Uitspraak Geschillencommissie Kifid nr. 2024-0954

(mr. J. van der Groen, voorzitter en mr. J. Hadziosmanovic, secretaris)

Datum uitspraak	4 november 2024
Klacht van	De consument
Tegen	Coöperatieve Rabobank U.A., gevestigd te Amsterdam, verder te noemen de bank
Aard uitspraak	Niet-bindend advies
Uitkomst	Vordering afgewezen

Samenvatting

De consument is opgelicht en daarbij is haar € 33.900,- afhandig gemaakt. De fraudeurs hebben zich onder meer voorgedaan als een medewerker van de bank en hebben haar ertoe bewogen om meekijkprogramma's op haar computer en mobiele telefoon te installeren en om haar mobiele telefoon en bankpas af te geven, waarna de fraudeurs (gelden van haar rekening hebben overgeboekt. De consument stelt de bank aansprakelijk voor het geleden verlies en verzoekt om vergoeding op grond van de coulanceregeling. De bank heeft zich verweerd en het verzoek van de consument afgewezen. De commissie oordeelt in lijn met eerdere uitspraken dat het coulancekader in dit geval niet van toepassing is, dat sprake is van grove nalatigheid in juridische zin aan de zijde van de consument en dat de bank niet de op haar rustende zorgplicht heeft geschonden. De vordering is 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) het verweerschrift van de bank; 3) de repliek van de consument en 4) de dupliek van de bank.

1.2 De consument is in deze zaak vertegenwoordigd door mr. P.F.M. Deijkers, advocaat, kantoorhoudende te Hoorn. De bank is vertegenwoordigd door mr. I.H.C. Jans, advocaat, kantoorhoudende te Eindhoven.

1.3 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.

1.4 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 houdt twee betaalrekeningen aan bij de bank met daaraan gekoppeld een bankpas met pincode, internetbankieren, mobielbankieren en een Raboscanner. Op haar rekeningen bij de bank zijn de Algemene Bankvoorwaarden (ABV) en de Voorwaarden betalen en online diensten van de Rabobank 2022 (AV 2022) van toepassing verklaard.[1] Daarnaast heeft de consument de volmacht over de bankrekening van een derde bij een andere bank. Zij heeft via het mobielbankieren en internetbankieren ook toegang tot deze rekening.

2.2 Tussen 20 en 25 april 2023 is de consument meermaals gebeld door fraudeurs die zich hebben voorgedaan als: medewerker van de bank; medeweker van de andere bank waar de consument als gevolmachtigde staat ingeschreven en als IT-consultant. De fraudeurs hebben de consument ervan overtuigd dat zich virussen bevonden op haar apparatuur; er een andere computer was gekoppeld aan haar internetbankieren en dat er transacties naar het buitenland werden klaargezet vanaf haar betaalrekening. De fraudeurs hebben de consument bewogen tot het installeren van Anydesk op haar computer en de Quicksupport App op haar mobiele telefoon. Vervolgens is de consument bewogen tot het afgeven van haar mobiele telefoon en haar bankpas aan de deur.

2.3 Op 25 april 2023 is vanaf de betaalrekening van de consument bij de bank in 13 transacties een bedrag van totaal € 33.900,- overgemaakt naar de betaalrekening bij de andere bank waartoe zij gevolmachtigd is. Vandaaruit is het bedrag in meerdere transacties overgeboekt naar een bankrekening van een derde.

2.4 De consument is de volgende dag bekend geraakt met het verlies van haar gelden en zij heeft contact opgenomen met de bank. Vervolgens heeft zij aangifte gedaan bij de politie. De aangifte maakt onderdeel uit van het dossier.

2.5 De consument heeft de bank aangesproken voor de schade die zij heeft geleden en verzocht om vergoeding op grond van de NVB (Nederlandse Verenging van Banken) coulanceregeling voor spoofingfraude. De bank heeft daar afwijzend op gereageerd. Een nadere uitwisseling van standpunten tussen partijen heeft niet tot een oplossing van het geschil geleid waarna de consument een klacht bij Kifid heeft ingediend.

[1] Alle in deze uitspraak genoemde bedingen, wet- en regelgeving staan opgenomen in de bijlage bij de uitspraak.

