Uitspraak Geschillencommissie Kifid nr. 2025-0278

(mr. J. van der Groen, voorzitter en mr. R.E. van Lambalgen, secretaris)

Datum uitspraak	4 april 2025
Klacht van	De consument
Tegen	bunq B.V., gevestigd te Amsterdam, verder te noemen de bank
Aard uitspraak	Bindend advies
Uitkomst	Vordering afgewezen
Bijlage	Relevante bepalingen

Samenvatting

Niet-toegestane betalingstransacties. De consument is slachtoffer geworden van bankhelpdeskfraude. De consument stelt dat de bank onvoldoende veiligheidsmaatregelen heeft genomen, maar de commissie gaat daar niet in mee. Anders dan de consument meent, was er sprake van sterke cliëntauthenticatie. Verder is de commissie van oordeel dat de consument grof nalatig is geweest in de zin van artikel 7:529 lid 1 BW. De vordering tot schadevergoeding 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.

1.2 Op de hoorzitting was de consument aanwezig. Namens de bank waren aanwezig: mevrouw [naam 1] (Legal Officer bunq) en de heer [naam 2] (jurist).

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 hield bij de bank een betaalrekening en een spaarrekening aan (hierna tezamen aangeduid als 'bunq-account'). Hierop waren de Algemene Voorwaarden bunq Personal van toepassing (hierna: de algemene voorwaarden).

2.2 Op 14 april 2023 heeft de consument zijn iPhone gekoppeld aan zijn bunq-account.

2.3 Op 24 januari 2024 om 14:17 uur is de consument gebeld door iemand die zich voordeed als medewerker van ING. Op instructies van deze zogenaamde bankmedewerker heeft de consument Anydesk geïnstalleerd op zijn computer.

2.4 Op 24 januari 2024 om 14:22 uur is er een nieuw apparaat gekoppeld aan het bunq-account van de consument. Om een nieuw apparaat te koppelen, moet de QR-code op het nieuwe apparaat gescand worden met een al eerder gekoppeld apparaat. Uit de administratie van de bank blijkt dat de QR-code om 14:22 uur gescand is met de iPhone van de consument, waarna het nieuwe apparaat toegang heeft gekregen tot het bunq-account van de consument.

2.5 Op 24 januari 2024 om 14:58 uur is de zescijferige beveiligingscode ingevoerd in het bunq-account van de consument. Vervolgens is er tussen 14:58 en 15:05 uur met het nieuwe apparaat een aantal transacties verricht op de betaalrekening van de consument. Daarbij is in totaal € 12.557,- van de bunq-rekeningen van de consument afgeschreven. Een klein deel daarvan (€ 1.957,15) kon veiliggesteld worden.

De klacht en vordering

2.6 De consument vordert dat de bank zijn schade vergoedt. De consument betwist dat hij – zoals de bank aanvoert – grof nalatig is geweest. Hij vindt dat hij hooguit naïef is geweest door Anydesk te installeren op zijn computer. Verder stelt hij dat juist de bank nalatig is geweest: de bank heeft namelijk onvoldoende veiligheidsmaatregelen genomen om de fraude te voorkomen. Zo was er volgens hem geen sprake van sterke cliëntauthenticatie: het invoeren van de zescijferige beveiligingscode was voldoende. Volgens de consument hebben andere banken veel betere veiligheidsmaatregelen en had de fraude daarom alleen bij deze bank kunnen plaatsvinden.

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

3.1 De commissie stelt voorop dat zij het betreurt dat de consument slachtoffer is geworden van bankhelpdeskfraude en dat hij daardoor schade heeft geleden. De vraag is echter of de bank gehouden is het bedrag van de betwiste betalingstransacties (minus de veiliggestelde gelden) aan de consument te vergoeden.

Grof nalatig?

3.2 Tussen partijen is niet in geschil dat de consument niet heeft ingestemd met de betalingstransacties. Een transactie waarmee de betaler niet heeft ingestemd, wordt volgens artikel 7:522 lid 2 van het Burgerlijk Wetboek (BW) als niet-toegestaan aangemerkt. Bij niet-toegestane betalingstransacties moet de betaaldienstverlener op grond van artikel 7:528 lid 1 BW de betaler onmiddellijk het bedrag van de niet-toegestane betalingstransacties terugbetalen.

