toegang tot de betalingssystemen en betaalrekeningen van de banken te verkrijgen ten behoeve van PSD2-betalingsinitiatiediensten die zij met de OK app verleent c.q. verlenen wil. De PSD2-regelgeving, onder meer geïmplementeerd in de Wet op het financieel toezicht, bepaalt onder welke voorwaarden en op welke wijze de PSD2-betaalinitatiedienstverleners toegang tot de betalingssystemen en betaalrekeningen(informatie) bij de banken kunnen krijgen.

4. In het initieel onderzoek stelt de ACM de volgende twee punten vast ten aanzien van die PSD2-regelgeving. Op de eerste plaats is gebleken dat OK IT B.V. niet de vereiste vergunning van De Nederlandsche Bank heeft om betaalinitiatiediensten in het kader van PSD2 uit te voeren. Op de tweede plaats constateert de ACM dat OK IT er ten onrechte vanuit gaat dat de PSD2-regels eraan in de weg staan dat de banken de toegang via de mogelijkheid van *redirection* laten plaatsvinden. De sterke cliënt authenticatie (SCA) die de PSD2-regels voorschrijven, mag wel via *redirection* verlopen. Uit het initieel onderzoek van de ACM blijkt dan ook dat doeltreffend en doelmatig optreden niet mogelijk is. Immers, bij toepassing van de mededingingsregels moet de ACM rekening houden met het regelgevend kader van PSD2, waaronder de vergunningplicht en de voorwaarden inzake de sterke cliënt authenticatie.

5. In dit besluit zet de ACM uiteen dat zij het handhavingsverzoek niet verder behandelt aangezien de ACM dit niet doelmatig en/of niet doeltreffend acht.

2 Verloop van de procedure

6. Op 7 oktober 2020 ontving de ACM een verzoek, namens OK IT B.V., om handhaving van de mededingingswet.[1]

7. Bij brief van 15 oktober 2020 bevestigde de ACM de ontvangst van het handhavingsverzoek.[2]

8. Eind november 2020 deelde de ACM telefonisch aan de gemachtigde van OK IT haar voorlopige mening over het handhavingsverzoek mede. In afwachting van een reactie van de gemachtigde werd afgesproken de 8-weken termijn uit artikel 4:13 Awb op te schorten.[3]

9. Op 11 januari 2021 liet de gemachtigde, namens OK IT B.V., in reactie op de voorlopige mening van de ACM weten het handhavingsverzoek te willen handhaven.[4] Vervolgens heeft de ACM bij brief d.d.14 januari 2021 aan de gemachtigde medegedeeld de termijn voor afhandeling van het handhavingsverzoek te verlengen tot en met 1 april 2021.[5]

10. De ACM heeft enkele malen contact gehad met De Nederlandsche Bank en op 25 februari 2021 en 8 maart 2021 per email gecorrespondeerd over het concept van dit besluit.[6]

3 Verzoeker

3.1 Inleiding

11. In dit hoofdstuk beschrijft de ACM kort de onderneming OK IT en haar product, de OK app.

3.2 OK IT B.V.

12. OK IT B.V. (hierna: OK IT) is een besloten vennootschap naar Nederlands recht, statutair gevestigd in Amsterdam. OK IT heeft volgens haar huidige statuten onder meer als doel:
"het doen ontwikkelen en exploiteren van digitale transactie- en interactiesystemen en het ontwikkelen en verlenen van transactie-, interactie-, data-, marketing- en adviesdiensten".[7]

13. OK IT is opgericht in 2015 en werkt sindsdien samen met Intersolve EGI B.V. in de Stichting Derdengelden OK IT, voorheen de Stichting Derdengelden Intersolve Trust.[8] OK IT heeft, volgens het handhavingsverzoek, de ambitie om uit te groeien tot een aanbieder van een geïntegreerde, slimme

[1] Zie de email en brief d.d. 7 oktober 2020 van de gemachtigde met kenmerk ACM/IN/565614 en ACM/IN544871.
[2] Zie de brief d.d. 15 oktober 2020 met kenmerk ACM/UIT/542856.
[3] Zie het gespreksverslag d.d. 1 december 2020 met kenmerk ACM/INT/415587 en de email d.d. 30 november 2020 met kenmerk ACM/UIT/545235.
[4] Zie de email d.d. 11 januari 2021 van de gemachtigde met kenmerk ACM/IN/572518.
[5] Zie de brief d.d. 14 januari 2021 met kenmerk ACM/UIT/547285.
[6] Zie de email d.d. 24 februari 2021 met kenmerk ACM/UIT/549653, de email d.d. 25 februari 2021 met kenmerk ACM/en de emails d.d. 8 maart 2021met kenmerk ACM/UIT/550257 en met kenmerk ACM/ IN/592139 en ACM/UIT/550259.
[7] Zie akte van oprichting en statutenwijziging OK IT, ACM/INT/419049.
[8] Zie Statutenwijziging 2015 Stichting Derdengelden Intersolve Trust, ACM/INT/419657, het bedijfsprofiel Stichting Derdengelden OK IT, ACM/INT/419561 en het handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, voetnoten 5 en 72.

mobiele betaaloplossing, door middel van de OK app.[9] De betaalapp van OK IT beoogt de fysieke portemonnee te vervangen door een *mobile smart wallet*.

3.3 OK app (slimme mobiele portemonnee)

14. OK IT wenst met haar diensten consumenten en zakelijk eindgebruikers de mogelijkheid te bieden alle online en offline betalingen en betalingsgerelateerde handelingen onder te brengen in één mobiele applicatie (de OK app). De OK app vervangt in dat geval de fysieke betaalpassen, kortingsvouchers, klantenkaarten, kassabonnetjes, tickets en dergelijke door QR-codes, aldus het handhavingsverzoek. De gebruiker hoeft in de winkel alleen de code te scannen in de OK app, waarna de betaling, eventuele kortingen, toepasselijke spaaracties en dergelijke allemaal automatisch in de OK app worden verwerkt.[10]

15. Voor de betalingsfunctie uit de OK app maakte OK IT voorheen gebruik van [vertrouwelijk] . OK IT licht dit als volgt toe. Bij [vertrouwelijk] . Voorts werd hierbij per betaling [vertrouwelijk] door OK IT. OK IT betaalde [vertrouwelijk] .[11] Deze werkwijze gaf OK IT [vertrouwelijk] , kon OK [vertrouwelijk] , leverde OK IT mogelijk [vertrouwelijk] en gaf [vertrouwelijk] .[12]