De klacht en vordering van de consument

2.6 De consument vordert een vergoeding van € 33.900,-. Daartoe heeft zij, kort en zakelijk weergegeven, het volgende aangevoerd.

2.7 De consument is gebeld door iemand die zich voordeed als medewerker van de bank. De fraudeur heeft haar vertrouwen ingewonnen. Door hem is ze doorverbonden met andere 'medewerkers'. De fraudeurs hebben haar overgehaald om haar bankbescheiden af te geven, althans handelingen te verrichten die in haar nadeel zijn geweest. Het is voor de consument niet exact vast te stellen hoe de fraudeurs aan haar geheime codes zijn gekomen. De consument heeft haar geheime (inlog)codes in ieder geval niet vrijwillig of bewust aan de fraudeurs verstrekt. De fraudeurs moeten deze hebben achterhaald nadat de consument op hun verzoek meekijkprogramma's heeft geïnstalleerd op haar computer en mobiele telefoon. De fraudeurs hebben mee kunnen kijken terwijl de consument inlogde in haar online bankomgevingen. De fraudeurs haar hadden wijsgemaakt dat haar apparatuur veel virussen had. De consument dacht daarom dat het om antivirusprogramma's ging.

2.8 De consument heeft hoe dan ook niet ingestemd met de transacties zodat sprake is van niet-toegestane transacties. De bank dient haar op grond van de relevante wetgeving daarom het bedrag terug te betalen. Er is geen sprake van grove nalatigheid aan de zijde van de consument omdat zij de veiligheidsvoorschriften, naar omstandigheden, zo volledig mogelijk heeft nageleefd. Ook heeft de consument het incident direct bij de bank gemeld.

2.9 Het is voor de consument verder niet te bevatten dat de frauduleuze transacties niet door de bank zijn gedetecteerd. Het monitoringssysteem van de bank had deze ongebruikelijke dan wel verdachte transacties, met name gelet op de hoeveelheid transacties, moeten opmerken en de bank had moeten ingrijpen. De bank heeft eerder ingegrepen en een transactie van haar rekening naar haar volmacht rekening geblokkeerd welke niet verdacht was, waarom deze transacties dan niet.

2.10 Bovendien dient de bank de schade van de consument te vergoeden op basis van de coulanceregeling. De consument voldoet aan de daarvoor gestelde criteria.

Het verweer van de bank

2.11 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 ziet zich voor de vraag gesteld of de bank gehouden kan worden het door de consument aan fraude verloren bedrag van € 33.900,- te vergoeden. De commissie is van oordeel dat dit niet het geval is en zij licht haar oordeel hierna toe.

De coulanceregeling is niet van toepassing

3.2 Het standpunt van de bank dat het coulancekader hier niet van toepassing is, is naar het oordeel van de commissie juist. Het coulancekader biedt namelijk, onder voorwaarden, een vergoeding in geval van bankhelpdeskfraude die als volgt is gedefinieerd:

Bij bankhelpdeskfraude, 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.

3.3 In het onderhavige geval staat vast dat de transacties van de rekeningen van de consument zijn verricht door de fraudeur nadat hij de beschikking heeft gekregen over haar rekeningen. Dit betekent dat (strikt genomen) geen sprake is van bankhelpdeskfraude, zoals gedefinieerd in het coulancekader, omdat de consument niet is overgehaald om zelf een betaling te doen naar een zogenaamd veilige rekening.[2] Daarmee is in elk geval aan één van de voorwaarden van het coulancekader niet voldaan en is deze niet van toepassing op de consument in relatie tot de bank. Het voorgaande leidt ertoe dat de bank niet gehouden is om de schade van de consument op grond van het coulancekader te vergoeden. De commissie merkt in dit kader op dat het niet aan haar is om het toetsingskader van de coulanceregeling op te rekken, gelet op de aard daarvan.[3]

