

## **Uitspraak Geschillencommissie Kifid nr. 2023-066 I**

(mr. dr. S.O.H. Bakkerus, voorzitter en mr. T. Veldhuizen, secretaris)

Datum uitspraak	25 augustus 2023
Klacht van	De consument
Tegen	ABN AMRO Bank N.V., gevestigd te Amsterdam, verder te noemen de bank
Aard uitspraak	Niet-bindend advies
Uitkomst	Vordering afgewezen
Bijlage	Relevante bepalingen uit wet- en regelgeving, de Algemene Voorwaarden en het Informatieblad Betaaldiensten Particulieren

### **Samenvatting**

Niet-toegestane betalingstransactie. Zorgplicht bank. Microsoft-fraude. De consument is benaderd door een persoon die zich heeft voorgedaan als een medewerker van Microsoft. Op verzoek van deze persoon heeft de consument die persoon via het programma 'TeamViewer' toegang gegeven tot zijn computer. Vervolgens is er zonder toestemming van de consument in totaal een bedrag van € 13.289,82 overgemaakt naar de bankrekening van een derde. De consument wil dat de bank zijn schade vergoedt. De commissie oordeelt dat de bank niet schadelijktig is. De coulanceregeling is niet van toepassing. De klacht is ongegrond en de vordering wordt afgewezen.

### **I. Procedure**

- I.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 reactie van de consument; 3) het verweerschrift van de bank; 4) de repliek van de consument; 5) de dupliek van de bank en 6) de aanvullende stukken van de consument.
- I.2 Partijen zijn opgeroepen voor een hoorzitting op 24 mei 2023. Op de hoorzitting was de consument aanwezig. Namens de bank waren aanwezig mevrouw [naam 1] en de heer mr. [naam 2].
- I.3 De consument heeft gekozen voor een niet-bindend advies. Dit betekent dat partijen elkaar niet aan de uitspraak kunnen houden.

## 2. Het geschil

*Wat is er gebeurd?*

- 2.1 De consument heeft een betaalrekening bij de bank. Op de overeenkomst tussen de consument en de bank zijn de Algemene Voorwaarden, de Voorwaarden Betaaldiensten Particulieren en het Informatieblad Betaaldiensten Particulieren van toepassing.
- 2.2 In april 2019 is de consument telefonisch benaderd door een persoon die zich voordeed als een medewerker van de fraudeafdeling van Microsoft. Volgens deze persoon zou de computer van de consument zijn gehackt. De consument heeft deze persoon via het computerprogramma 'Teamviewer' toegang gegeven tot zijn computer. Op 25 en 26 april 2019 hebben er vanaf de betaalrekening van de consument meerdere IDEAL-betalingen plaatsgevonden naar een bankrekening bij ING Bank voor in totaal € 13.289,82.
- 2.3 De consument heeft de bank op 24 november 2021 verzocht om vergoeding van € 13.289,92. De bank heeft het verzoek van de consument afgewezen. Verdere uitwisseling van standpunten tussen partijen in de interne klachtprocedure heeft niet geleid tot een oplossing van de klacht. Daarom heeft de consument de klacht bij Kifid ingediend.

*De klacht en vordering*

- 2.4 De consument is van mening dat de bank haar zorgplicht heeft geschonden en vordert vergoeding van € 13.289,83. Ter onderbouwing van zijn vordering voert de consument het volgende aan.
- 2.5 De consument heeft de fraudeur alleen toegang gegeven tot zijn computer. Op dat moment was de consument niet ingelogd in zijn internetbankieren. In het proces-verbaal is een verklaring van zijn zoon opgenomen dat de consument heeft ingelogd op internetbankieren terwijl hij de fraudeur aan de telefoon had. Dit klopt niet en zijn zoon was op dat moment niet aanwezig. Vervolgens zijn gedurende twee dagen meerdere betalingstransacties uitgevoerd zonder toestemming van de consument. Daarbij heeft de consument zijn betaalpas steeds in zijn bezit gehad en zijn pincode niet aan de fraudeur gegeven.
- 2.6 Nadat de consument de fraude had geconstateerd, is hij met zijn andere zoon naar een kantoor van de bank gegaan. De bank had volgens de consument meer kunnen doen om zijn geld terug te kunnen halen en heeft daarom zijn belangen onvoldoende behartigd. Als de bank navraag had gedaan bij de andere bank, zou het mogelijk zijn geweest om de persoonsgegevens van de fraudeur te achterhalen.

