Uitspraak Geschillencommissie Kifid nr. 2025-0570

(mr. F.H.E. Boerma, voorzitter, mr. L. van Berkum, A.E. Tevel, leden en mr. B. Breman, secretaris)

Datum uitspraak	17 juli 2025
Klacht van	De consument
Tegen	De Volksbank N.V. h.o.d.n. ASN Bank, gevestigd te Den Haag, verder te noemen de bank
Aard uitspraak	Bindend advies
Uitkomst	Vordering afgewezen
Bijlage	Relevante bepalingen uit wet- en regelgeving en de algemene voorwaarden

Samenvatting

Fraude. Niet-toegestane betalingstransacties. De consument is het slachtoffer geworden van fraude. De bank heeft beargumenteerd dat de consument naar alle waarschijnlijkheid de fraudeur toegang heeft verschaft tot haar computer en beveiligingscodes. De fraudeur heeft vervolgens frauduleuze transacties verricht ten laste van haar betaalrekening, als gevolg waarvan de consument schade heeft geleden. De commissie is van oordeel dat de consument onvoldoende inzicht heeft gegeven in de wijze waarop de fraudeur zich toegang heeft verschaft tot haar computer en beveiligingscodes. De consument heeft daarmee niet aan haar verzwaarde stelplicht voldaan. De commissie kan daarom niet anders dan oordelen dat de consument in juridische zin grof nalatig heeft gehandeld door zich niet aan de veiligheidsvoorschriften te houden. De vordering wordt afgewezen.

1. Procedure

1.1 De behandelend commissie, verder te noemen de commissie, beslist op basis van het reglement en op basis van de door partijen aan Kifid ingestuurde documenten inclusief bijlagen. Het gaat om: 1) het klachtformulier van de consument; 2) de aanvullende stukken van de consument; 3) het verweerschrift van de bank; 4) de repliek van de consument en 5) de dupliek van de bank.

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 en de bank hebben gekozen voor een bindend advies. Dit betekent dat partijen elkaar aan de uitspraak kunnen houden.

2. Het geschil

Wat is er gebeurd?

2.1 De consument houdt een betaal- en spaarrekening aan bij de bank. Op de betaal- en spaarrekening zijn de Voorwaarden ASN Online Bankieren (hierna: algemene voorwaarden) van toepassing.

2.2 Op 15 oktober 2024 omstreeks 18:15 uur is de consument op haar vaste telefoon gebeld door iemand die zich voordeed als medewerker van 'het fraudeteam' (hierna: de fraudeur) die haar informeerde dat er iemand op haar geld uit was. Op de vaste telefoon werd geen telefoonnummer weergegeven. Na een kort gesprek deed de fraudeur het voorkomen alsof hij de consument zogenaamd doorverbond met een medewerker van de bank.

2.3 In het gesprek dat daarop volgde, vroeg de fraudeur de consument de afboekingen op haar betaalrekening te controleren. Nadat de consument via haar computer op de website van de bank had ingelogd, gaf zij aan geen afboekingen te zien. De fraudeur heeft de consument daarop verteld dat deze afboekingen alleen voor hem zichtbaar waren. De fraudeur heeft de consument daarna opgedragen allerlei handelingen te verrichten, waaronder het inloggen in haar mailbox en een foto te maken van haar rijbewijs en van haar gezicht. Op enig moment zag de consument dat een derde op afstand gebruikmaakte van haar computer.

2.4 Vervolgens zag de consument tijdens het gesprek bedragen van haar spaarrekening naar haar betaalrekening overgeboekt worden. Op enig moment heeft zij opgemerkt dat er meer geld van haar betaalrekening verdween dan dat er binnenkwam, waarna de fraudeur haar ervan heeft verzekerd dat een eventueel tekort door de bank zou worden aangevuld.

2.5 Uit de bankadministratie volgt dat de browsercode op de computer van de consument is gebruikt bij het verrichten en autoriseren van zes frauduleuze transacties via iDeal en twee interne overboekingen op 15 oktober 2024 tussen 18:57 uur en 20:43 uur. Bij alle transacties is het IP-adres van de consument geregistreerd. Daarnaast zijn de Mobiel Bankieren App en Apple Pay op dezelfde dag tussen 20:04 uur en 20:16 uur geïnstalleerd op een iPhone SE, waarbij achtereenvolgens de betaalpasgegevens van de consument en een zescijferige code zijn ingevoerd. De zescijferige code is naar zowel het e-mailadres als het bij de bank bekende telefoonnummer van de consument verstuurd. Vanaf deze iPhone SE is vervolgens één interne overboeking van € 1.500, - gedaan van de spaarrekening van de consument naar haar betaalrekening. In totaal is € 4.915,35 van de betaalrekening afgeschreven, waarvan de bank € 969,- achteraf heeft weten veilig te stellen.