16. Gelet op de in het vorige randnummer omschreven nadelen van [vertrouwelijk] geeft OK IT de voorkeur aan [vertrouwelijk] , volgens OK IT, vindt [vertrouwelijk] .[13] Het [vertrouwelijk] .[14] OK IT wenst [vertrouwelijk] dat de transactie(s) volledig plaatsvindt(en) binnen de OK IT-omgeving en niet dat de gebruiker, doordat de banken de authenticatie zelf (laten) uitvoeren, naar of langs de (virtuele) bankomgeving wordt geleid (*redirection*). De gebruiker zou in vier stappen in de OK app het betaalproces, inclusief eigen authenticatieprocedure, doorlopen.[15] Omdat OK IT geen rechtstreekse koppeling tussen de OK app en de betaalsystemen of de betaalrekeningen van de banken kan krijgen, heeft OK IT een tijd lang [vertrouwelijk] .[16]

[9] Zie het handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, randnummer 7.
[10] Zie het handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, randnummer 10.
[11] Zie het handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, randnummer 11.
[12] Zie het handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, randnummer 13.
[13] Het is niet zeker of alle [vertrouwelijk] opdrachten als *instant payment* worden verwerkt. Banken doen dat (vrijwillig) voor boekingen die via internet- en mobiel bankieren worden aangeboden. Welke andere stromen instant worden verwerkt, bepalen de banken zelf.
[14] Zie het handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, randnummer 14.
[15] Zie het handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, randnummers 15, 16, 17, 27, 28 en 30.
[16] Zie het handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, randnummer 36.

4 Betrokkenen

4.1 Inleiding

17. In dit hoofdstuk geeft de ACM een beschrijving van de vier banken tegen welke het handhavingsverzoek is gericht, alsmede van het samenwerkingsverband Payconiq Netherlands B.V. en de gezamenlijke betaaldienst Payconiq.

4.2 ING, Rabobank, Volksbank en ABNAMRO

18. ING Bank N.V., opgericht in 1927, is statutair gevestigd te Amsterdam. Eén van de doelen volgens haar statuten is het uitoefenen van het bankbedrijf in de ruimste zin.

19. Coöperatieve Rabobank U.A., opgericht in 1970, is statutair gevestigd te Amsterdam. Eén van de doelen volgens haar statuten is het uitoefenen van het bankbedrijf, het verlenen van andere financiële diensten en het in dat kader sluiten van overeenkomsten met haar leden.

20. De Volksbank N.V., opgericht in 1990, is statutair gevestigd te Utrecht. Eén van de doelen volgens haar statuten is het uitoefenen van het bedrijf van kredietinstelling in de ruimste zin.

21. ABN AMRO N.V., opgericht in 2009, is statutair gevestigd te Amsterdam. Eén van de doelen volgens haar statuten is het zijn van kredietinstelling.

4.3 Payconiq Netherlands B.V.

22. Payconiq Netherlands B.V. (hierna: Payconiq) is een besloten vennootschap naar Nederlands recht, statutair gevestigd in Amsterdam. Payconiq heeft statutair als doel, onder andere:
“het op de markt brengen van de betaaloplossing ‘Payconiq’ in Nederland als een omnichannel betaaloplossing voor zowel consumenten als handelaren”.

23. Payconiq is op 1 juni 2018 opgericht door ING, Rabobank en de Volksbank.[17] Volgens de huidige statuten houden ING en Rabobank ieder 45% en de Volksbank 10% van de aandelen in Payconiq. Payconiq is de gezamenlijke onderneming en het samenwerkingsverband van deze drie banken in Nederland voor online, in winkels en onderling mobiel betalen.

4.4 Payconiq app (omnichannel betaaloplossing)

24. Voorafgaand aan de formele oprichting in 2018 had ING in 2015 Payconiq reeds als mobiele betaaldienst geïntroduceerd. In 2017 werd het een gezamenlijke betaaldienst van ING, Rabobank, Volksbank en ABNAMRO. In 2018 is ABNAMRO uit de samenwerking gestapt om zich te richten op haar eigen betaalapp Tikkie. Met de Payconiq-app kunnen gebruikers online, in winkels en onderling betalen. Payconiq is behalve in Nederland, actief in Duitsland, België en Luxemburg (waar ook andere banken meedoen).[18] In 2019 verkreeg Payconiq International S.A., gevestigd in Luxemburg,

[17] Zie Akte van Oprichting. In het geval van Rabobank gaat het om Rabo Frontier Ventures B.V., opgericht in 2017 door de Rabobank.
[18] Zie interne email d.d. 24 februari 2021 met kenmerk ACM/INT/420564 met pdf’s van nieuwsberichten over Payconiq van ecommercenews.nl, emerce.nl en www.wikipedia.org/wiki/Payconiq.

een vergunning voor betaalinitiatiediensten (in de EU).[19]

25. Via de app van Payconiq op bijvoorbeeld een smartphone kunnen consumenten offline (in de winkel) en ook online (in webshops) betalingen doen. Een transactie wordt uitgevoerd nadat de consument een QR-code scant op een betaalterminal, kassascherm, kassabon, telefoon of iPad, QR-sticker of online. De QR-code van Payconiq zal (binnenkort) ook te scannen zijn via de eigen app van diverse banken, waaronder de ING en Rabobank. Payconiq richt zich voorts op het ontwikkelen van additionele diensten en functies, waaronder loyalty-programma's zodat via de Payconiq-app punten kunnen worden gespaard.[20]

26. Het betaalproces via de Payconiq app verloopt van het koppelen van de bankrekening aan de app en vervolgens het scannen van de QR code, naar het intoetsen van de pincode en tot slot het akkoord van de betaling.

5 Inhoud handhavingsverzoek

27. Volgens het handhavingsverzoek zouden de banken weigeren (via een API)[21] rechtstreekse toegang te verlenen tot hun betalingssystemen en de betaalrekeningen aan OK IT. OK IT wenst die toegang voor de OK app te verkrijgen ten behoeve van de PSD2-betalingsinitiatiediensten die zij [vertrouwelijk] wil verlenen.[22] Uit het handhavingsverzoek blijkt dat OK IT eind 2017 schriftelijk, met een beroep op de PSD2-regels, aan de banken gevraagd heeft om toegang, dat er veelvuldig contact is geweest met de banken eind 2017 en begin 2018 en dat de banken hebben aangegeven te wachten tot het (formeel) van kracht worden van de PSD2-regels in Nederland.[23]

28. Uit het handhavingsverzoek volgt dat OK IT, zelf of via de samenwerking met Intersolve EGI B.V., niet beschikt over een vergunning voor betalingsinitiatiediensten. Daarover merkt OK IT op dat [vertrouwelijk] . OK IT ziet de mogelijkheid van toegang tot de betalingssystemen en de betaalrekeningen van de banken onder de PSD2-regels hierdoor geblokkeerd.[24]