Doordat de bank dit niet heeft gedaan, is zij nalatig geweest, aldus de consument. Ook heeft de bank in een eerder soortgelijk geval de bank de schade vergoed uit coulance.

*Het verweer*

2.7 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**

*Inleiding*

3.1 De commissie moet beoordelen of de schade van € 13.289,83 moet vergoeden. De commissie beantwoordt deze vraag ontkennend en zij licht dit hierna toe.

*Wat is het beoordelingskader?*

3.2 Een betaaldienstverlener, in dit geval de bank, voert een betalingstransactie alleen uit als de betaler, in dit geval de consument, met de uitvoering van de betaalopdracht heeft ingestemd (zie artikel 7:522 lid 1 Burgerlijk Wetboek (BW)). In die situatie is sprake van een toegestane betalingstransactie.

3.3 Een zonder instemming van de betaler uitgevoerde betaalopdracht wordt beschouwd als een niet-toegestane betaling. Voor die situatie schrijft de wet voor dat de betaaldienstverlener het bedrag van de niet-toegestane betalingstransactie onmiddellijk terugbetaalt en, in voorkomend geval, de betaalrekening van de betaler herstelt in de toestand zoals die geweest zou zijn indien de niet-toegestane betalingstransactie niet had plaatsgevonden (zie artikel 7:528 lid 1 en lid 2 BW). Maar de betaler moet zelf alle verliezen uit niet-toegestane betalingstransacties dragen, als die betalingstransacties zich hebben voorgedaan doordat hij met grove nalatigheid één of meer verplichtingen uit artikel 7:524 BW niet is nagekomen (zie artikel 7:529 lid 1 BW). Dit artikel verplicht de betaler het betaalinstrument overeenkomstig de voorwaarden te gebruiken.

*De bank is niet schadeplichtig*

3.4 Het is onduidelijk of de betalingstransacties waar het in deze zaak om gaat, toegestane dan wel niet-toegestane betalingstransacties zijn. De consument stelt dat sprake is van niet-toegestane betalingstransacties, omdat hij daarmee niet heeft ingestemd. In die situatie is het dan aan de bank om te bewijzen dat sprake is van betalingstransacties met instemming van de consument. De betalingstransacties zijn volgens de bank geaccordeerd met de e.dentifier, betaalpas, pincode en responscode. Dat bewijs heeft de bank naar het oordeel van de commissie echter niet geleverd, zodat de commissie ervan uitgaat dat sprake is van niet-toegestane betalingstransacties.

- 3.5 Maar de bank voert als aanvullend verweer aan dat de consument grove nalatigheid kan worden verweten omdat hij zich niet heeft gehouden aan de veiligheidsregels. Alhoewel het aan de bank is om te stellen en – bij gemotiveerde betwisting – te bewijzen dat sprake is van grove nalatigheid door de consument, rust op de consument een ‘verzwaarde motiveringsplicht’. Een andere regel zou de bank voor onaanvaardbare risico’s van misbruik plaatsen.<sup>1</sup> Dat betekent dat de consument ten minste enig inzicht dient te geven in de wijze waarop de fraudeur op afstand de betalingstransacties heeft kunnen uitvoeren. De consument kan niet volstaan met de stelling dat hij dat niet weet.<sup>2</sup>
- 3.6 De commissie overweegt als volgt. Uit het dossier blijkt dat de consument de fraudeur toegang heeft gegeven tot zijn computer via het programma ‘TeamViewer’. Hoewel de consument betwist dat hij daarna heeft ingelogd op zijn internetbankieren, is dit wel opgenomen in het proces-verbaal. De consument heeft daarnaast geen verklaring gegeven voor de omstandigheid dat de fraudeur op afstand de betalingstransacties heeft kunnen uitvoeren met IDEAL, terwijl hij stelt dat hij altijd in het bezit is geweest van zijn betaalpas en zijn pincode niet aan derden heeft verstrekt.
- 3.7 Naar het oordeel van de commissie is daarmee voldoende aannemelijk geworden dat de consument in strijd heeft gehandeld met de veiligheidsregels in artikel 21 van de Algemene Voorwaarden en het Informatieblad Betaaldiensten Particulieren (zie bijlage), door zijn vertrouwelijke codes met de fraudeur te delen doordat deze via het programma ‘TeamViewer’ toegang had tot de computer van de consument. Dit leidt tot het oordeel dat moet worden aangenomen dat de consument met grove nalatigheid een of meer verplichtingen van de veiligheidsregels niet is nagekomen en derhalve, in de betekenis die de wet daaraan geeft, ‘grov nalatig’ is geweest. Dat betekent dat de commissie een juridisch oordeel geeft en dus geen moreel waardeoordeel over de handelwijze van de consument.
- 3.8 De wet biedt de ruimte om de aansprakelijkheid van de consument te beperken als de specifieke omstandigheden van het geval daartoe aanleiding geven (zie artikel 7:529 lid 2 BW) (zie bijlage). De commissie oordeelt dat in deze zaak niet is gebleken dat er sprake is van specifieke omstandigheden die aanleiding geven om de aansprakelijkheid van de consument op grond van artikel 7:529 lid 2 BW te beperken. De bank is daarom niet gehouden om enige schade van de consument te vergoeden.