2.6 Op 16 oktober 2024 heeft de consument een e-mail van de bank gekregen met het verzoek om contact op te nemen met de fraudedesk van de bank. De medewerker van de bank heeft haar vervolgens medegedeeld dat er afschrijvingen van haar betaalrekening waren gedaan en dat zij is opgelicht.

2.7 Op 3 december 2024 heeft de consument intern haar beklag gedaan bij de bank. Verdere correspondentie tussen partijen in de interne klachtenprocedure heeft niet geleid tot een oplossing van de klacht.

De vordering en klacht

2.8 De consument heeft schade van € 3.946,35 geleden. Zij vordert dat de bank haar een coulancevergoeding aanbiedt. Ter onderbouwing van haar vordering voert ze verder het volgende aan.

- Ze stelt voorop dat zij is misleid door de fraudeur. De fraudeur kwam geloofwaardig over, doordat hij op de hoogte was van haar woon- en e-mailadres. Zij is zo door de fraudeur verzocht allerlei handelingen te verrichten en zag op een gegeven moment bedragen van haar spaarrekening naar haar betaalrekening overgeboekt worden. Telkens wanneer zij haar twijfels uitsprak over het handelen van de fraudeur, loog hij tegen haar en verzekerde hij haar ervan dat een eventueel tekort op haar betaalrekening de dag daarna door de bank zou worden aangevuld.

- Bovendien zijn meerdere stellingen van de bank onjuist. Zij heeft de iDeal betalingstransacties *niet* geautoriseerd door (middel van het doorgeven van) haar browsercode, dat was namelijk alleen nodig om toegang te krijgen tot haar bankgegevens. Zij heeft ook *geen* beveiligingscode doorgegeven die per sms naar een mobiele telefoon van haar verzonden zou zijn. De mobiele telefoon waarnaar de bank verwijst gebruikte zij immers ten tijde van de fraude niet meer. Tot slot weet zij zeker dat ze de fraudeur geen toegang tot haar computer heeft verschaft via Teamviewer. Zij heeft geheel geen Teamviewer gebruikt. De enige die buiten haar toegang heeft tot Teamviewer is haar schoonzoon die haar af en toe helpt met computerzaken. De hacker moet een andere manier hebben gevonden om het systeem van de consument binnen te dringen. De consument heeft alle veiligheidsregels in acht genomen zoals die door de bank zijn geformuleerd.

- Ten slotte wil zij specifiek ingaan op de browsercode. Het gebruik van een browsercode voor het goedkeuren van betalingstransacties is een zwak beveiligde manier ten opzichte van de tweefactor-authenticatie. Op internet is te vinden dat de browsercode is te misbruiken als een derde toegang krijgt tot de computer. De bank had haar deze manier van autorisatie van betalingstransacties niet aan moeten bieden, want er zijn andere alternatieven die veel veiliger zijn.

Het verweer

2.9 De bank heeft verweer gevoerd tegen de stellingen van de consument. Voor zover relevant zal de commissie bij de beoordeling daarop ingaan.

3. De beoordeling

Waarover de commissie moet oordelen

3.1 De commissie stelt voorop dat zij het betreurt dat de consument slachtoffer is geworden van fraude en dat zij daardoor schade heeft geleden. De vraag die de commissie echter moet beantwoorden is of de bank verplicht kan worden tot vergoeding van de schade van de consument. De commissie is van oordeel dat de bank daartoe niet verplicht kan worden en licht dat hieronder toe.

Niet-toegestane betalingstransacties

3.2 Tussen partijen is niet in geschil dat de consument niet heeft ingestemd met de betalingstransacties. Dergelijke transacties worden volgens artikel 7:522 lid 2 van het Burgerlijk Wetboek (hierna: BW) aangemerkt als niet-toegestane betalingstransacties. In beginsel is de bank volgens artikel 7:528 lid 1 BW verplicht het bedrag van de niet-toegestane betalingstransacties (onmiddellijk) terug te betalen. Hierop bestaat echter een uitzondering. Artikel 7:529 lid 1 BW bepaalt dat de bank niet hoeft te vergoeden als de niet-toegestane betalingstransacties voortvloeien uit frauduleus of opzettelijk handelen van de consument of het met grove nalatigheid niet nakomen van één of meer verplichtingen die gelden op grond van artikel 7:524 BW. Dit artikel bepaalt onder meer dat de consument zich moet houden aan de veiligheidsregels van de bank en moet handelen volgens de algemene voorwaarden die van toepassing zijn op het betaalinstrument.

