Uitspraak Geschillencommissie Kifid nr. 2025-0026

(mr. dr. D.P.C.M. Hellegers, voorzitter en mr. Y.A. Gottenbos, secretaris)

Datum uitspraak	13 januari 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 bepaling uit de algemene voorwaarden

Samenvatting

De consument is slachtoffer geworden van oplichting. Een derde heeft haar betaalpas toegevoegd aan een Apple Pay-wallet en betalingen verricht ten laste van haar rekening. De consument vordert vergoeding van de schade. De commissie overweegt dat de consument geen inzicht heeft gegeven in de wijze waarop een derde de beschikking over haar rekening heeft kunnen krijgen. Zij kan daarom niet anders dan concluderen dat de consument de veiligheidsvoorschriften met grove nalatigheid niet is nagekomen. 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; 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 heeft een rekening bij de bank met een bijbehorende betaalpas. Op de overeenkomst tussen de consument en de bank zijn de bunq Terms and Conditions (hierna: de algemene voorwaarden) van toepassing. De relevante bepaling uit de algemene voorwaarden zijn opgenomen in de bijlage bij deze uitspraak.

2.2 Op 24 juni 2024 is de betaalpas van de consument toegevoegd aan een nieuwe Apple Pay-wallet.

2.3 Op 26 juni 2024 zijn meerdere transacties verricht vanaf de rekening van de consument via Apple Pay. In totaal is een bedrag van € € 5.813,- afgeschreven.

2.4 Op 26 juni 2024 heeft de consument aangifte gedaan van fraude bij de politie in Portugal.

De klacht en vordering

2.5 De consument vordert een schadevergoeding van € 5.813,-. Aan deze vordering legt de consument – kort weergegeven – het volgende ten grondslag.

2.6 De consument heeft de transacties waar het in deze procedure over gaat niet geautoriseerd. De consument heeft direct nadat zij de transacties opmerkte contact opgenomen met de bank en haar rekening geblokkeerd. De bank heeft de consument niet geholpen en heeft de schade niet vergoed.

2.7 De consument heeft niet grof nalatig gehandeld. Zij heeft geen beveiligingscodes, wachtwoorden of andere gevoelige informatie met derden gedeeld. De telefoon en de betaalpas van de consument zijn niet uit haar bezit geweest. De consument kan geen verklaring geven hoe de fraude heeft plaatsgevonden, maar het is mogelijk dat geavanceerde phishing technieken of andere vormen van cyberaanvallen zijn gebruikt om toegang tot de rekening te krijgen.

2.8 De bank is verplicht om veiligheidsmaatregelen, zoals sterke cliëntauthenticatie, te nemen om fraude te voorkomen. Dat een fraudeur de betaalpas heeft kunnen toevoegen aan Apple Pay wijst op een mogelijk gat in de beveiliging van de bank en roept de vraag op of de bank haar verplichting om veiligheidsmaatregelen te nemen is nagekomen. De bank heeft op haar website gezet waarin de bank erkent dat Apple Pay mogelijk fraudegevoelig is. De bank geeft in het bericht aan dat bepaalde functies daarom worden geblokkeerd. Ook staan op een internetforum berichten over vergelijkbare gevallen waarbij Apple Pay is gebruikt om geld te stelen van mensen terwijl er geen beveiligingscodes zijn gedeeld.

Het verweer

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

3. De beoordeling

Waar het om gaat

3.1 De commissie merkt op dat zij het betreurt dat de consument slachtoffer is geworden van fraude en dat zij daardoor schade heeft geleden.

Dit staat evenwel los van de taak van de commissie om te onderzoeken of de bank juridisch gezien verplicht is de schade die zij heeft geleden te vergoeden. De commissie komt tot het oordeel dat de bank de schade niet hoeft te vergoeden en licht dat hieronder toe.

Grove nalatigheid

3.2 Tussen partijen is niet in geschil dat de consument niet heeft ingestemd met de betalingstransacties. Een transactie waarmee de consument niet heeft ingestemd, wordt volgens artikel 7:522 lid 2 van het Burgerlijk Wetboek (hierna: BW) als niet-toegestaan aangemerkt. Op grond van artikel 7:528 lid 1 BW moet een bank in geval van een niet-toegestane betalingstransactie de consumenten onmiddellijk het bedrag van de niet-toegestane betalingstransactie terugbetalen. Op die regel bestaat een uitzondering. Volgens artikel 7:529 lid 1 BW hoeft de bank de niet-toegestane betalingstransacties niet terug te betalen als de consument 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.[1] Volgens artikel 7:524 lid 1 BW moet de consument een betaalinstrument gebruiken overeenkomstig de voorwaarden die op het gebruik daarvan van toepassing zijn.