Er is sprake van grove nalatigheid in juridische zin

3.4 De commissie gaat over tot beoordeling van de klacht op grond het relevante juridische kader dat volgt uit het Burgerlijk Wetboek (hierna: BW). De wet maakt een onderscheid tussen toegestane en niet-toegestane betalingstransacties. Vooropgesteld moet worden dat de consument niet heeft ingestemd met de transacties ten bedrage van € 33.900,-.[4] Dit is tussen partijen ook niet in geschil. De hoofdregel bij niet-toegestane betalings-transacties is dat de bank het bedrag van de niet-toegestane betalingstransactie moet terugbetalen aan de consument, tenzij de consument frauduleus heeft gehandeld dan wel opzettelijk of met grove nalatigheid één of meer verplichtingen uit hoofde van artikel 7:524 BW niet is nagekomen.[5] Of de consument in dit geval grof nalatig is geweest, beoordeelt de commissie aan de hand van de vraag of sprake is van 'aan opzet grenzende schuld'.[6] De bewijslast van grove nalatigheid rust op de bank.[7]

---

[2] Zie ook GC nr. 2024-0015.
[3] Zie ook GC Kifid nrs. 2024-0586, 2023-0897, 2023-0171, 2022-0935 en 2022-0953.
[4] Zie artikel 7:522 lid 2 BW.
[5] Zie Hoge Raad 21 mei 2021, ECLI:NL:HR:2021:749, r.o. 3.2.2.
[6] Zie GC Kifid nr. 2023-0779 onder 3.8.
[7] Zie CvB Kifid nr. 2020-027.

3.5 Volgens artikel 7:524 lid 1 BW moet de consument de betaalinstrumenten gebruiken overeenkomstig de voorwaarden die op het gebruik van toepassing zijn. In hoofdstuk 2 van de AV van de bank zijn bepalingen opgenomen die betrekking hebben op de veiligheid van de betaalrekening. Daarin is onder meer opgenomen dat (1) beveiligingscodes, zoals de pincode, geheimgehouden moeten worden, ook voor de bank, (2) betaalpassen nooit door iemand anders gebruikt mogen worden, (3) rekeningen zo spoedig mogelijk gecontroleerd moeten worden op transacties waarvoor geen toestemming is gegeven, (4) apparatuur waarop bankzaken worden gedaan goed beveiligd moet zijn zodat onbevoegden er geen gebruik van kunnen maken en (5) incidenten direct gemeld moeten worden bij de bank.

3.6 De bank heeft in dit kader gesteld dat de consument urenlang telefonisch heeft gesproken met de fraudeurs. De fraudeurs hebben daarbij het telefoonnummer van Interpolis misbruikt en zij hebben zich voorgedaan als: een medewerker van de bank, een medewerker van de andere bank waar de consument gevolmachtigd is tot een betaalrekening, en als IT-consultant. De consument heeft zich vervolgens niet aan de veiligheidsregels gehouden door, in opdracht van de fraudeurs, meekijkprogramma's te installeren op haar computer en mobiele telefoon en in te loggen in haar online bankomgeving. Tot slot heeft zij op verzoek van de fraudeurs haar mobiele telefoon en haar bankpas afgegeven aan de deur. Daarna hebben de fraudeurs transacties vanaf haar betaalrekeningen uitgevoerd volgens de tussen de bank en de consument overeengekomen procedure. Hiervoor is door de fraudeurs gebruik gemaakt van het mobielbankieren van de consument, haar bankpas, de bijbehorende pincode en een Raboscanner. Zonder deze bankbescheiden, inlogcodes en pincode hadden de transacties niet kunnen plaatsvinden. De consument moet aldus haar geheime codes hebben afgegeven. De consument had alert moeten zijn. De bank waarschuwt immers via diverse kanalen voor diverse vormen van fraude. Ook heeft de consument de twijfels die haar echtgenoot uitte over de verzoeken van de fraudeurs weggewuifd.

3.7 De consument heeft hier tegenin gebracht dat zij zich niet bewust is geweest van de oplichting en te goeder trouw heeft gehandeld, nadat de fraudeur die zich voordeed als medewerker van de bank haar vertrouwen had ingewonnen. De consument heeft de veiligheidsvoorschriften, naar omstandigheden, zo volledig mogelijk nageleefd en direct na het ontdekken van de fraude contact opgenomen met de bank. De consument heeft de fraude als zeer traumatisch ervaren.

