Uitspraak Geschillencommissie Kifid nr. 2025-0573

(prof. mr. M.L. Hendrikse, voorzitter en mr. A. Kanhai, secretaris)

Datum uitspraak	18 juli 2025
Klacht van	De consument
Tegen	International Card Services B.V., gevestigd te Diemen, verder te noemen ICS
Aard uitspraak	Bindend advies
Uitkomst	Vordering afgewezen
Bijlage	Relevante bepalingen uit de wet en de algemene voorwaarden

Samenvatting

Niet-toegestane betalingstransacties. De consument is slachtoffer geworden van oplichting. Een oplichter heeft zijn creditcard toegevoegd aan een Apple Pay-Wallet en heeft betalingen verricht die ten laste van de creditcardrekening zijn gebracht. De consument vordert terugbetaling van de opgenomen bedragen. De commissie oordeelt dat de consument niet heeft voldaan aan zijn verzwaarde motiveringsplicht: hij heeft onvoldoende inzicht gegeven in de wijze waarop de fraude heeft kunnen plaatsvinden. Dit leidt ertoe dat ICS de schade niet hoeft te vergoeden. De vordering wordt afgewezen.

1. Procedure

1.1 De commissie beslist volgens haar reglement en op basis van de stukken ingediend door partijen.

1.2 De commissie is van oordeel dat het niet nodig is de zaak mondeling te behandelen. De zaak wordt daarom op grond van de stukken beslist.

1.3 De consument heeft gekozen voor een bindend advies. Dit betekent dat partijen elkaar aan de uitspraak kunnen houden.

2. Het geschil

Wat is er gebeurd?

2.1 Op 24 juni 2024 heeft ICS de creditcard naar de consument verstuurd. Op 26 juni 2024 heeft de consument de creditcard geactiveerd. Op de overeenkomst tussen de consument en ICS zijn de Algemene Card-voorwaarden ABN AMRO en ABN AMRO MeesPierson (hierna: de algemene voorwaarden) van toepassing. Voor de beoordeling is artikel 5 van de algemene voorwaarden relevant. Dit artikel is opgenomen in de bijlage bij deze uitspraak.

2.2 Via de ABN AMRO Creditcardapp (hierna: de app) kan Apple Pay aan de creditcardrekening worden gekoppeld. ICS heeft naast de app ook een webportaal (hierna: de portal). Voor activatie van zowel de app als de portal is het noodzakelijk dat degene die de app/portal wil activeren, beschikt over door ICS verzonden verificatiecodes (hierna: de verificatiecodes). ICS verstuurt zowel bij activatie van de app, als activatie van de portal twee verificatiecodes. De eerste verificatiecode wordt per e-mail verstuurd naar het e-mailadres dat is geregistreerd (hierna: de eerste verificatiecode). Als de eerste verificatiecode correct is ingevoerd, dan wordt per SMS de tweede verificatiecode naar het geregistreerde telefoon-nummer (hierna: de tweede verificatiecode)verstuurd. Daarnaast geldt dat ICS voor het activeren van en bij iedere inlogpoging op de portal per SMS een 'One Time Password' (hierna: OTP[1]) naar het geregistreerde telefoonnummer van de consument verstuurt.

2.3 Op 26 juni 2024 om 13:30 uur is de app geactiveerd. Hieronder zal het koppelingsproces worden beschreven. Vaststaat dat het geregistreerde telefoonnummer en het e-mailadres van de consument zijn.

Beschrijving koppelingsproces		
Stap	tijdstip	actie
Stap 1:		Het invoeren van de creditcardgegevens. Het gaat om: • de naam van de houder (in dit geval de consument); • het creditcardnummer; • de vervaldatum van de creditcard; • de veiligheidscode (CVC-code) die op de creditcard staat.
Stap 2:	13:29:07	ICS heeft **via e-mail** een verificatiecode naar het e-mailadres van de consument gezonden. Deze code is correct ingevoerd.
Stap 3:	13:29:55	ICS heeft – nadat de verificatiecode uit stap 2 correct is ingevoerd- **via SMS** een tweede verificatiecode naar het telefoonnummer van de consument gestuurd.

2.4 Op 28 juni 2024 om 10:31 uur is het webportaal van ICS (hierna: de portal) geactiveerd. Hierbij zijn de juiste verificatiecodes en het OTP ingevoerd. Om 13:22 uur wordt er opnieuw ingelogd met de verificatiecodes en het OTP. Daarbij wordt het telefoonnummer van de consument gewijzigd. ICS heeft hiervan een bevestiging gestuurd naar het oude telefoonnummer dat tot de wijziging was geregistreerd (het telefoonnummer van de consument).