De consument heeft in juridische zin grof nalatig gehandeld

3.3 Het uitgangspunt is dat de betaaldienstverlener, in dit geval de bank, moet bewijzen dat de consument grove nalatigheid kan worden verweten.[1] In dat kader heeft de bank onder meer verwezen naar haar algemene voorwaarden[2], waarin onder meer staat dat een particuliere gebruiker te allen tijde beveiligingscodes geheim moet houden en zelf zorg moet dragen voor een goede beveiliging van de apparatuur die hij of zij gebruikt voor bankzaken.[3] De consument heeft gesteld dat twee factor-authenticatie onveilig is. De bank stelt dat zij dient te voldoen aan de vereisten van *Strong Customer Authentication (SCA)*, zoals opgenomen in de EU Richtlijn inzake de veiligheid van betaaldiensten (PSD2), en dat er geen sprake is van een twee factor authenticatie. Deze wetgeving verplicht de bank de identiteit van de klant bij het inloggen en autoriseren van betalingen te controleren. Hierbij controleert de bank twee van de volgende drie gegevens:

- *Iets wat alleen de klant weet en onthoudt, zoals een pincode of een browsercode*
- *Iets wat alleen de klant in bezit heeft, zoals een betaalpas of computer*

[1] Zie onder meer CvB Kifid nr. 2020-027 (overweging 5.14), te vinden op www.kifid.nl.
[2] Zie de Bijlagen bij deze uitspraak.
[3] Idem.

- *Iets wat alleen van de klant is en die kenmerkt, zoals een vingerafdruk*

Gebruikers van de bank kunnen betalingstransacties autoriseren met een browsercode; een persoonlijke en unieke code in combinatie met de browser en het apparaat van de gebruiker.

3.4 Op basis van de voornoemde bankadministratie (zie hiervoor onder 2.5) is naar het oordeel van de commissie voldoende vast komen te staan dat de zes frauduleuze transacties zijn verricht op de computer van de consument met behulp van haar browsercode (een beveiligingscode in de zin van de algemene voorwaarden). Er ontbreekt volgens de bank aan de zijde van de consument elke redelijke verklaring voor het feit dat zes frauduleuze transacties en twee interne overboekingen zijn verricht op de computer van de consument met haar browsercode. Daarnaast heeft zij te weinig inzicht gegeven in de wijze waarop de Mobiel Bankieren App van de bank en Apple Pay op een ander apparaat zijn geïnstalleerd met behulp van een code die exclusief naar haar telefoonnummer en e-mailadres zijn gestuurd en de daaropvolgende interne overboekingen.

3.5 Op de consument rust in dit kader een verzwaarde stelplicht. Zij moet de bank voldoende feitelijke gegevens aanreiken om het verwijt van grove nalatigheid te ontzenuwen. Hierbij gaat het om gegevens die zich in het domein van de consument bevinden. Als de consument geen verzwaarde stelplicht zou hebben, zou dat de bank voor onaanvaardbare risico's van misbruik plaatsen. In deze zaak betekent dit concreet dat de consument een zo goed mogelijke verklaring moet geven voor het feit dat de frauduleuze transacties op haar computer en met behulp van haar browsercode zijn verricht, alsmede voor het feit dat met behulp van een zescijferige code die alleen naar haar e-mailadres en telefoonnummer zijn gestuurd de Mobiel Bankieren App van de bank en Apple Pay op een ander apparaat geïnstalleerd zijn.

3.6 Naar het oordeel van de commissie heeft de consument, in het kader van haar verzwaarde stelplicht, onvoldoende inzicht gegeven in de wijze waarop cruciale gegevens in handen zijn gekomen bij de fraudeur. De consument heeft verklaard dat zij tijdens het telefoongesprek met de fraudeur op zijn verzoek heeft ingelogd in haar mailbox en bankomgeving en foto's van haar rijbewijs en gezicht heeft gemaakt en die heeft verstrekt aan de fraudeur. Zij heeft echter geen toereikende verklaring gegeven voor het feit dat de frauduleuze transacties op haar computer met behulp van haar browsercode zijn verricht. De enkele verklaring dat zij allerlei handelingen moest verrichten waarvan zij zelf niet meer precies weet wat deze inhielden, volstaat niet. Ook een verklaring voor het feit dat de Mobiel Bankieren App van de bank en Apple Pay op een ander apparaat zijn geïnstalleerd met behulp van een zescijferige code die alleen bij haar bekend kon zijn, heeft zij niet gegeven. Ten slotte heeft zij over Teamviewer (of andere software voor besturing van computers op afstand) en het gebruik daarvan wisselend verklaard, maar zich uiteindelijk op het standpunt gesteld dat zij de fraudeur met zekerheid *geen* toegang heeft gegeven tot haar computer via Teamviewer.