3.8 De commissie betreurt het dat de consument slachtoffer is geworden van fraude. De bank kan echter niet gehouden worden om haar schade te vergoeden. De commissie is van oordeel dat de consument, in juridische zin, grof nalatig heeft gehandeld. Hiervoor is redengevend dat de consument zeer ongebruikelijke en risicovolle handelingen in opdracht van de fraudeurs heeft verricht, zonder daarbij contact met de bank te zoeken.

Zo volgt uit het dossier dat de consument lange tijd telefonisch contact heeft gehad met iemand die zich eerst voordeed als medewerker van de bank en deze, nadat de consument informatie had gegeven over haar bankzaken, haar doorverbond met iemand die zich voordeed als medewerker van de andere bank waar zij als gevolmachtigde de beschikking had over een betaalrekening van een derde, en nadien ook als iemand die zich voordeed als IT-consultant. De fraudeurs hebben haar overgehaald om meekijkprogramma's te installeren op haar computer en mobiele telefoon, en om vervolgens in te loggen in haar online bankomgeving. Daarna hebben ze haar overgehaald om haar mobiele telefoon en bankpas af te geven aan de deur.

3.9 De commissie concludeert hieruit dat de consument de fraudeurs in staat heeft gesteld om haar geheime inlogcodes en pincode te achterhalen en te beschikken over haar bankrekeningen. De consument zal daarom zelf de verliezen moeten dragen als gevolg daarvan.

De bank heeft niet de op haar rustende zorgplicht geschonden door de transacties niet tegen te houden

3.10 Op de bank rust een bijzondere zorgplicht, welke kort gezegd inhoudt dat de bank rekening dient te houden met de gerechtvaardigde belangen van de rekeninghouder. De reikwijdte van de zorgplicht hangt af van de omstandigheden van het geval. Volgens de vaste lijn van de commissie mag van de bank worden verwacht dat zij zich redelijkerwijs inspant om fraude en misbruik van het betalingsverkeer te voorkomen.[8] Deze zorgplicht strekt echter niet zo ver dat de bank gehouden is om in het algemeen betalingstransacties te monitoren. Een algemene monitoringsverplichting zou het proces van geautomatiseerde gegevens-verwerking en het maatschappelijk belang dat daarmee gediend is, kunnen schaden. Wel kan van de bank worden verwacht dat zij tot onderzoek overgaat indien zij weet van ongebruikelijk betalingsverkeer en van het daaraan verbonden gevaar. Bepalend is datgene waarvan de bank zich daadwerkelijk bewust was.[9]

3.11 In deze zaak is niet gebleken dat de bank ten tijde van de uitvoering van de transacties wetenschap had van ongebruikelijk betalingsverkeer of van omstandigheden die een risico voor de consument meebrachten. De bank heeft onweersproken gesteld dat er geen alerts zijn afgegaan. De consument heeft naar het oordeel van de commissie ook onvoldoende duidelijk gemaakt waarom de bank de betreffende overboekingen had moeten detecteren. Het enkele feit dat het gaat om meerdere betalingen en dat de consument niet eerder bedragen naar deze partij heeft overgemaakt, is onvoldoende om aan te nemen dat de bank deze betalingen als frauduleus had moeten detecteren. Dat de bank eerder een transactie heeft tegengehouden maakt dat niet anders.

[8] Zie GC Kifid nr. 2016-602.
[9] Zie Hoge Raad 27 november 2015, ECLI:NL:HR:2015:3399.

Ambtshalve toetsing

3.12 Voor de beoordeling van de klacht zijn de Uniforme veiligheidsregels in hoofdstuk 2 van de AV 2022 getoetst aan het Europese en Nederlandse (consumenten)recht waarvoor ambtshalve toetsing geldt en de commissie acht deze bedingen niet in strijd met deze regelgeving.