29. Vanaf medio 2018 is er nauwelijks nog contact geweest tussen OK IT en de banken omdat, volgens het handhavingsverzoek, de banken aan OK IT duidelijk hadden gemaakt dat contact alleen zinvol was wanneer OK IT zich kon beroepen op PSD2-verplichtingen voor de banken. Volgens OK IT is het zonder vergunning voor betalingsinitiatiediensten niet mogelijk om, [vertrouwelijk] door middel van een rechtstreekse koppeling toegang te krijgen tot de betalingssystemen en betaalrekeningen van de

[19] Zie interne email d.d. 24 februari 2021met kenmerk ACM/INT/420567 met nieuwsbericht over vergunning Payconiq (https://www.payconiq.nl/2019/09/10/payconiq-international-krijgt-pis-licentie-voor-betalingen-in-heel-europa/).
[20] Zie de website van Payconiq, oa: https://www.payconiq.nl/qr-betaaloplossing/ , https://www.payconiq.nl/kassasysteem en https://www.payconiq.nl/omnichannel .
[21] *Application Programming Interface.*
[22] Zie het handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, randnummer 149.
[23] Zie het handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, randnummers 24, 25, 26 en 32 alsmede bijlagen 1, 2, 3 en 10 bij het handhavingsverzoek. De PSD2-regels zijn per 14 september 2019 in Nederland van kracht.
[24] Zie het handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, randnummers 33, 35 en 117. Overigens beschikt Intersolve Payments B.V., die als elektronische geldinstelling in het register van DNB staat, wel over een vergunning voor betaalinitiatiediensten (en rekeninginformatiediensten).

banken.[25]

30. OK IT voert in het handhavingsverzoek aan dat een betalingsinitiatiedienstverlener in de zin en op grond van de PSD2-regels (via een API) directe toegang tot de betaalsystemen of de betaalrekeningen van de banken dient te krijgen. De kern van het geschil met de banken, aldus het handhavingsverzoek, is de vraag of bij de toegangsverlening de SCA (Sterke Cliënt Authenticatie) alleen door de banken mag worden uitgevoerd of ook door betalingsinitiatie-dienstverleners.[26] OK IT meent, onder verwijzing naar de PSD2-regels, dat zij zelf, wanneer zij (vergunninghoudend) betalingsinitiatiedienstverlener zou zijn, de SCA mag uitvoeren en dat de banken niet mogen volstaan met het beschikbaar maken van een *redirect* voor de SCA.[27] Bovendien stelt OK IT daarbij aanspraak te kunnen maken op dezelfde, niet-*redirect*, SCA-mogelijkheid voor de toegang (via een API) die de banken aan Payconiq beschikbaar hebben gesteld.[28]

31. Naast de PSD2-regels zijn, aldus het handhavingsverzoek, de mededingingsregels zoals neergelegd in artikel 6 en 24 Mededingingswet en artikel 101 en 102 Verdrag betreffende de Werking van de Europese Unie (VWEU) toepasselijk. De weigering toegang te verlenen tot hun betalingssystemen en de betaalrekeningen door de banken is, volgens het handhavingsverzoek, een overtreding van die mededingingsregels. De door OK IT voorgestane wijze van uitleg van de PSD2-regels is hierbij, volgens het handhavingsverzoek, van belang.[29]

32. OK IT betoogt dat de banken hun economische machtspositie misbruiken door toegang te weigeren tot hun betalingssystemen en de betaalrekeningen. Daarnaast zouden de banken door de samenwerking met en in Payconiq Netherlands B.V. onderling een afspraak hebben gemaakt met als doel of gevolg de mededinging met fintechs als OK IT te beperken. OK IT betitelt het gedrag van de banken grofweg als bevoordeling van de eigen betaalapp(s) ten opzichte van de OK app en uitsluiting of afscherming van de OK app van de markt door de toegang tot de betalingssystemen van de banken te belemmeren.[30]

33. Volgens het handhavingsverzoek is OK IT niet in staat effectief te concurreren met Payconiq. De Payconiq app maakt gebruik van een rechtstreekse koppeling met de banken middels een daartoe ontwikkelde API. Daarentegen verschaffen de banken aan OK IT een *redirect* naar de bankomgeving voor het uitvoeren van de SCA (Sterke Cliënt Authenticatie). De gebruiker blijft bij de *redirect* niet in de visuele en virtuele omgeving van OK IT.[31]

---

[25] Zie het handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, randnummers 32 en 34.
[26] Zie het handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, randnummers 27, 118 en 119.
[27] Zie het handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, randnummers 120 – 148.
[28] Zie het handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, randnummers 105, 106 en 144-148.
[29] Zie het handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, randnummers 153 en 154 alsmede 35, 117 en 120.
[30] Zie het handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, randnummers 4, 37, 38, 39, 86, 87, 95, 107, 112 en 116.
[31] Zie het handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, randnummers 16, 17, 20, 21, 28, 30, 31 en 138.

6 Toetsingskader

34. Voor een goed begrip van de beoordeling van het handhavingsverzoek, meer in het bijzonder de doeltreffendheid en doelmatigheid van de afhandeling ervan, is het hieronder beschreven toetsingskader relevant. Dit hoofdstuk bespreekt dit door in te gaan op het prioriteringsbeleid van de ACM.

35. Het prioriteringsbeleid dat de ACM hanteert, is gepubliceerd op 18 maart 2019 in de Staatscourant.[32] Het prioriteringsbeleid van de ACM gaat over de vraag of de ACM een volledig handhavingsonderzoek start en uitvoert. Voordat een volledig handhavingsonderzoek wordt gestart, voert de ACM eerst een initieel onderzoek uit. De ACM hanteert drie criteria op basis waarvan zij verzoeken om handhaving over mogelijke overtredingen van de Mededingingswet beoordeelt.

36. Het prioriteringsbeleid is geen optelsom en op basis van een lage(re) score bij één criterium, kan de ACM reeds concluderen dat een volledig handhavingsonderzoek niet is aangewezen. Eén van de criteria uit het prioriteringsbeleid betreft de vraag in hoeverre de ACM in staat is om doeltreffend en doelmatig op te treden.

37. Bij doeltreffendheid gaat het, volgens het prioriteringsbeleid, om de inschatting of met de inzet van een geschikt handhavingsinstrument op korte termijn een gewenste situatie kan worden bereikt of in voldoende mate kan worden benaderd.