2.5 Op 30 juni 2024 is opnieuw op de portal ingelogd met de verificatiecodes en het OTP. Daarbij is het e-mailadres van de consument gewijzigd. Vaststaat dat er nu een andere telefoonnummer en e-mailadres zijn geregistreerd.

[1] Een OTP is een wachtwoord dat eenmalig kan worden gebruikt voor authenticatie.

2.6 Op 3 juli 2024 is Apple Pay aan de creditcardrekening gekoppeld. Dit is gebeurd via de app door de creditcard toe te voegen aan Apple Wallet. Om Apple Pay te kunnen koppelen zijn de verificatiecodes nodig. Deze zijn echter naar het gewijzigde e-mailadres en telefoon-nummer verzonden.

2.7 Tussen 4 en 10 juli 2024 is met Apple Pay in totaal voor € 2.233,80 aan onbekende betalingen verricht, waaronder contante opnames bij een geldautomaat. Voor het opnemen van contanten bij een geldautomaat met Apple Pay dient men te beschikken over de pincode die bij de fysieke creditcard hoort.

2.8 Op enig moment heeft de consument ICS verzocht de door hem geleden schade aan hem te vergoeden. Daartoe heeft hij op 12 augustus 2024 aangifte gedaan bij de politie. Op 27 augustus 2024 heeft de consument op verzoek van ICS een aanvullende aangifte gedaan omdat uit de eerste aangifte niet blijkt hoe de fraude plaats heeft kunnen vinden. In de aanvullende aangifte staat dat de consument heeft geprobeerd de app te installeren maar dat dit hem niet is gelukt.

2.9 Op 17 september 2024 heeft ICS de claim van de consument afgewezen en naar Kifid verwezen.

De klacht en vordering

2.10 De consument vordert € 2.233,-. De consument voert hiertoe het volgende aan. De consument is niet onzorgvuldig met zijn gegevens omgegaan. De berichten en verificatiecodes die ICS heeft verzonden heeft de consument niet ontvangen. Het is voor hem een raadsel hoe die codes in handen van derden zijn geraakt. Wel heeft hij geprobeerd om de app te installeren maar dit is hem niet gelukt. Het kan zijn dat toen de beveiligings-gegevens bij anderen terecht zijn gekomen. Ook heeft de consument geen iPhone. De consument vindt het niet eerlijk dat het aan hem is om te bewijzen wat er gebeurd zou kunnen zijn. Dit is voor de consument namelijk ook onduidelijk. Daarnaast vindt de consument het een kwalijke zaak dat ICS niet in een eerder stadium het door de oplichter gewijzigde e-mailadres en het telefoonnummer heeft verstrekt. Mogelijk had de politie meer kunnen doen als deze gegevens eerder met de consument waren gedeeld.

Het verweer

2.11 ICS voert verweer tegen de stellingen van de consument. Voor zover relevant zal de commissie bij de beoordeling daarop ingaan.

3. De beoordeling

Waar deze zaak om gaat

3.1 De commissie moet beoordelen of ICS een bedrag van € 2.233,- aan de consument moet betalen. De commissie komt tot de conclusie dat ICS dat niet hoeft te doen en licht dat hieronder toe.

Het juridisch kader bij niet-toegestane betalingstransacties

3.2 Partijen zijn het erover eens dat de consument geen toestemming heeft gegeven voor de betaalopdrachten. De commissie gaat er daarom van uit dat sprake is van niet-toegestane betalingstransacties. Bij een niet-toegestane betalingstransactie geldt dat de betaaldienstverlener – in dit geval ICS – het bedrag van de betalingstransactie onmiddellijk aan de consument moet terugbetalen.[2] Op deze regel bestaat een uitzondering. Als de consument – kort gezegd – met grove nalatigheid de overeengekomen veiligheidsregels ten aanzien van betaalinstrumenten niet is nagekomen, draagt de consument zelf de verliezen.[3]