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 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 de Algemene Voorwaarden

Relevante artikelen uit de Voorwaarden betalen en online diensten van de Rabobank 2022 (AV 2022)

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 en toegangscode van het apparaat met een digitale pas die u in combinatie met de betaalpas, creditcard of digitale pas gebruikt. Het zijn ook alle andere codes die u moet gebruiken om elektronisch betaalopdrachten te geven en/of gebruik te maken van Rabo Online Bankieren en Rabofoon. Bijvoorbeeld de inlogcode/I-code en signeercode/S-code, die u aanmaakt met een Rabo Scanner of Random Reader. En de 5-cijferige code, het patroon van uw smartphone, het wachtwoord of de toegangscode van uw smartphone en de 3-cijferige code achterop uw creditcard of betaalpas (de CVC-code of CVV-code).
• U mag deze beveiligingscodes alleen zelf gebruiken. U moet dat doen op de manier die wij aangeven. Meer informatie vindt u op rabobank.nl/veilig.
• Schrijf of sla de codes niet op. Of, als het echt niet anders kan, alleen in een voor anderen onherkenbare vorm die alleen door uzelf is te ontcijferen. Bewaar in dit geval de versleutelde informatie niet bij uw betaalpas, creditcard of digitale pas of apparatuur waarmee u uw bankzaken regelt.
• Als u zelf een beveiligingscode kunt kiezen, zorg dan dat die niet gemakkelijk te raden is. Kies bijvoorbeeld geen geboortejaar, naam van een familielid of postcode.
• Zorg ervoor dat niemand kan meekijken als u uw beveiligingscodes intoetst. Het gaat hier niet alleen om uw pincode en toegangscode van het apparaat met een digitale pas, maar ook om alle andere codes die u moet gebruiken om elektronische betalingen bijvoorbeeld met uw betaalpas, creditcard of digitale pas te doen en/of gebruik te maken van Rabo Online Bankieren en Rabofoon.
• Geef nooit een beveiligingscode door per telefoon, e-mail, op een website of in een app anders dan die van Rabobank, of op een andere wijze dan wij u hebben voorgeschreven. Dat geldt ook als u telefonisch, per e-mail of persoonlijk door iemand wordt benaderd die aangeeft medewerker te zijn van de Rabobank, een andere bank of een andere dienstverlener, bijvoorbeeld een computerbeveiligingsbedrijf of een (fraude)helpdesk. Wij of een andere dienstverlener zullen u op deze wijze nooit om beveiligingscodes vragen.
• Zorg er ook voor dat iemand anders geen iris, vingerafdruk of gezicht kan toevoegen die gebruikt kan worden voor Rabo Online Bankieren, of een apparaat met een digitale pas. Houd uw beveiligingscodes voor iedereen geheim, ook voor ons. Wij zullen u nooit om deze codes vragen!

2) Zorg ervoor dat een ander uw betaalpas, creditcard en digitale pas nooit gebruikt
Denk hierbij aan het volgende:
• Laat u niet afleiden als u uw betaalpas, creditcard of digitale pas gebruikt en controleer of u uw eigen betaalpas, creditcard of apparaat met een digitale pas daarna terugkrijgt.
• Berg de betaalpas, creditcard en apparaat met een digitale pas altijd op een veilige plaats op en zorg ervoor dat u deze niet gemakkelijk kunt verliezen. Controleer regelmatig of u de betaalpas, creditcard en apparaat met een digitale pas nog in uw bezit heeft.

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 voor het regelen van uw bankzaken gebruikt, is voorzien van actuele (beveiligings)updates. Geïnstalleerde software is bijvoorbeeld het besturingssysteem en beveiligingsprogramma's, zoals een 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 ons verstrekte toepassingen, op de apparatuur die u gebruikt voor het regelen van uw bankzaken, niet door onbevoegden kunnen worden gebruikt.
• Log altijd uit als u klaar bent met het regelen van uw bankzaken.

4) Controleer uw rekening
Controleer altijd zo spoedig mogelijk uw elektronische of papieren rekeninginformatie op eventuele transacties waarvoor u geen toestemming heeft gegeven. Doe dit in ieder geval elke twee weken als wij voor u elektronische rekeninginformatie ter beschikking stellen. Als u alleen rekeninginformatie op papier ontvangt, controleer deze dan in ieder geval binnen twee weken na ontvangst. Als er schade voor ons ontstaat doordat het voor u enige tijd onmogelijk is geweest uw rekeninginformatie te controleren, kunnen wij u vragen aan te tonen dat dit in alle redelijkheid niet mogelijk was.