Op die regel bestaat een uitzondering: volgens artikel 7:529 lid 1 BW hoeft de betaaldienstverlener de niet-toegestane betalingstransacties niet terug te betalen als de betaler frauduleus heeft gehandeld of in juridische zin opzettelijk of met grove nalatigheid één of meer verplichtingen uit hoofde van artikel 7:524 BW niet is nagekomen. Op grond van artikel 7:524 BW moet de consument zich houden aan de veiligheidsregels die de bank stelt. Die veiligheidsregels houden onder meer in dat de consument inlogcodes en andere beveiligingscodes strikt geheim moet houden.[1]

3.3 De vraag is of de consument – in juridische zin – grof nalatig heeft gehandeld met betrekking tot het naleven van de veiligheidsregels. Hoewel het aan de bank is om te stellen en – na gemotiveerde betwisting door de consument – te bewijzen dat sprake is van grove nalatigheid aan de zijde van de consument, rust op de consument een verzwaarde motiveringsplicht.[2] Dat betekent dat de consument tenminste enig inzicht dient te geven in de wijze waarop een onbevoegde derde de mogelijkheid heeft gehad om toegang te krijgen tot zijn bunq-account. Een andere regel zou de bank voor onaanvaardbare risico's van misbruik plaatsen.

3.4 Uit de administratie van de bank blijkt dat de betalingstransacties om 14:58 uur geautoriseerd zijn met de zescijferige code vanaf een apparaat dat om 14:22 uur aan het bunq-account gekoppeld was. Om de transacties te kunnen verrichten, moet de oplichter er dus in geslaagd zijn 1) om de zescijferige code te bemachtigen en 2) om een nieuw apparaat aan het bunq-account te koppelen.

3.5 Wat betreft het eerste punt heeft de consument aangegeven dat hij op instructie van de 'bankmedewerker' Anydesk heeft geïnstalleerd op zijn computer en dat hij met zijn zescijferige code is ingelogd op zijn bunq-account. Waarschijnlijk heeft de oplichter op die manier de zescijferige code weten te bemachtigen.

3.6 Wat betreft het tweede punt blijkt uit de administratie van de bank dat de QR-code op het nieuwe apparaat om 14:22 uur gescand is *met de iPhone van de consument* en dat het nieuwe apparaat daarmee toegang heeft gekregen tot het bunq-account van de consument. De consument betwist echter dat hij met zijn iPhone (die hij die middag al die tijd bij zich had) een QR-code heeft gescand. De commissie overweegt als volgt. Hoewel het aan de consument is om enig inzicht te geven in hoe zijn iPhone (feitelijk) gebruikt is voor het scannen van de QR-code, heeft de bank maar weinig moeite gedaan om toe te lichten hoe het (technisch) mogelijk is dat een QR-code op het ene apparaat gescand wordt door een ander apparaat, terwijl die apparaten niet fysiek bij elkaar in de buurt zijn.

---

[1] Meer in het bijzonder gaat het om artikel 40 van de algemene voorwaarden (zie de bijlage bij deze uitspraak). Voor de volledigheid merkt de commissie dat dit artikel de oneerlijkheidstoets van de Richtlijn oneerlijke bedingen doorstaat; vgl. GC Kifid nr. 2025-0026.

[2] Zie onder meer GC Kifid nr. 2019-308, 2019-733, 2022-0011 en 2022-0604.

Wellicht dat de QR-code op een of andere manier op het beeldscherm van de computer is geprojecteerd – de oplichter had immers via Anydesk toegang tot de computer van de consument – en dat de consument dit vervolgens met zijn iPhone gescand heeft. Voor de commissie blijft het enigszins onduidelijk *hoe* de iPhone van de consument precies gebruikt is voor het scannen van de QR-code op het nieuwe apparaat, maar wat wél duidelijk is, is *dat* de iPhone van de consument daarvoor gebruikt is (dat blijkt immers uit de administratie van de bank). De consument betwist weliswaar dat hij met zijn iPhone een QR-code heeft gescand, maar naar het oordeel van de commissie is deze 'blote' betwisting onvoldoende gemotiveerd (gelet op de verzwaarde motiveringsplicht die op de consument rust).

3.7 Dit alles leidt tot het oordeel dat moet worden aangenomen dat de consument de verplichtingen voor het veilige gebruik van zijn bunq-account niet is nagekomen. De commissie oordeelt daarom dat de consument in juridische zin grof nalatig heeft gehandeld en dat de bank de geleden schade op grond van artikel 7:529 lid 1 BW niet aan de consument hoeft te vergoeden.

3.8 Op grond van artikel 7:529 lid 2 BW kan de aansprakelijkheid van de consument worden beperkt als de omstandigheden van het geval daartoe aanleiding geven. De commissie ziet in dit geval geen aanleiding om van die mogelijkheid gebruik te maken.

Onvoldoende veiligheidsmaatregelen?

3.9 Vervolgens is de vraag aan de orde of de bank – zoals de consument stelt – onvoldoende veiligheidsmaatregelen heeft genomen om de fraude te voorkomen.