3.3 In artikel 43 van de algemene voorwaarden zijn bepalingen opgenomen die betrekking hebben op de veiligheid van de rekening. Daarin is onder meer opgenomen dat de consument inlogcodes en andere beveiligingscodes strikt geheim moet houden. De commissie moet beoordelen of de consument – in juridische zin – grof nalatig heeft gehandeld met betrekking tot het naleven van deze veiligheidsvoorschriften.

3.4 Hoewel het aan de bank is om te bewijzen dat de consument grof nalatig heeft gehandeld, rust op de consument een verzwaarde stelplicht.[2] Dat betekent dat de consument aanknopingspunten dient te verstrekken over de wijze waarop een onbevoegde derde de mogelijkheid heeft gehad om de betaalpas van de consument toe te voegen aan een Apple Pay-wallet. Een andere regel zou banken voor onaanvaardbare risico's van misbruik plaatsen.

3.5 De bank heeft toegelicht dat voor het koppelen van een betaalpas aan Apple Pay het nummer van de betaalpas en de verloopdatum van de pas moeten worden opgegeven. Om te verifiëren dat de consument instemt met het toevoegen van de betaalpas aan Apple Pay wordt per sms een verificatiecode gestuurd die moet worden ingevoerd op de iPhone waar de betaalpas aan wordt toegevoegd. Deze sms is verstuurd naar het bij de bank bekende telefoonnummer van de consument. De bank heeft dat onderbouwd door een log uit haar administratie te overleggen. In de sms staat dat de consument de verificatiecode niet mag delen met derden, aldus de bank.

[1] Commissie van Beroep, nr. 2020-027.
[2] Geschillencommissie Kifid, nrs. 2024-0124, 2019-308 en 2019-733.

3.6 De commissie is van oordeel dat de consument, gelet op de verzwaarde stelplicht, onvoldoende tegenover de toelichting van de bank heeft gesteld. De consument heeft verklaard dat zij het slachtoffer is geworden van fraude en dat er betalingstransacties zijn uitgevoerd waarvoor zij geen toestemming heeft gegeven. Zij heeft geen inzicht gegeven over de wijze waarop de gegevens van de betaalpas en de verificatiecode kennelijk in handen van een derde zijn gekomen. Hoe een derde haar betaalpas aan een Apple Pay-wallet kon toevoegen is onduidelijk gebleven. Zoals hiervoor is overwogen is het aan de consument om hier enig inzicht in te geven. Nu de consument dit niet heeft gedaan, kan de commissie niet anders dan concluderen dat de consument onvoldoende zorgvuldigheid heeft betracht waardoor de fraudeur in de gelegenheid is geweest om de betaalpas aan een Apple Pay-Wallet toe te voegen. Dit leidt tot het oordeel dat moet worden aangenomen dat de consument de verplichtingen voor het veilige gebruik van de rekening zoals opgenomen in de voorwaarden niet is nagekomen. Derhalve concludeert de commissie 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.

3.7 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.

Veiligheidsmaatregelen

3.8 De consument heeft gesteld dat de bank mogelijk onvoldoende veiligheidsmaatregelen, zoals sterke cliëntenauthenticatie, heeft genomen om de fraude te voorkomen. De commissie volgt de consument hierin niet en licht dit hierna toe.

3.9 In artikel 7:529 lid 3 is bepaald dat de betaler (de consument) geen financiële verliezen draag in het geval dat een betaaldienstverlener (de bank) geen sterke cliëntauthenticatie vraagt. Volgens artikel 7:514 onder ab BW is sprake van sterke cliëntauthenticatie op het moment dat in een authenticatieprocedure twee of meer onderling onafhankelijke factoren worden gebruikt zoals die in het artikel worden beschreven. In dit geval heeft de bank toegelicht dat voor het koppelen van een betaalpas aan Apple Pay het nummer van de betaalpas en de verloopdatum van de pas moeten worden opgegeven. Dit is factor I. Daarnaast wordt per sms een verificatiecode gestuurd die moet worden ingevoerd op de iPhone waar de betaalpas aan wordt toegevoegd. Dit is factor II. Volgens de bank is deze procedure bij het koppelen van de betaalpas aan Apple Pay op 24 juni 2024 vereist en doorlopen. De sms met verificatiecode is verstuurd naar het bij de bank bekende telefoon-nummer van de consument. De bank heeft dit onderbouwd door een log uit haar administratie te verstrekken. De commissie is van oordeel dat de bank hiermee voldoende heeft onderbouwd dat zij op 24 juni 2024 sterke cliëntauthenticatie heeft verlangd in de zin van artikel 7:529 lid 3 BW voor het gebruik van de rekening.