3.3 Het is in beginsel aan ICS om te stellen – en bij gemotiveerde betwisting door de consument te bewijzen – dat sprake is van grove nalatigheid aan de zijde van de consument. Maar op de consument rust bij de gemotiveerde betwisting wel een verzwaarde motiveringsplicht: hij moet ICS voldoende feitelijke gegevens aanreiken om het verwijt van grove nalatigheid rond te maken of deze laatste tot de conclusie te laten komen dat grove nalatigheid in het geheel niet aan de orde is. Het gaat daarbij om gegevens die zich in het domein van de consument bevinden en die licht kunnen werpen op de wijze waarop zijn creditcardgegevens, pincode en/of codes voor het installeren van de app in handen van de onbevoegde derde (fraudeur) hebben kunnen komen. Dat betekent meer concreet dat van de consument mag worden verwacht dat hij zo goed mogelijk een verklaring biedt voor de omstandigheid dat zijn creditcardgegevens en/of de codes in handen van een onbevoegde derde zijn gekomen. De enkele stelling van de consument dat hij dit niet kan verklaren, is hiervoor onvoldoende.[4] Zoals de commissie in eerdere uitspraken heeft overwogen zou de betaaldienstverlener anders voor onaanvaardbare risico's van misbruik geplaatst worden nu het alleen de consument is die weet wat hij in dezen heeft gedaan.[5]

Het juridisch kader toegepast op deze zaak

3.4 De consument heeft gesteld dat hij geen idee heeft hoe de fraude plaats heeft kunnen vinden. De enige verklaring die de consument heeft gegeven dat hij in de door ICS genoemde periode heeft geprobeerd de app te installeren, maar dat dit hem niet is gelukt. Mogelijk zijn zijn gegevens toen in de handen van de fraudeur gekomen. Hij heeft geen verklaring voor het feit dat de verificatiecodes, OTP's en de pincode in handen van de fraudeur zijn gekomen.

3.5 ICS heeft daar tegenover het volgende gesteld. Uit haar administratie blijkt dat op 26 juni 2024 de app is geactiveerd op een iPhone. Hierbij zijn de juiste creditcardgegevens en verificatiecodes ingevuld (zie 2.2 en 2.3; eerst dient men de creditcardgegevens in te vullen, vervolgens volgt een e-mail met een verificatiecode 1.

---

[2] Dit volgt uit artikel 7:528 lid 1 BW.
[3] Artikel 7:529 lid 1 BW in samenhang met artikel 7:524 lid 1 BW.
[4] Zie GC Kifid, nrs. 2022-0604, 2025-0151 en 2025-0410.
[5] Zie GC Kifid, nrs. 2019-733, 2021-0265 en 2025-0410.

Als die verificatiecode correct is ingevuld volgt een verificatiecode 2 per SMS). Daarnaast heeft ICS gemotiveerd gesteld dat men met Apple Pay alleen contante opnames bij een geldautomaat kan verrichten als men beschikt over de bij de fysieke creditcard behorende pincode.

3.6 De commissie overweegt dat het activeren van de app en de portal alleen mogelijk is met gebruik van de verificatiecodes die alleen aan het e-mailadres en het telefoonnummer van de consument worden verstuurd. De consument heeft niet verklaard hoe een derde in staat is geweest de app en de portal te activeren met gebruik van deze persoonlijke codes. Als de consument zelf geen codes heeft gedeeld, dan moet een derde toegang hebben gehad tot zijn mobiele telefoon en persoonlijke mailbox. Dat ligt in zijn risicosfeer. Dit geldt eveneens voor het feit dat een derde kon beschikken over de persoonlijke pincode van de fysieke creditcard.

3.7 De commissie komt tot het oordeel dat de consument niet aan zijn verzwaarde motiveringsplicht heeft voldaan. De consument heeft geen feiten of omstandigheden gesteld die verklaren hoe een derde met gebruik van de persoonlijke verificatiecodes, waar alleen de consument toegang tot zou moeten hebben, de app en de portal heeft kunnen activeren. Vervolgens is via de app Apple Pay aan de creditcardrekening gekoppeld en zijn daarmee de betwiste betalingstransacties verricht. Via de portal zijn voorts de contact-gegevens van de consument gewijzigd. De commissie kan dan ook niet anders dan concluderen dat de consument onvoldoende zorgvuldigheid heeft betracht waardoor een derde toegang heeft gehad tot de persoonlijke beveiligingscodes waardoor de fraude heeft kunnen plaatsvinden De commissie komt daarom tot het oordeel dat de consument in juridische zin met grove nalatigheid de in artikel 5 van de algemene voorwaarden opgenomen voorschriften niet heeft nageleefd nu hij de stellingen van de bank onvoldoende heeft betwist door niet te voldoen aan de op hem rustende motiveringsplicht. ICS hoeft het bedrag van € 2.233,- niet aan de consument te vergoeden. De stellingen van de consument dat hij geen iPhone heeft en dat hij het niet eens is met de omstandigheid dat de bewijslast bij hem ligt, maken het oordeel van de commissie niet anders. Ook het verwijt van de consument aan ICS dat zij in de interne klachtenprocedure niet het gewijzigde e-mailadres en telefoonnummer wilde prijsgeven kan niet tot een ander oordeel leiden. Dit verwijt staat immers los van de vraag of de ICS gehouden is de consument schadeloos te stellen zodat de commissie daar ook niet op in zal gaan.