38. Bij doelmatigheid gaat het om een kosten-batenanalyse; de afweging of de uitvoering van het handhavingsonderzoek mogelijk en opportuun is met de beschikbare menskracht en de toegekende financiële middelen, mede gelet op de verdeling daarvan tussen en binnen de toezichtstaken van de ACM.

7 Context

39. Dit hoofdstuk gaat met name in op de PSD2-regels. Daarbij komen aan bod: de vergunningplicht, de Sterke Cliënt Authenticatie en de obstakelvrije klantreis. Allereerst staat de ACM kort stil bij het mobiel contactloos betalen.

7.1 Mobiel contactloos betalen

40. De OK app en Payconiq app maken allebei gebruik van QR codes. Hiermee kan onderling, op afstand en ook op locatie, zoals in (fysieke) winkels, de horeca, bij benzinestations of in het openbaar vervoer, worden betaald. Terzake van de zogeheten toonbankbetalingen, dus op locatie, komen betalingen met fysieke bankpassen (pinpassen) het meest voor in Nederland, waarvan het overgrote deel contactloos. Het aandeel contactloos betalen met een smartphone, sieraad of horloge

[32] Zie 'Prioritering van handhavingsonderzoeken door de Autoriteit Consument en Markt', Staatscourant nr 14564, 18 maart 2016.

(*wearables*) neemt toe.[33] Hiervoor genoemde en vergelijkbare functies voor contactloos mobiel betalen vallen onder het begrip 'mobiele portemonnee' (*mobile wallet* of *e-wallet*).

41. Onderzoek uit 2020 wijst erop dat *e-wallets* die zijn gebaseerd op de Near Field Communication (NFC)-chip technologie zoals diverse bankieren-apps of Apple Pay sneller worden geaccepteerd dan *e-wallets* gebaseerd op QR-codes. Dit is omdat de consument het betaalgemak van betalingen met de NFC-chip hoger inschat.[34] Alhoewel mobiele contactloze toonbankbetalingen met QR codes niet de voorkeur hebben van consumenten en winkeliers in Nederland, zijn in het algemeen nieuwe manieren van contactloze toonbankbetalingen groeiende en in ontwikkeling.[35] De technologische ontwikkelingen zien ook op de authenticatie (en autorisatie) tijdens de betaaltransactie of het betaalproces.[36]

7.2 Revised Payment Services Directive (PSD2)

42. De Revised Payment Services Directive (PSD2) is de herziene versie van de Payment Services Directive uit 2007.[37] PSD2 heeft verschillende doelstellingen, waaronder het bevorderen van de concurrentie op de Europese betaalmarkt, het stimuleren en faciliteren van innovaties in het betalingsverkeer, het vergroten van de veiligheid van het betalingsverkeer en de bescherming van deelnemers aan het betalingsverkeer.

43. In Nederland is deze herziene richtlijn onder andere opgenomen in de Wet op het financieel toezicht (Wft), de bij deze wet behorende lagere regelgeving[38] en in titel 7B van Boek 7 van het Burgerlijk Wetboek (BW)[39]. Dat is gedaan via de Implementatiewet herziene richtlijn betaaldiensten[40] en het Implementatiebesluit herziene richtlijn betaaldiensten[41]. De Implementatiewet en het Implementatiebesluit zijn van kracht sinds 14 september 2019.[42]

---

[33] Zie interne email d.d. 24 februari 2021 met kenmerk ACM/INT/420569 met factsheets betalingsverkeer 2019 en 2020 van Betaalvereniging Nederland. Zie ook Enqueteonderzoek "Betaalgedrag van consumenten en winkeliers", september 2020, PwC, blz 13: 88% van de respondenten in het onderzoek heeft een betaal app van de eigen bank op de smartphone.

[34] Zie Rapportage 'Big Techs in het betalingsverkeer', 16 november 2020, ACM, blz 3, 12 en 13 en zie ook blz 15 t/m 20.

[35] Zie Enqueteonderzoek "Betaalgedrag van consumenten en winkeliers", september 2020, PwC, blz 17, 23, 24, 25, 32, 33, 34, 35, 42, 43, 72, 73, 74, 78, 79, 80, 82 en 83. Zie voorts interne email d.d. 24 februari 2021 met kenmerk ACM/INT/420571: Trouw, 31 juli 2019, " Waarom pinnen met je pas als het met je horloge kan?".

[36] Zie bijvoorbeeld ook https://findbiometrics.com/applications/financial-biometrics/ en https://zwipe.com/ .

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

[38] Zoals het Besluit prudentiële regels Wft ('Bpr Wft'), het Besluit Markttoegang financiële ondernemingen Wft ('BMfo Wft') en het Besluit Gedragstoezicht financiële ondernemingen Wft ('BGfo Wft').

[39] Titel 7B ('Betalingstransactie') van Boek 7 BW is ingevoerd bij wet van 15 oktober 2009, Staatsblad 2009, 436 (Implementatiewet PSD1) en is in werking getreden op 1 november 2009.

[40] Wet van 5 december 2018 tot wijziging van de Wet op het financieel toezicht, de Wet bekostiging financieel toezicht, het Burgerlijk Wetboek en de Wet handhaving consumentenbescherming ter implementatie van richtlijn nr. 2015/2366/EU van het Europees Parlement en de Raad, Staatsblad 2018, 503.

[41] Besluit van 8 februari 2019 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. Staatsblad 2019, 59.

[42] Besluit van 8 februari 2019 tot vaststelling van het tijdstip van inwerkingtreding van de Implementatiewet herziene richtlijn betaaldiensten en het Implementatiebesluit herziene richtlijn betaaldiensten, Staatsblad 2019, 60.

44. In Nederland zijn verschillende toezichthouders aangewezen om toezicht te houden op de naleving van PSD2. De Nederlandsche Bank ('DNB'), de Autoriteit Financiële Markten ('AFM'), de Autoriteit Persoonsgegevens ('AP') en de ACM zijn ieder verantwoordelijk voor een eigen onderdeel van het toezicht. Zo is DNB belast met het prudentiële toezicht op betaaldienstverleners (artikel 3:17 Wft). Zij verleent vergunningen aan betaaldienstverleners (banken, betaalinstellingen en elektronischgeldinstellingen). Verder ziet DNB toe op (onder meer) de financiële positie van betaaldienstverleners, de veilige toegang tot betaalrekeningen, de beheersing van risico's en de authenticatie (de wijze waarop de betaalrekeninghouder zich identificeert en toestemming geeft tot toegang tot de betaalrekening). De verantwoordelijkheid voor het gedragstoezicht berust bij de AFM (informatieverstrekking van betaaldienstverleners en hoe zij omgaan met hun klanten). De AP ziet toe op de verwerking van persoonsgegevens. Het toezicht op de toegang tot betalingssystemen en betaalrekeningdiensten uit hoofde van PSD2 ligt, naast het mededingingstoezicht, bij de ACM[43].