---

<sup>1</sup> Zie bijvoorbeeld GC Kifid nrs. 2017-606, 2019-733, 2021-0265 en 2023-0531, 2023-0597, te vinden op [www.kifid.nl](http://www.kifid.nl).

<sup>2</sup> Zie bijvoorbeeld ook GC Kifid 2022-0935, overweging 3.9, te vinden op [www.kifid.nl](http://www.kifid.nl).

*De bank heeft zijn zorgplicht niet geschonden*

3.9 De commissie stelt voorop dat de maatschappelijke functie van de bank een bijzondere zorgplicht meebrengt tegenover de consument, die in een contractuele relatie tot de bank staat. De reikwijdte van de zorgplicht hangt af van alle omstandigheden van het geval. Kort gezegd houdt deze zorgplicht in dat de bank rekening dient te houden met de gerechtvaardigde belangen van de rekeninghouder.<sup>3</sup> Deze zorgplicht is ook opgenomen in artikel 2 van de Algemene Bankvoorwaarden 2017 (zie bijlage). De rol van de bank als betaaldienstverlener is in beginsel beperkt tot het optimaliseren van het betalingsverkeer. De op de bank rustende zorgplicht strekt in beginsel niet zo ver dat zij verplicht is om in het algemeen betalingstransacties te monitoren.<sup>4</sup> Ook is zij niet verplicht onderzoek te doen naar de begunstigde van een betaling.<sup>5</sup> Wel kan van de bank worden verwacht dat zij tot onderzoek zou overgaan indien zij op de hoogte was van ongebruikelijk betalingsverkeer, alsmede het daaraan verbonden gevaar. Bepalend is datgene waar de bank zich daadwerkelijk van bewust was.<sup>6</sup>

3.10 Naar het oordeel van de commissie heeft de bank haar zorgplicht niet geschonden. De commissie overweegt dat de bank enkel is opgetreden als betaaldienstverlener. Het is de commissie niet gebleken dat de bank zich daadwerkelijk bewust was van enig gevaar op het moment dat zij de betreffende betalingstransacties uitvoerde. Daar komt bij dat de bank ter zitting heeft aangegeven dat de consument in eerste instantie niet wilde geloven dat sprake was van fraude. De consument betwist dit niet. Daarnaast heeft de consument, voor zover bekend, de bank pas ruim tweeënhalf jaar na de frauduleuze betalingstransacties voor het eerst aangeschreven tot vergoeding van zijn geleden schade. Gelet op het voorgaande is geen sprake van een zorgplichtschending.

*De coulanceregeling is niet van toepassing*

3.11 Voor zover de consument een beroep doet op de coulanceregeling van de Nederlandse Vereniging van Banken met betrekking tot 'spoofing', overweegt de commissie als volgt. Eind 2020 hebben de vier grootbanken besloten tot de 'coulanceregeling', die inhoudt dat particuliere klanten die slachtoffer zijn geworden van bankhelpdeskfraude, ook wel 'spoofing' genoemd, in bepaalde gevallen hun schade vergoed krijgen. Aanleiding voor die beslissing was het feit dat er bij deze vorm van fraude misbruik wordt gemaakt van het vertrouwen dat klanten in hun (eigen) bank hebben doordat het telefoonnummer en/of de naam van de bank worden misbruikt.<sup>7</sup>

---

<sup>3</sup> Zie bijvoorbeeld GC Kifid 2023-0364, overweging 3.5, te vinden op [www.kifid.nl](http://www.kifid.nl).

<sup>4</sup> Zie bijvoorbeeld GC 2023-0364, overweging 3.5, te vinden op [www.kifid.nl](http://www.kifid.nl).