Ambtshalve toetsing

3.8 Voor de beoordeling van de klacht is artikel 5 van de algemene voorwaarden van belang. Dit beding is door de commissie getoetst aan het Europese en Nederlandse (consumenten)-recht waarvoor ambtshalve toetsing geldt en de commissie acht het beding niet in strijd met deze regelgeving.

4. De beslissing

De commissie wijst de vorderingen af.

Deze uitspraak is bindend. Of u tegen deze uitspraak beroep kunt instellen, kunt u nalezen in regel 7 van het Reglement Commissie van Beroep Kifid – vanaf 1 april 2024, te vinden op de website www.kifid.nl/reglementen-en-statuten. In regel 18.1 van dat reglement is bepaald dat beroep kan worden ingesteld tot 6 weken na de dag van deze uitspraak. Meer informatie over het instellen van beroep kunt u vinden op de website www.kifid.nl/in-beroep-gaan-bij-kifid.

Binnen 2 weken na verzending van de uitspraak kunt u schriftelijk verzoeken een overduidelijke vergissing in de uitspraak zoals een schrijffout, een verkeerde naam/datum of een rekenfout te herstellen. De beslissing in de uitspraak kan hiermee niet ter discussie worden gesteld. Ook kunt u binnen 2 weken na verzending van de uitspraak schriftelijk verzoeken de uitspraak aan te vullen als u vindt dat niet op alle onderdelen van uw vordering is beslist. Dit ziet niet op de situatie waarin u meent dat de Geschillencommissie Kifid niet op al uw argumenten is ingegaan. Meer informatie hierover staat onder vraag 58 en 59 van het Reglement Geschillencommissie Kifid – vanaf 1 april 2024, te vinden op de website www.kifid.nl/reglementen-en-statuten.

Contactgegevens Klachteninstituut financiële dienstverlening

Telefoonnummer: 070 - 333 8 999
Website: www.kifid.nl

Bijlage - Relevante bepalingen uit wetgeving en de algemene voorwaarden

Afdeling 2. Toestaan van betalingstransacties

Artikel 522

2 De instemming met een betaalopdracht wordt verleend overeenkomstig de tussen de betaler en zijn relevante betaaldienstverlener(s) overeengekomen vorm en procedure. De instemming met de uitvoering van een betalingstransactie kan ook worden verleend via de begunstigde of de betaalinitiatiedienstverlener. Bij gebreke van een dergelijke instemming wordt een betalingstransactie als niet toegestaan aangemerkt.

Artikel 524

1 De betaaldienstgebruiker die gemachtigd is om een betaalinstrument te gebruiken,

a. gebruikt het betaalinstrument overeenkomstig de voorwaarden die op de uitgifte en het gebruik van het betaalinstrument van toepassing zijn, en

b. (...)

Afdeling 2. Toestaan van betalingstransacties

Artikel 528

1 Onverminderd artikel 526, betaalt de betaaldienstverlener van de betaler, in geval van een niet-toegestane betalingstransactie, de betaler onmiddellijk het bedrag van de niet-toegestane betalingstransactie terug en in elk geval uiterlijk aan het einde van de eerstvolgende werkdag, nadat hij bekend is geworden met de transactie of daarvan in kennis is gesteld.

(...)

Afdeling 2. Toestaan van betalingstransacties

Artikel 529

1 De betaler draagt alle verliezen die uit niet-toegestane betalingstransacties voortvloeien, indien deze zich hebben voorgedaan doordat hij frauduleus heeft gehandeld of opzettelijk of met grove nalatigheid een of meer verplichtingen uit hoofde van artikel 524 niet is nagekomen.

(...)

Artikel 5 van de algemene voorwaarden

"Artikel 5 Pincode en geheimhouding	
5.1	*Uw Card heeft een pincode. Deze pincode heeft u zelf gekozen of is automatisch aan u toegekend. De pincode is net zoals uw Card persoonlijk en mag alleen door u worden gebruikt. Wij kunnen instructies geven over het kiezen van de pincode. Deze moet u opvolgen.*
	(...)
5.4	*Ook andere persoonlijke beveiligingscodes met betrekking tot uw Card, zoals een inlogneem, een (3D Secure) wachtwoord, Biometrie, Toegangscode of SMS Code mogen alleen door u worden gebruikt en moet u geheimhouden."*