45. PSD2 is aangevuld met diverse richtsnoeren (*guidelines*) en technische reguleringsnormen (*Regulatory Technical Standards* (RTS)), opgesteld door de Europese Banken Autoriteit (*European Banking Authority* (EBA)). Deze omvatten onder andere de *RTS on Strong Customer Authentication and Common and Secure Communication* (RTS on SCA & CSC).[44] De genoemde RTS zijn in een gedelegeerde verordening neergelegd die vanaf 14 september 2019 moet worden toegepast. De Gedelegeerde Verordening bevat technische reguleringsnormen inzake de toegang via het internet van betaaldienstgebruikers en (derde-) betaaldienstverleners tot de bij een rekeninghoudende betaaldienstverlener (lees: bank) bestaande betaalrekening(en).[45]

46. De EBA geeft ook zogeheten "*Opinions*" waarin zij uiteenzet hoe de regels uit PSD2 moeten worden uitgelegd en toegepast. De bevoegdheid van de EBA om deze *Opinions* te geven is gebaseerd op artikel 29(1)(a) van Verordening (EU) 1093/2010 als onderdeel van de doelstelling van de EBA om een actieve rol te spelen in het bouwen aan een uniforme toezicht cultuur en consistente toezichtspraktijken binnen de EU. *Opinions* van de EBA zijn gericht aan de nationale toezichthouders, zoals DNB, op het gebied van PSD2. De *Opinions* zijn niet bindend voor de toezichthouders, maar zij worden wel geacht zich in het kader van de convergentie van het toezicht in de EU aan de *Opinions* te houden.

47. Een belangrijke vernieuwing uit PSD2 is de introductie van twee nieuwe (digitale) betaaldiensten waar rekeninghouders gebruik van kunnen maken: betaalinitiatiediensten[46] en rekeninginformatiediensten[47].

---

[43] Artikelen 1:25a, 5:88 en 5:88a Wft en artikelen 35 en 36 PSD2.

[44] De genoemde RTS zijn een gedelegeerde handeling als bedoeld in artikel 290 Verdrag betreffende de werking van de Europese Unie (VwEU).

[45] Artikel 98 PSD2 en GEDELEGEERDE VERORDENING (EU) 2018/389 VAN DE COMMISSIE van 27 november 2017 tot aanvulling van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad wat betreft technische reguleringsnormen voor sterke cliëntauthenticatie en gemeenschappelijke en veilige open communicatiestandaarden.

[46] Zie artikel 4 punt 15 PSD2, geïmplementeerd in artikel 1:1 Wft respectievelijk artikel 7:514 onder v BW.

[47] Voorzover OK IT ook betalingsinformatiediensten wil verlenen (handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, randnummers 15 en 17), wordt dat in dit besluit verder buiten beschouwing gelaten.

48. Op grond van artikel 35 PSD2 – geïmplementeerd in artikel 5:88 lid 1 Wft – dienen banken vergunninghoudende betalingsdienstaanbieders toegang te verlenen tot hun online betalingssystemen. Daarbij dient de toegang objectief, niet-discriminerend en evenredig te zijn.[48] Volgens PSD2 moeten rekeninghoudende betaaldienstverleners (banken) toegang tot hun betalingssystemen en de betaalrekeningen van betalingsdienstgebruikers – na diens instemming – verschaffen aan betalingsdienstaanbieders, zoals betaalinitiatiedienstverleners. Dat kan via een zogeheten “API” (*Application Programming Interface*). De rekeninghoudende betaaldienstverleners (banken) zijn vrij te kiezen of zij een interface aanbieden die specifiek bestemd is voor derde-betaaldienstverleners of het gebruik van de eigen interface toestaan (de interface die zij zelf gebruiken voor de identificatie van en de communicatie met de betaaldienstgebruikers).[49]

49. PSD2 regelt dat de toegang tot de betaalrekening van betalingsdienstgebruikers veilig is. Daartoe geldt een vergunningvereiste voor de betaaldienstverlener (zie verderop meer over de vergunningplicht). Voorts stelt PSD2 een aantal technische normen, zoals reeds aangehaald in randnummer 45, aan de beveiliging van de betaaltransacties en de (technische) communicatie tussen de bank en deze nieuwe betaaldienstverleners (zie verderop meer over Sterke Cliënt Authenticatie en *Redirection*). Hiernaast regelt titel 7B van Boek 7 BW de verantwoordelijkheids- en aansprakelijkheidsverdeling tussen bank en betaalinitiatiedienstverlener. Ter bescherming van de consument tegen de risico’s[50] van het gebruik van betaaldiensten zijn de banken primair aangewezen, zo blijkt uit artikelen 73, 74 en 90 PSD2, geïmplementeerd in artikelen 7:528, 7:529 en 7:543-547 BW, om schade te vergoeden aan de betaaldienstgebruiker (consument).

50. In het hiernavolgende gaat de ACM in op de verschillende veiligheids- en gebruiksvoorschriften uit het regelgevend kader van PSD2 die bepalen onder welke voorwaarden en op welke wijze betaalinitatiedienstverleners toegang tot de betalingssystemen en betaalrekening(informatie) bij de banken kunnen krijgen. Dat zijn achtereenvolgens: 7.3) vergunningplicht, 7.4) sterke cliënt authenticatie en 7.5) obstakelvrije klantreis.

7.3 Vergunningplicht

51. Indien de betaaldienstverlener in Nederland gevestigd is, moet een vergunning worden aangevraagd bij DNB (artikel 2:3a Wft).[51] Een betaaldienstverlener aan wie een vergunning is verleend, definieert de Wft als een betalingsinstelling. De betalingsinstelling is de rechtspersoon aan wie overeenkomstig artikel 11 PSD2 vergunning is verleend om overal in de Europese Unie betalingsdiensten, waaronder betaalinitiatiediensten, aan te bieden en uit te voeren.[52] DNB registreert op haar website welke betaaldienstverleners een vergunning hebben om betalingsdiensten, waaronder

[48] Artikel 36 PSD2 – geïmplementeerd in artikel 5:88a lid 1 Wft – bepaalt voorts dat betalingsinstellingen op objectieve, niet-discriminerende en evenredige wijze toegang moeten hebben tot de betaalrekeningdiensten van kredietinstellingen. Deze bepalingen zien op gevallen waarin betaaldienstverleners een zakelijke betaalrekening willen openen.
[49] Zie considerans, overweging 20, en artikel 30 t/m 33 van de Gedelegeerde Verordening.
[50] Risico’s zoals betaalfraude, diefstal, misbruik van betaalgegevens, wachtwoorden en toegangscodes en gebrekkig uitgevoerde betalingstransacties.
[51] Zie interne email d.d. 25 februari 2021 met kenmerk ACM/INT/420624 met pdf van DNB nieuwsbrief juni 2018 over starten aanvraag vergunning.
[52] Artikel 4 punt 4 PSD2, in Nederland geïmplementeerd in (artikel 1:1 Wft).

betaalinitiatiediensten, uit te oefenen. Betaaldienstverleners met een zetel in een andere lidstaat hebben in beginsel een vergunning nodig die is verleend door de toezichthoudende instantie van die lidstaat.