5) Meld incidenten direct aan ons en volg onze aanwijzingen op
Denk hierbij aan het volgende:
• Neem in de volgende gevallen in elk geval direct contact op met het in artikel 43 vermelde Rabobank meldpunt:
• U heeft uw betaalpas, creditcard of apparaat met een digitale pas niet meer in uw bezit of weet niet waar deze is.
• U weet of vermoedt dat iemand anders een beveiligingscode kent of heeft gebruikt. Dit geldt ook als het gaat om de beveiligingscode van uw apparaat met een digitale pas.
• U weet of vermoedt dat iemand een iris, vingerafdruk of gezicht toegevoegd heeft voor Rabo Online Bankieren of apparaat met een digitale pas.
• U ziet dat er transacties op uw rekening hebben plaatsgevonden, waarvoor u geen toestemming heeft gegeven.
• U heeft uw mobiele apparaat met daarop één van onze apps waarmee u kunt betalen of bankieren of een apparaat waarop u een digitale pas gebruikt niet meer, tenzij u dit apparaat aan een ander heeft overgedragen en eerst de apps en/of digitale pas heeft verwijderd.
• Neem ook direct contact op met het in artikel 43 vermelde Rabobank meldpunt bij iets dat u als vreemd of ongebruikelijk ervaart bij het elektronisch betalen of online regelen van uw bankzaken, Bijvoorbeeld een andere manier van inloggen. Wij kunnen zorgen voor een blokkade om (verdere) schade te voorkomen. Als wij u aanwijzingen geven, bijvoorbeeld om nieuwe incidenten te voorkomen, dan moet u deze aanwijzingen opvolgen. Ook hierbij zullen wij u nooit om beveiligingscodes vragen.

Relevante artikelen uit het 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 betaaldienstverlener overeengekomen vorm en procedure. Bij gebreke van een dergelijke instemming wordt een betalingstransactie als niet toegestaan aangemerkt.

3. De instemming kan te allen tijde, doch uiterlijk op het tijdstip van het onherroepelijk worden, krachtens artikel 534 van de betaalopdracht door de betaler worden ingetrokken. Hetzelfde geldt voor een instemming met de uitvoering van een betaalopdracht betreffende een reeks betalingstransacties, die kan worden ingetrokken met als gevolg dat iedere toekomstige betalingstransactie als niet-toegestaan wordt 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 gepersonaliseerde veiligheidskenmerken ervan te waarborgen. (...)

Art. 7:526
1. De betaaldienstgebruiker die bekend is met een niet-toegestane of onjuist uitgevoerde betalingstransactie waarvoor hij de betaaldienstverlener aansprakelijk kan stellen met inbegrip van de aansprakelijkheidsgronden van artikel 543, 544 en 545, verkrijgt alleen rectificatie van zijn betaaldienstverlener indien hij hem onverwijld en uiterlijk dertien maanden na de valutadatum waarop zijn rekening is gedebiteerd, kennis geeft van de bewuste transactie, tenzij de betaaldienstverlener, in voorkomend geval, de informatie betreffende die betalingstransactie niet heeft verstrekt of ter beschikking heeft gesteld overeenkomstig de wijze vastgesteld bij of krachtens de in artikel 4:22 van de Wet op het financieel toezicht bedoelde algemene maatregel van bestuur. (...)

Art. 7:527
1. Indien een betaaldienstgebruiker ontkent dat hij met een uitgevoerde betalingstransactie heeft ingestemd of aanvoert dat de betalingstransactie niet correct is uitgevoerd, is zijn betaaldienstverlener gehouden het bewijs te leveren dat de betalingstransactie is geauthenticeerd, juist is geregistreerd en geboekt en niet door een technische storing of enig ander falen van de door de betaaldienstverlener aangeboden diensten is beïnvloed. Indien de betalingstransactie geïnitieerd wordt via een betaalinitiatiedienstverlener, levert deze het bewijs dat, binnen zijn verantwoordelijkheid, de betalingstransactie is geauthenticeerd, juist is geregistreerd en niet door een technische storing of enig ander falen in verband met de betaaldienst waarmee hij is belast, is beïnvloed.