3.10 In de eerste plaats stelt de consument dat er geen sprake was van sterke cliëntauthenticatie. De commissie gaat daar niet in mee. Sterke cliëntauthenticatie is authenticatie met gebruikmaking van twee (of meer) van de volgende factoren: 1) 'kennis': iets wat alleen de gebruiker weet, zoals een pincode of wachtwoord, 2) 'bezit': iets wat alleen de gebruiker heeft, zoals een pinpas of een aan de rekening gekoppelde smartphone; 3) 'inherente eigenschap': iets wat de gebruiker is, zoals een gezichtsscan of een vingerafdruk ('biometrische authenticatie').[3] De consument lijkt te menen dat de zescijferige code (de factor 'kennis') voldoende was voor de oplichter om de betalingstransacties te kunnen verrichten. De transacties zijn evenwel verricht met een apparaat dat aan het bunq-account gekoppeld was (oftewel de factor 'bezit'). De bank heeft dus voor het verrichten van de betwiste transacties twee factoren verlangd – 'kennis' en 'bezit' – waardoor er sprake was van sterke cliëntauthenticatie.

[3] Zie artikel 7:514 onder ab BW. De juridische relevantie van sterke cliëntauthenticatie volgt uit artikel 7:529 lid 3 BW, waarin is bepaald dat de betaler (de consument) geen financiële verliezen draagt in het geval dat een betaaldienstverlener (de bank) geen sterke cliëntauthenticatie verlangt.

3.11 In de tweede plaats stelt de consument dat de oplichter binnen enkele minuten grote geldbedragen heeft kunnen overmaken zonder dat de bank deze opvallende transacties heeft opgemerkt. Verder wijst hij erop dat andere banken limieten hanteren (waarbij limietverhogingen pas na enige tijd ingaan) waardoor het niet mogelijk is om binnen enkele minuten grote geldbedragen over te maken. De commissie overweegt dat er op banken geen algemene transactiemonitoringsplicht rust[4] en dat er ook geen wettelijke verplichting voor banken is om limieten in te stellen. Op dit punt is van een tekortkoming van de bank dan ook geen sprake.

Slotsom

3.12 Dit alles leidt tot de slotsom dat de vordering van de consument moet worden afgewezen.

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 oktober 2023, 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] Zie onder meer GC Kifid nr. 2019-759 (overweging 4.3).

Bijlage - Relevante bepalingen uit de Algemene Voorwaarden bunq Personal

40. Algemene beveiliging van je account

Om je geld en je account veilig te houden, zullen we moeten samenwerken. Hieronder vind je hoe.

Neem alsjeblieft adequate maatregelen en span je naar beste kunnen in om ongewenste toegang tot en gebruik van je account te voorkomen. Doe alsjeblieft hetzelfde voor de informatie die je via onze diensten verzamelt. Om je op weg te helpen hebben wij veiligheidsvoorschriften opgesteld. Onderstaand de belangrijkste voorschriften:

- houd je inlogcodes en andere beveiligingsfeatures strikt geheim, deel ze niet met anderen en gebruik ze nooit ergens anders dan in de officiële bunq apps of in onze officiële web interface;
- zorg ervoor dat niemand anders dan jij je passen gebruikt;
- zorg ervoor dat je telefoon en je andere apparaten beveiligd zijn (stel in ieder geval een vorm van toegangsbeveiliging in, bijvoorbeeld een inlogcode);
- gebruik altijd de laatste versie van onze apps en zorg dat het besturingssysteem van al je apparaten up-to-date en in orde is (geen illegale software);
- wanneer je de bunq app of web interface in het openbaar gebruikt, kijk dan over je schouders om zeker te zijn dat er geen ongeautoriseerde mensen meekijken;
- controleer je account in ieder geval eens per twee weken;
- breng jezelf op de hoogte van veelvoorkomende (online) oplichtingspraktijken, zoals phishing;
- meld onregelmatigheden altijd direct en volg onze instructies.

Wij zullen nooit om jouw inlogcodes of andere zaken gerelateerd aan de beveiliging van je account vragen via de telefoon, email of WhatsApp. Mocht je berichten van ons ontvangen die je niet (helemaal) vertrouwt, neem dan alsjeblieft onmiddellijk contact met ons op via de support chat. Mocht je ooit berichten ontvangen van een verdacht telefoonnummer of e-mailadres die claimen van bunq te zijn, klik dan alsjeblieft niet op een link, verstrek geen persoonlijke informatie en deel geen inloggegevens via zo'n link en meld het onmiddellijk aan ons.

Wees je alsjeblieft bewust van phishing. Phishing betreft andere mensen die proberen om jouw inlogcodes of andere vertrouwelijke informatie te verkrijgen. Veelvoorkomende phishing manieren vinden plaats via online websites zoals Marktplaats, betreft personen die zich voordoen als medewerker van bunq of van een overheidsinstantie (zoals de Belastingdienst). Klik nooit op links die je niet herkent en vul nooit gegevens in op websites die je niet bekend voorkomen. Als je niet zeker weet of iemand je probeert te phishen, neem dan zo snel mogelijk contact met ons op zodat we je kunnen helpen.

Volg deze veiligheidsvoorschriften alsjeblieft te allen tijde. Kijk voor een volledig overzicht van onze voorschriften op Together. (...)