52. De voorschriften uit artikel 5 PSD2 houden onder meer in dat de aanvrager van een vergunning: (i) een bedrijfsplan voor de eerste drie boekjaren indient, zodat de aanvrager kan aantonen in staat te zijn om op een gezonde basis te opereren; (ii) bewijs verstrekt dat hij over startkapitaal beschikt zoals bedoeld in artikel 7 PSD2 (voor betaalinitiatiediensten ten minste een kapitaal van te allen tijde EUR 50.000); (iii) een beschrijving van de *governance* regelingen verstrekt en mechanismen voor interne controle (o.a. administratieve, boekhoudkundige en risicobeheersingsprocedures) heeft ingesteld; (iv) bepaalde veiligheidsmaatregelen heeft getroffen etc (artikel 2:3b Wft).

7.4 Sterke Cliënt Authenticatie

53. Artikel 66 en 67 PSD2 bepalen dat betalingsdienstaanbieders om toegang te krijgen tot de (gegevens van) betaalrekeningen uitdrukkelijke instemming nodig hebben van hun gebruikers (de betaalrekeninghouders).[53] Deze uitdrukkelijke instemming wordt gegeven door afgifte van sterke cliëntauthenticatie (SCA).[54] Sterke cliëntauthenticatie is in een aantal gevallen niet verplicht, zoals bij contactloze toonbankbetalingen tot 50 euro.[55]

54. In PSD2 is SCA gedefinieerd als: "*authenticatie met gebruikmaking van twee of meer factoren … die onderling onafhankelijk zijn, in die zin dat compromittering van één ervan geen afbreuk doet aan de betrouwbaarheid van de andere en die zodanig is opgezet dat de vertrouwelijkheid van de authenticatiegegevens wordt beschermd*."[56] De factoren zijn:
a) wetenschap, dat is iets wat alleen de gebruiker weet, zoals een wachtwoord of een pincode;
b) bezit, dat is iets wat alleen de gebruiker bezit, zoals een pinpas of een instrument dat een authenticatiecode genereert; en
c) een inherente eigenschap, dat is een unieke persoonlijke eigenschap van de gebruiker, zoals een vingerafdruk of de stem van de gebruiker.

55. In een *Opinion*[57] uit 2018 geeft de EBA duidelijkheid over de SCA in enkele PSD2-artikelen. In randnummers 37 en 38 van deze Opinion staat (onderstrepingen en voetnoten door ACM):

37. Article 97(5) of PSD2 states that the ASPSP[58] shall allow PISPs[59] and AISPs[60] to rely on the authentication procedures provided to its PSUs and Article 67(2)(b) states that the security credentials are accessible to the AISPs and PISPs. Recital 30 of PSD2 also states that 'The personalised

---

[53] Artikel 66 lid 2 respectievelijk art. 67 lid 2 onder a PSD2.
[54] Artikel 97 PSD2. Artikel 26h lid 4, 26i lid 3 en 26j lid 3 Bpr Wft.
[55] Artikelen 10 t/m 18 Gedelegeerde Verordening. Voor de contactloze toonbankbetalingen gelden daarbij restricties m.b.t. de omvang van voorafgaande betalingen en het aantal opeenvolgende betalingen.
[56] Zie artikel 4 punt 30 PSD2.
[57] EBA-OP-2018-04, Opinion of the EBA on the implementation of the RTS on SCA and CSC, d.d. 13 juni 2018.
[58] *Account servicing payment service providers*, oftewel de rekeninghoudende betaaldienstverleners (banken).
[59] *Payment initiation service providers*, oftewel betaalinitiatiedienstverleners.
[60] *Account information service providers*, oftewel rekeninginformatiedienstverleners.

security credentials used for secure customer authentication by the payment service user or by the payment initiation service provider are usually those issued by the account servicing payment service providers'.[61]

38. The articles mentioned above are to be read in conjunction with one another, which means that the PSP applying SCA is the PSP that issues the personalised security credentials. It is consequently also the same provider that decides whether or not to apply an exemption in the context of AIS[62] *and PIS.*[63] *The ASPSP may, however, choose to contract with other providers such as wallet providers or PISPs and AISPs for them to conduct SCA on the ASPSP's behalf and determine the liability between them. The EBA also notes that a number of governmental (national) agreements on universal sets of personalised security credentials that can be used by PSUs with multiple PSPs already exist in some Member States.*"

56. Uit deze Opinion van de EBA volgt dat, ingevolge de PSD2-regels, de rekeninghoudende betaaldienstverleners (banken) en niet de derde-betaaldienstverleners, zoals betaalinitiatiedienstverleners, verantwoordelijk zijn voor het uitvoeren van de SCA. De betaaldienstverlener die verantwoordelijk is voor de SCA is dezelfde bank die verantwoordelijk is voor het uitgeven van de *personalised security credentials*. Dit is de bank waar de betaalrekeninghouder zijn betaalrekening heeft. Dit neemt niet weg dat de bank ervoor kan kiezen om het uitvoeren van de SCA te delegeren aan een derde (zie eveneens randnummer 38 van de *Opinion* hierboven). Dit gebeurt op contractuele basis waarbij de aansprakelijkheid tussen de bank en de derde-betaaldienstverlener wordt geregeld.