2. Indien een betaaldienstgebruiker ontkent dat hij met een uitgevoerde betalingstransactie heeft ingestemd, vormt het feit dat het gebruik van een betaalinstrument door de betaaldienstverlener, daaronder in voorkomende geval de betaalinitiatiedienstverlener begrepen, is geregistreerd niet noodzakelijkerwijze afdoende bewijs dat met de betalingstransactie door de betaler is ingestemd of dat de betaler frauduleus heeft gehandeld of opzettelijk of met grove nalatigheid een of meer van zijn verplichtingen uit hoofde van artikel 524 niet is nagekomen. De betaaldienstverlener, daaronder in voorkomend geval de betaalinitiatiedienstverlener begrepen, verstrekt ondersteunend bewijs om fraude of grove nalatigheid van de zijde van de betaler te bewijzen.

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. Op grond van het eerste lid herstelt de betaaldienstverlener van de betaler de betaalrekening die met dat bedrag is gedebiteerd in de toestand zoals die geweest zou zijn wanneer de niet-toegestane betalingstransactie niet had plaatsgevonden. De valutadatum van de creditering van de betaalrekening van de betaler is uiterlijk de datum waarop het bedrag was gedebiteerd.

3. Het eerste lid is niet van toepassing indien de betaaldienstverlener van de betaler redelijke gronden heeft om fraude te vermoeden en hij deze gronden schriftelijk aan de Autoriteit Financiële Markten meedeelt.

4. Indien de betalingstransactie via een betaalinitiatiedienstverlener wordt geïnitieerd, betaalt de rekeninghoudende betaaldienstverlener onmiddellijk, en in elk geval uiterlijk aan het einde van de eerstvolgende werkdag, het bedrag van de niet-toegestane betalingstransactie terug en herstelt hij, in voorkomend geval, de betaalrekening die met dat bedrag was gedebiteerd, in de toestand zoals die geweest zou zijn wanneer de niet-toegestane betalingstransactie niet had plaatsgevonden.

5. Ingeval de betaalinitiatiedienstverlener aansprakelijk is voor de niet-toegestane betalingstransactie, vergoedt hij de rekeninghoudende betaaldienstverlener op diens verzoek onmiddellijk de geleden verliezen of de aan de betaler terugbetaalde bedragen, waaronder het bedrag van de niet-toegestane betalingstransactie. Overeenkomstig artikel 527, tweede lid, is de betaalinitiatiedienstverlener gehouden te bewijzen dat, binnen zijn verantwoordelijkheid, de betalingstransactie is geauthenticeerd, juist is geregistreerd en niet door een technische storing of enig ander falen in verband met de betaaldienst waarmee hij is belast, is beïnvloed.

6. Aanvullende financiële compensatie kan worden vastgesteld overeenkomstig het recht dat van toepassing is op de tussen de betaler en zijn betaaldienstverlener gesloten overeenkomst of de tussen de betaler en de betaalinitiatiedienstverlener gesloten overeenkomst, indien van toepassing.

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 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.

3. Indien de betaaldienstverlener van de betaler geen sterke cliëntauthenticatie verlangt, draagt de betaler geen financiële verliezen, tenzij de betaler frauduleus heeft gehandeld. Indien de sterke cliëntauthenticatie door de begunstigde of de betaaldienstverlener van de begunstigde niet wordt aanvaard, wordt de door de betaaldienstverlener van de betaler geleden financiële schade door hen vergoed.

4. Na de kennisgeving overeenkomstig artikel 524, eerste lid, onder b, heeft het gebruik van het betaalinstrument geen financiële gevolgen voor de betaler, tenzij deze frauduleus heeft gehandeld.

5. Indien de betaaldienstverlener nalaat om overeenkomstig artikel 525, eerste lid, onder c, passende middelen beschikbaar te stellen waarmee te allen tijde een kennisgeving als bedoeld in artikel 524, eerste lid, onder b, kan worden gedaan, is de betaler niet aansprakelijk voor de financiële gevolgen die uit het gebruik van dat betaalinstrument voortvloeien, tenzij hij frauduleus heeft gehandeld.