<sup>5</sup> Zie ook GC Kifid 2022-0490, overweging 3.6, te vinden op [www.kifid.nl](http://www.kifid.nl).

<sup>6</sup> HR 27 november 2015, ECLI:NL:HR:2015:3399, rechtsoverweging 4.6, te vinden op [www.rechtspraak.nl](http://www.rechtspraak.nl).

<sup>7</sup> Bron: <https://www.nvb.nl/nieuws/toetsingscriteria-voor-coulance-bij-bankhelpdesk-fraude-spoofing>, geraadpleegd op 10 augustus 2023.

De coulanceregeling definieert ‘spoofing’ als volgt:

*“(...) Bij bankhelpdesk fraude, ook wel spoofing genoemd, doet de crimineel zich voor als een medewerker van de bank van het slachtoffer. De crimineel misbruikt hiervoor de naam en/of telefoonnummer van de bank. De crimineel wint het vertrouwen van het slachtoffer en door de hoedanigheid van bankmedewerker aan te nemen haalt hij het slachtoffer over een betaling te doen naar een zogenaamd veilige rekening bij zijn of haar bank. (...)”*

- 3.12 Naar het oordeel van de commissie is de coulanceregeling, gelet op de definitie van spoofing, niet van toepassing op de situatie van de consument. In dit geval heeft de fraudeur zich niet voorgedaan als een medewerker van de bank van de consument, maar als een medewerker van Microsoft. Dit betekent dat niet is voldaan aan de vereisen van de coulanceregeling.

#### Conclusie

- 3.13 Het voorgaande leidt tot de conclusie dat de bank de schade van € 13.289,83 niet aan de consument hoeft te vergoeden. De klacht is ongegrond en zijn vordering wordt afgewezen.

## 4. De beslissing

De commissie wijst de vordering af.

*Deze uitspraak is niet-bindend. Tegen deze uitspraak staat geen beroep open bij de Commissie van Beroep Kifid. U kunt de zaak nog wel aan de rechter voorleggen.*

*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 2022, te vinden op de website [www.kifid.nl/reglementen-en-statuten](http://www.kifid.nl/reglementen-en-statuten).*

### Contactgegevens Klachteninstituut Financiële Dienstverlening

Telefoonnummer: 070 - 333 8 999

Website: [www.kifid.nl](http://www.kifid.nl)

## **Bijlage - Relevante bepalingen uit wet- en regelgeving, de Algemene Voorwaarden en het Informatieblad Betaaldiensten Particulieren**

### **Burgerlijk Wetboek**

#### **Artikel 7:522**

1. Een betaaldienstverlener voert een betalingstransactie slechts uit met instemming van de betaler met de uitvoering van de betaalopdracht.

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 7:524**

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. stelt de betaaldienstverlener, of de door laatstgenoemde gespecificeerde entiteit, onverwijld in kennis van het verlies, de diefstal of onrechtmatig gebruik van het betaalinstrument of van het niet-toegestane gebruik ervan.

2. Voor de toepassing van het eerste lid, onder a, neemt de betaaldienstgebruiker, zodra hij een betaalinstrument ontvangt, in het bijzonder alle redelijke maatregelen om de veiligheid van de persoonlijke beveiligingsgegevens ervan te waarborgen.

3. De voorwaarden bedoeld in het eerste lid, onderdeel a, zijn objectief, niet-discriminerend en evenredig.

#### **Artikel 7:528**

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.

2. Deze bepaling geldt onverminderd het recht op schadevergoeding uit hoofde van de algemene regels van overeenkomstenrecht.

#### **Artikel 7:529**

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.

2. In gevallen waarin de betaler, zonder frauduleus of opzettelijk te hebben gehandeld, zijn verplichtingen uit hoofde van artikel 524 niet is nagekomen, kan de rechter de in het eerste 8 lid van dit artikel bedoelde aansprakelijkheid beperken, met name rekening houdend met de aard van de persoonlijke beveiligingsgegevens van het betaalinstrument en met de omstandigheden waarin het is verloren, gestolen of onrechtmatig gebruikt. (...)

## **Algemene Voorwaarden - Algemene Bankvoorwaarden 2017**

### **Artikel 2 – Zorgplicht**

Wij hebben een zorgplicht. U bent ook zorgvuldig tegenover ons en u mag van onze dienstverlening geen misbruik maken.