7.5 De obstakelvrije klantreis

57. Er bestaan diverse mogelijkheden voor het uitvoeren van de SCA. De mogelijkheden, *redirection*, *embedded* en *decoupled,* noemt de EBA in de *Opinion*[64] uit 2018. De EBA merkt op (onderstrepingen en voetnoten door ACM):

48. There would appear to currently be three main ways or methods of carrying out the authentication procedure of the PSU[65] *through a dedicated interface, and APIs in particular, namely redirection, embedded approaches and decoupled approaches (or a combination thereof). In the cases of redirection and decoupled approaches, PSU's authentication data are exchanged directly between PSUs and ASPSPs*[66]*, as opposed to embedded approaches, in which PSU's authentication data are exchanged between TPPs*[67] *and ASPSPs through the interface. In a number of national markets, many ASPSPs have traditionally used redirection, while other markets have used a more embedded approach.*

---

61 *"De persoonlijke beveiligingsgegevens die worden gebruikt voor veilige cliëntauthenticatie, door de betalingsdienstgebruiker of door de betalingsinitiatiedienstaanbieder, zijn gewoonlijk de gegevens die door de rekeninghoudende betalingsdienstaanbieders worden verstrekt."*

62 *Account Information Services*, oftewel rekeninginformatiediensten.

63 *Payment initiation services*, oftewel betaalinitiatiediensten.

64 EBA-OP-2018-04, Opinion of the EBA on the implementation of the RTS on SCA and CSC, d.d. 13 juni 2018. *Redirection* wordt ook genoemd in artikel 32 lid 3 Gedelegeerde Verordening.

65 *Payment Service User*, oftewel betaaldienstgebruiker.

66 *Account servicing payment service providers*, oftewel de rekeninghoudende betaaldienstverleners (banken).

67 *Third Party Providers*, oftewel derde-dienstverleners.

58. Ingegeven door de wijze waarop *redirection* in artikel 32 lid 3 van de Gedelegeerde Verordening is beschreven, rees de vraag of *redirection* bij het uitvoeren van de SCA al dan niet een obstakel zou vormen voor betaalinitiatiedienstverleners. De EBA heeft hierover duidelijkheid geboden in de genoemde *Opinion*[68] uit 2018 (onderstrepingen door ACM):

    49. Redirection is mentioned in the RTS under Article 32(3), and its featuring in the RTS has generated some debate in the industry, with some market participants expressing the view that the reference suggested that redirection would be an obstacle to the provision of AIS and PIS. The EBA hereby clarifies that the RTS do not state that redirection per se is an obstacle to AISPs and PISPs providing services to their PSUs. Instead, the RTS state that it 'may' be so, if the ASPSP implements it in a manner which is restrictive or obstructive for AISPs or PISPs.

    50. When determining which method(s) to use for the purpose of carrying out the authentication procedure, in line with Article 97(5) PSD2 and Article 30(2) of the RTS, all methods of SCA provided to the PSU need to be supported when an AISP or PISP is used. If they were not, this would constitute an obstacle. Therefore, which method, or combination of methods, any particular ASPSP needs to use will depend on the authentication procedures it offers to its own PSUs.

59. Uit voorgaande volgt dat, volgens de nadere duiding van de PSD2-regels door de EBA, *redirection* op zichzelf géén obstakel vormt voor betaalinitiatiedienstverleners. Wel dienen de banken *redirection* op een even gebruiksvriendelijke wijze (geen onnodige frictie en niet extra omslachtig) ter beschikking te stellen als de SCA-procedures die zij zelf hanteren in hun directe relatie tot de rekeninghouder. Dit blijkt uit een andere *Opinion*[69] van de EBA (onderstreping door ACM):

    6. As clarified in the EBA Opinion on the implementation of the RTS (EBA-Op-2018-04)3 and the EBA Guidelines on the exemption from the contingency mechanism under Article 33(6) RTS (EBA/GL/2018/07)4, the EBA is of the view that redirection is not, in itself, an obstacle, but that it may be an obstacle depending on the way it is implemented. The EBA clarifies that redirection can be an obstacle if implemented in a manner that creates unnecessary friction in the customer experience when using TPPs' services, or if the authentication procedure with the ASPSP is more cumbersome compared to the equivalent experience PSUs have when directly accessing their payment accounts or initiating a payment with the ASPSP.

60. Banken mogen tijdens de sterke cliëntauthenticatie geen obstakels opwerpen voor derde betaaldienstaanbieders, zoals betaalinitiatiedienstverleners. De Q&A die DNB hierover heeft gepubliceerd heeft specifiek betrekking op het door de EBA toegestane *redirection*-model en betreft de gehele klantreis in zowel het domein van de derde partij als het domein van de bank. Obstakels, volgens DNB, zijn bijvoorbeeld: in één klantreis (betaalproces/transactie) twee keer *strong customer authentication* (SCA) uitvoeren, management van de scope van consent of consent management-gerelateerde stappen, additionele bevestigingsschermen (bijv. een overzichtspagina met 'verder' knop), *redirection*-schermen die een actie verlangen van de betaaldienstgebruiker en ontmoedigend

[68] EBA-OP-2018-04, Opinion of the EBA on the implementation of the RTS on SCA and CSC, d.d. 13 juni 2018.
[69] EBA/OP/2020/10, "*Opinion of the EBA on obstacles under Article 32(2) of the RTS on SCA and CSC*", d.d. 4 juni 2020.

taalgebruik.[70]

8 Beoordeling

8.1 Inleiding

61. In dit hoofdstuk beoordeelt de ACM het handhavingsverzoek aan de hand van het criterium uit haar prioriteringsbeleid dat betrekking heeft op de vraag in hoeverre de ACM in staat is om doeltreffend en doelmatig op te treden.

8.2 PSD2 in het initieel onderzoek

62. Een volledig onderzoek van de ACM zou gericht zijn op het vaststellen of wel of niet sprake is van overtreding van de Mededingingswet (en het Verdrag betreffende de werking van de Europese Unie) bestaande uit het misbruik maken van een machtspositie en/of het maken van mededingingsbeperkende afspraken. In dit geval staan de regels uit de Mededingingswet naast het uitgebreide regelgevend kader van PSD2, meer in het bijzonder het vergunningvereiste en de SCA-vereisten waarop DNB toeziet. Het handhavingsverzoek steunt in belangrijke mate ook op de – door OK IT voorgestane wijze van uitleg van – regels (rondom de SCA) uit PSD2. De regels uit PSD2 inzake de vergunning en de SCA kunnen evenwel niet worden doorkruist of buiten beschouwing blijven bij het toepassen van het verbod op mededingingsbeperkende afspraken (artikel 6 Mw en artikel 101 VWEU) en/of van het verbod op misbruik van een economische machtspositie (artikel 24 Mw en artikel 102 VWEU). Alleen als naast, dat wil zeggen met inachtneming van, de PSD2-regelgeving een overtreding van de mededingingsregels zou kunnen worden vastgesteld, zou de ACM doelmatig en doeltreffend kunnen optreden al naar gelang de uitkomst van een volledig onderzoek.