3.7 Dit leidt tot de conclusie dat de consument haar verplichtingen uit hoofde van artikel 7:524 BW niet is nagekomen en daarmee in juridische zin grof nalatig is geweest.

Geen recht op vergoeding van de schade op grond van het coulancekader

3.8 De consument heeft aangevoerd dat zij recht heeft op een coulancevergoeding. Voor zover zij daarmee een beroep doet op het coulancekader van de Nederlandse Vereniging van Banken[4], oordeelt de commissie dat het coulancekader niet van toepassing is op deze zaak, aangezien het coulancekader alleen ziet op toegestane betalingstransacties. In deze zaak draait het om schade die is voortgevloeid uit niet-toegestane betalingstransacties. Daarbij merkt de commissie ook op dat een vergoeding uit coulance niet juridisch afdwingbaar is.[5]

Conclusie

3.9 De commissie is op basis van het voorgaande van oordeel dat er voor de bank geen verplichting tot schadevergoeding bestaat.

4. De beslissing

De commissie wijst de vordering 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

[4] Bron: https://nvb.nl/media/4528/toetingscriteria-coulancekader-bij-spoofing-versie-2-juni-2021.pdf; zie ook GC Kifid nr. 2024-0864.
[5] Zie ook GC Kifid nr. 2024-0216 (overweging 3.2), te vinden op www.kifid.nl en Rechtbank Amsterdam 14 maart 2025, ECLI:NL:RBAMS:2025:1751, te vinden op www.rechtspraak.nl.

Bijlage - Relevante bepalingen uit wet- en regelgeving en de algemene voorwaarden

Boek 6 van het Burgerlijk Wetboek

Artikel 6:248 BW

1. *Een overeenkomst heeft niet alleen de door partijen overeengekomen rechtsgevolgen, maar ook die welke, naar aard van de overeenkomst, uit de wet, de gewoonte of de eisen van redelijkheid en billijkheid voortvloeien.*
2. *Een tussen partijen als gevolg van de overeenkomst geldende regel is niet van toepassing, voor zover dit in de gegeven omstandigheden naar maatstaven van redelijkheid en billijkheid onaanvaardbaar zou zijn.*

Voorwaarden ASN Online Bankieren

8.3.1. Houd je beveiligingscodes geheim

Denk hierbij aan het volgende:

- *Zorg ervoor dat je beveiligingscodes nooit bij een ander bekend worden.*
- *Beveiligingscodes zijn niet alleen de pincode die je in combinatie met je betaalpas gebruikt. Het zijn ook nadere codes die je moet gebruiken om elektronische betalingen te doen. Of de codes die je gebruikt voor internetbankieren en mobiele bankapps. Bijvoorbeeld (...) codes die je per sms of e-mail van ons krijgt. (...)*
- *Zorg ervoor dat niemand kan meekijken als je je beveiligingscodes intikt. Daarbij gaat het niet alleen om je pincode. Het geldt ook voor alle andere codes die je gebruikt om elektronische betalingen te doen. (...)*

8.3.3. Zorg voor een goede beveiliging van de apparatuur die je gebruikt voor je bankzaken.

Denk hierbij aan het volgende (...)

- *Zorg ervoor dat onze toepassingen op de apparatuur voor je bankzaken niet door onbevoegden gebruikt kunnen worden. Met toepassingen bedoen we bijvoorbeeld (...) de browsercode.*

8.3.5. Meld incidenten direct aan ons en volg onze aanwijzingen op

Neem in de volgende gevallen in elk geval meteen contact met ons op: (...)

- *Je weet of vermoedt dat iemand anders je beveiligingscode kent of heeft gebruikt.*
- *Je ziet dat er bedragen van je betaalrekening zijn afschreven waarvoor je geen toestemming hebt gegeven. (...)*
- *Als je iets vreemds of ongebruikelijks ziet.*