1. Wij zijn bij onze dienstverlening zorgvuldig en houden hierbij zo goed mogelijk rekening met uw belangen. Dit doen wij op een manier die aansluit bij de aard van de dienstverlening. Deze belangrijke regel geldt altijd. Andere regels in de ABV of in de voor producten of diensten geldende overeenkomsten en de daarbij behorende bijzondere voorwaarden kunnen dit niet veranderen. Wij streven naar begrijpelijke producten en diensten. Ook streven wij naar begrijpelijke informatie over die producten en diensten en de risico's ervan. (...)

### **Artikel 21 – Bewaar- en geheimhoudingsplicht**

U gaat zorgvuldig om met codes, formulieren en passen. Als misbruik aannemelijk is, meldt u dit meteen.

1. U moet zorgvuldig en veilig omgaan met codes, formulieren, (bank)passen of andere hulpmiddelen. Zo helpt u voorkomen dat deze in verkeerde handen raken of dat iemand ervan misbruik kan maken.
2. Het kan gebeuren dat een code, formulier, (bank)pas, of ander hulpmiddel in verkeerde handen komt of dat iemand daarvan misbruik maakt of kan maken. Als u dit weet of redelijkerwijs kan vermoeden, meldt u dit meteen aan ons. Door uw melding kunnen wij proberen (verder) misbruik te voorkomen.
3. Houdt u er rekening mee dat wij nog andere veiligheidsregels stellen (zoals de Uniforme Veiligheidsregels Particulieren).

### **Informatieblad Betaaldiensten Particulieren**

In dit Informatieblad leest u meer regels en informatie over onderwerpen uit de:

- ▶ Algemene Voorwaarden ABN AMRO Bank N.V. (deze bestaan uit de Algemene Bankvoorwaarden en de Voorwaarden Cliëntrelatie).
- ▶ Voorwaarden Betaaldiensten Particulieren.

### **I. Veiligheid**

Naast de veiligheidsvoorschriften die staan in de Algemene Voorwaarden ABN AMRO Bank N.V. moet u zich houden aan de volgende veiligheidsregels.



## **IA Veiligheidsregels**

(...)

### **1. Houd uw beveiligingscodes geheim**

Denk hierbij aan het volgende:

- ▶ Zorg ervoor dat beveiligingscodes nooit aan een ander bekend kunnen worden.

Beveiligingscodes zijn niet alleen de pincode die u in combinatie met de (digitale) betaalpas gebruikt. Het zijn ook alle andere codes die u moet gebruiken om elektronische betalingen te doen en gebruik te maken van Internet Bankieren en mobiele bankapps. Dat kunnen bijvoorbeeld de codes zijn die een door de bank verstrekte codecalculator aangeeft (zoals de e.dentifier), codes die u via een mobiele bankapp en/of die u per SMS van uw bank ontvangt.

(...)

- ▶ U mag deze beveiligingscodes alleen zelf gebruiken.
- ▶ Geef nooit een beveiligingscode door per telefoon, e-mail of op een andere manier dan de bank heeft voorgeschreven. Dat geldt ook als u telefonisch, per e-mail of persoonlijk door iemand wordt benaderd die aangeeft medewerker van de bank of andere dienstverlener (zoals een computer-beveiligingsbedrijf) te zijn. De bank of andere dienstverleners zullen u op deze wijze nooit om beveiligingscodes vragen.
- ▶ Zorg ervoor dat niemand kan meekijken wanneer u uw beveiligingscodes intikt. Het gaat hier niet alleen om uw pincode maar ook om andere codes die u moet gebruiken om elektronische betalingen te doen en gebruik te maken van Internet Bankieren en Mobiel Bankieren.

(...)

### **3. Zorg voor een goede beveiliging van de apparatuur die u gebruikt voor uw bankzaken**

Denk hierbij aan het volgende:

- ▶ Zorg dat de geïnstalleerde software op de apparatuur (zoals computer, tablet en/of smartphone), die u gebruikt voor het regelen van uw bankzaken, is voorzien van actuele (beveiligings)updates. Geïnstalleerde software is bijvoorbeeld het besturingssysteem en beveiligingsprogramma's, zoals virusscanner en firewall.
- ▶ Installeer geen illegale software.
- ▶ Beveilig de toegang tot de apparatuur die u gebruikt voor het regelen van uw bankzaken met een toegangscode.
- ▶ Zorg er daarnaast voor dat door de bank verstrekte toepassingen op de apparatuur die u gebruikt voor het regelen van uw bankzaken niet door onbevoegden kunnen worden gebruikt.
- ▶ Log altijd uit wanneer u klaar bent met het regelen van uw bankzaken.