63. Onderstaand gaat de ACM op basis van het initieel onderzoek in op het vergunningvereiste en de vereiste sterke cliënt authenticatie uit PSD2.

8.3 Geen vergunning voor betaalinitiatiediensten

64. De ACM stelt vast dat OK IT geen vergunning heeft van DNB voor de uitoefening van betaalinitiatiediensten in de zin van PSD2 (randnummers 13, 28 en 29). Payconiq heeft overigens wel een vergunning, verkregen in Luxemburg (randnummer 24). Zonder vergunning is het op grond van de PSD2-regelgeving verboden betaalinitiatiediensten te verlenen en het toezicht hieromtrent is in handen van DNB (randnummers 44, 51 en 52). De verplichting voor banken om toegang tot de betalingssystemen en betaalrekeningen te verlenen ziet, ingevolge de PSD2-regels, ook uitsluitend op derde-betaaldienstverleners, zoals betaalinitatiedienstverleners met vergunning (randnummer 48).

65. Uitgaande van het in de PSD2-regelgeving neergelegde vergunningvereiste en gegeven het feit dat OK IT niet over een vergunning van DNB beschikt, acht de ACM verdere behandeling van het handhavingsverzoek niet doelmatig en doeltreffend.

[70] Zie “Klantreis zonder obstakels inzake betaalinitiatie- en rekeninginformatiediensten via derde partijen in het geval van “redirection”.”, 8 augustus 2019, Q&A, DNB, in ACM/INT/420572. Zie voorts “Een obstakelvrije klantreis voor betaalinitiatie- en rekeninginformatiediensten via een speciale interface op basis van redirection.”, 1 juli 2020, Q&A, DNB, in ACM/INT/420572.

8.4 Sterke Cliënt Authenticatie via *redirection*

66. De ACM merkt op dat er, volgens het handhavingsverzoek, sprake zou zijn van een toegangsweigering. Echter, uit de verdere toelichting en onderbouwing die het handhavingsverzoek geeft, blijkt geen toegangsweigering door de banken, maar dat er sprake zou kunnen zijn van toegang door middel van '*redirect*' ten behoeve van de SCA (randnummers 30 en 33). Bovendien blijkt uit het handhavingsverzoek dat hierover ruim voor het van kracht worden van de PSD2-regels per 14 september 2019 contact geweest is tussen OK IT en de banken en dat OK IT het daarna niet meer bij de banken heeft aangekaart (randnummers 27 en 29).[71]

67. Voorts merkt de ACM op dat het vereiste van de Sterke Cliënt Authenticatie (hierna: SCA) volgens de PSD2-regels door de banken uitgevoerd c.q. nageleefd moet worden (randnummers 55 en 56) en niet door de betaalinitiatiedienstverleners, zoals OK IT stelt. Hierbij kunnen de banken gebruik maken van verschillende methoden, waaronder '*redirect*'. (randnummer 57) Het gaat hier om een volgens de PSD2-regels en de in *Opinions* gegeven verduidelijkingen van de EBA, toegestane SCA-methode (randnummer 58). Ten onrechte beklaagt OK IT zich dan ook over het toepassen van de banken van deze toegestane methode voor de SCA.

68. Het vereiste van de SCA mag dus door de banken uitgevoerd worden via de mogelijkheid van *redirection*.[72] Deze mogelijkheid vormt op zich geen obstakel voor betaalinitiatie-dienstverleners volgens de PSD2-regelgeving. Slechts in bepaalde gevallen waar sprake is van onnodige frictie en/of een, in vergelijking met andere SCA-mogelijkheden, extra omslachtige betaalprocedure, kan sprake zijn van obstakels (randnummers 59 en 60). Uit het handhavingsverzoek, waar dergelijke gevallen niet zijn genoemd, blijkt volgens de ACM niet dat daar in deze zaak sprake van is. Het handhavingsverzoek wijst er alleen op dat OK IT wenst dat de gebruiker, net als bij de Payconiq app, in de visuele en virtuele omgeving van de OK app blijft, en dat OK IT geen *redirection* wil (randnummer 16).[73] Er blijkt niet dat en hoe de gebruiksomgang, de bediening van het mobiele apparaat en de te verrichten opdrachten en/of handelingen, tijdens de betalingstransactie of het betaalproces verschilt tussen de OK app en de Payconiq app (randnummers 16 en 26). Van obstakels, onnodige frictie of extra omslachtige betaalprocedure, blijkt dan ook geen sprake te zijn.

69. Mede gelet op het voorgaande acht de ACM het niet doelmatig en doeltreffend om het handhavingsverzoek verder in behandeling te nemen en een volledig mededingingsonderzoek te starten.

---

[71] Zie het handhavingsverzoek d.d. 7 oktober 2020 met kenmerk ACM/IN/544871, randnummers 25 – 27 en 32 alsmede bijlagen 1, 2, 3 en 10 bij het handhavingsverzoek.
[72] De ACM merkt op dat bij het betalen onderling, op afstand en op locatie verschillende redirect-toepassingen, zoals browser-redirection en app-to-app redirection, zijn te onderscheiden.
[73] Overigens brengt de omleiding (*redirect*) naar de bankomgeving de consument tijdens de betaaltransactie in contact met de virtuele omgeving van zijn of haar eigen bank, wat voor hem of haar niet vreemd of storend zal zijn en mogelijk zelfs het vertrouwen in OK IT als betaaldienst versterken kan.

8.5 Conclusie beoordeling

70. De ACM komt op basis van haar initieel onderzoek tot de conclusie dat zij niet in staat zal zijn doelmatig en doeltreffend op te treden en om die reden geen volledig mededingingsonderzoek start en het handhavingsverzoek niet (verder) in behandeling neemt.

9 Besluit

71. De Autoriteit Consument en Markt (ACM) wijst de aanvraag tot handhaving van de Mededingingswet en het nemen van een besluit als bedoeld in artikel 56, eerste lid Mededingingswet af.

Hoogachtend,

Autoriteit Consument en Markt,
Namens deze,

M. Denkers BA, Msc, MBA
Directeur Directie Mededinging

Als u belanghebbende bent, kunt u schriftelijk bezwaar maken tegen dit besluit. Stuur uw gemotiveerde bezwaarschrift naar de Autoriteit Consument en Markt, Juridische Zaken, postbus 16326, 2500 BH Den Haag. Dit moet u doen binnen zes weken na de dag waarop dit besluit bekend is gemaakt. In uw bezwaarschrift kunt u de Autoriteit Consument en Markt verzoeken in te stemmen met rechtstreeks beroep bij de bestuursrechter.