3.10 De consument heeft aangevoerd dat op een internetforum berichten staan over vergelijkbare gevallen waarbij Apple Pay is gebruikt om geld te stelen van mensen terwijl er geen beveiligingscodes zijn gedeeld. De consument heeft schermuitdraaien van deze berichten verstrekt. De commissie kan op basis van deze berichten niet vaststellen hoe de fraude in de gevallen van de berichten precies heeft plaatsgevonden, of in die gevallen de bank (of andere banken) onvoldoende veiligheidsmaatregelen heeft genomen en of de bank ook in het geval van de consument onvoldoende veiligheidsmaatregelen heeft genomen. De commissie concludeert dat niet is komen vast te staan dat de bank in dit geval onvoldoende veiligheidsmaatregelen heeft genomen om de fraude te voorkomen.

De bank hoefde het geld niet terug te halen

3.11 Voor zover de consument stelt dat de bank een actie had moeten ondernemen om het geld terug te halen, overweegt de commissie het volgende. Het is niet gebleken dat de bank het geld had kunnen terughalen op het moment dat de consument voor het eerst contact opnam met de bank over de transacties. De commissie merkt daarbij op dat de bank niet de bevoegdheid heeft om eigenhandig onterechte betalingen terug te draaien.[3]

Conclusie

3.12 De conclusie is dat de klacht van de consument ongegrond is. De vordering wordt dan ook afgewezen.

Ambtshalve toetsing

3.13 Voor de beoordeling van de klacht is artikel 43 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 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.

[3] Hof 's-Hertogenbosch 19 juni 2012, ECLI:NL:GHSHE:2012:bw9175.

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 wet- en regelgeving en uit de algemene voorwaarden

43. General account security

To keep your money and your account safe, we need to work together, here's how.
Please take adequate measures and use best efforts to prevent unauthorized access/use of your account and the information you collect via our services.

To help you keep your account secure, we have made some safety guidelines, stated below are the most important ones you need to follow at all times:
- keep your login codes and other security features strictly to yourself, do not share them with anyone else and never use them anywhere but in our official apps or in our official web interface;
- make sure that your cards are not used by anyone else but you;
- make sure all your devices are properly protected (set at least one form of access protection, for example a login code);
- use the latest versions of our apps and keep the operating systems of your devices clean (no illegal software) and up-to-date;
- when using the de bank app or web interface in a public place, look over your shoulder to make sure that no unauthorized person is peeking;
- check your account at least once every two weeks;
- inform yourself about common (online) scams, such as phishing;
- always immediately report irregularities and follow our instructions.

We will never ask you for your login codes or other security features via phone, email or Whatsapp. If you receive any communication from us that you do not (completely) trust, please contact us via the support chat immediately. If you receive any communication from a suspicious phone number or email address claiming to be from us, please do not click on any links or provide any personal information or your de bank credentials via such links and immediately report it to us.

Please be aware of phishing. Phishing involves other people trying to obtain your security credentials. Common phishing scams involve online websites such as Marktplaats or involve persons purporting to be from de bank or from a governmental institution (such as the Tax Authorities). Never click on links you don't recognize and never enter your information on websites that you're not familiar with. If you're unsure whether or not someone is trying to phish you, contact us at the soonest opportunity and we'll assist you.

For the (additional) security guidelines for using de bank cards, please see the security section in the de bank card rules.

Because of the applicable laws and regulations, we need to know who uses our services. This means we need to identify you when you open your account and that your account is personal, so please only use it (for) yourself. You may authorise another person to use your account on your behalf. However, please do not allow another person to use your account on his/her or someone else's behalf. Please remember that you remain responsible for any (unlawful) use of your account if you do so.

As part of our due diligence, we are required to investigate unusual (transaction) behaviour. You're obligated to cooperate in these investigations and we expect you to provide us with any relevant information we require. A refusal to cooperate could ultimately lead to the closure of your account.