Uitspraak Geschillencommissie Kifid nr. 2023-0897

(mr. F.H.E. Boerma, voorzitter en mr. P. Meijer, secretaris)

Datum uitspraak	28 november 2023
Klacht van	De consument
Tegen	Coöperatieve Rabobank U.A., gevestigd te Amsterdam, verder te noemen de bank
Aard uitspraak	Bindend advies
Uitkomst	Vordering afgewezen
Bijlage	Relevante bepalingen uit wet- en regelgeving en de algemene voorwaarden

Samenvatting

Spoofing Bankhelpdeskfraude. De consument is slachtoffer geworden van bankhelpdesk-fraude, zijnde een vorm van spoofing. De commissie is van oordeel dat de bank de schade van de consument niet hoeft te vergoeden. De coulanceregeling voor bankhelpdeskfraude is niet van toepassing en de bank heeft haar zorgplicht niet geschonden. Verder is de commissie van oordeel dat er sprake is van een toegestane betalingstransactie en de schade daarom voor rekening van de consument blijft. De commissie overweegt hierbij dat, ook in het geval er sprake zou zijn van een niet-toegestane betalingstransactie, de schade voor rekening van de consument blijft, omdat de consument grof nalatig gehandeld heeft door onder meer de fraudeur toegang te geven tot zijn computer en telefoon. 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 consument is in deze zaak vertegenwoordigd door professioneel gemachtigde mr. P.M.W. Spiertz van Achmea Rechtsbijstand. De bank is in deze zaak vertegenwoordigd door professioneel gemachtigde mr. F.J. Laagland, 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 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 betaalrekening aan bij de bank (hierna: de betaalrekening). Op het gebruik van de betaalrekening zijn de Algemene Bankvoorwaarden en de Voorwaarden Betalen en online diensten 2022 van toepassing verklaard (hierna: de voorwaarden). Relevante artikelen uit de voorwaarden zijn in de bijlage opgenomen.

2.2 Op 12 oktober 2022 is de consument telefonisch benaderd door een persoon die zich voordeed als een medewerker van ING Bank N.V. (hierna te noemen: ING Bank). Deze persoon (verder te noemen: de fraudeur) heeft de consument een accreditatie laten zien en verteld dat er Bitcoins van zijn rekening werden afgeschreven. Dit terwijl de consument geen Bitcoins bezat.

2.3 De fraudeur heeft de consument er vervolgens toe bewogen om remote-access software (Anydesk) te downloaden en te installeren op zijn computer en telefoon. Ook is de consument ertoe bewogen een foto te maken van zijn gelaat en paspoort en van een bankafschrift van zijn rekening bij ING Bank. Vervolgens werden er door de fraudeur diverse handelingen verricht op de computer en telefoon van de consument. De consument werd zelf ook gevraagd om bepaalde handelingen te verrichten, zoals het invullen van bedragen.

2.4 Vanaf de betaalrekening zijn er twee transacties verricht naar een rekening op naam van “Moon Pay Limited”. De eerste transactie betrof een bedrag van € 3.008,-, de tweede transactie een bedrag van € 1.789,-. Na de eerste transactie signaleerde het detectie-systeem van de bank de tweede transactie als verdacht en kon deze tegengehouden worden. De betaalrekening werd vervolgens door de bank ook geblokkeerd. Na contact met de consument is door de bank geprobeerd het bedrag van de eerste transactie veilig te stellen bij de bank van de ontvanger, maar dit is niet gelukt. Vanaf de rekening die de consument aanhield bij ING Bank is ook een transactie verricht door de fraudeur. Deze transactie kon echter direct geblokkeerd worden door ING Bank.

2.5 De consument heeft de bank verzocht om de eerste transactie van € 3.008,- aan hem te vergoeden. De bank heeft geen gehoor gegeven aan dit verzoek. Omdat een verdere uitwisseling van standpunten tussen partijen niet tot een oplossing heeft geleid, heeft de consument vervolgens een klacht ingediend bij Kifid.

De klacht en vordering

2.6 De consument vordert van de bank een schadevergoeding van € 3.008,-, vermeerderd met de wettelijke rente over dit bedrag vanaf 12 oktober 2022. De consument legt de volgende argumenten aan zijn vordering ten grondslag.

- Er is sprake van bankhelpdeskfraude c.q. “spoofing” en de schade zou vergoed moeten worden op basis van de hiervoor opgestelde coulanceregeling. De consument is immers slachtoffer geworden van iemand die zich voordeed als een medewerker van zijn bank. Weliswaar stelde deze persoon zich voor als een vertegenwoordiger van ING Bank (waar de consument ook bankiert) en is er geld ontvreemd van de rekening bij de bank, maar er is wel sprake geweest van iemand die zich presenteert als de medewerker van de bank van de consument.
- Op verzoek van de bank is in het verleden een koppeling gemaakt tussen de betaalrekening en de rekening die de consument aanhield bij ING Bank. Als deze koppeling er niet zou zijn geweest dan had de frauduleuze transactie van de betaalrekening niet hebben kunnen plaatsvinden.
- De bank heeft haar zorgplicht geschonden door de frauduleuze transactie niet tegen te houden. De bank had moeten opmerken dat de opdrachten niet strookten met de reguliere bancaire opdrachten van de consument. Verder is het de consument niet duidelijk waarom de tweede frauduleuze transactie wel kon worden teruggeboekt door de bank, maar de eerste transactie niet. Deze transacties zijn namelijk vrij snel na elkaar uitgevoerd.
- De consument heeft niet grof nalatig of bewust roekeloos gehandeld. De consument heeft niets (welbewust) geautoriseerd. De Raboscanner is door de consument niet gebruikt. De consument was zich ten tijde van het telefoon-gesprek met de fraudeur op geen enkel moment daadwerkelijk bewust van het gevaar. In tegendeel, de consument dacht juist dat hij er goed aan deed zijn medewerking te verlenen en hij bezig was met “bereddingswerk”.

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

Waar gaat het om?

3.1 De commissie stelt voorop dat het te betreuren is dat de consument slachtoffer is geworden van fraudeurs. De vraag die echter voorligt is of de bank gehouden is om de door de consument geleden schade van € 3.008,- te vergoeden. De commissie is van oordeel dat de bank hiertoe niet gehouden is en licht hieronder toe waarom niet.

Coulanceregeling spoofing

3.2 Eind 2020 hebben de vier grootbanken de ‘coulanceregeling’ opgesteld, die inhoudt dat particuliere klanten die slachtoffer zijn geworden van bankhelpdeskfraude, zijnde een vorm van ‘spoofing’, 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. De Nederlandse Vereniging van Banken (NVB) heeft een toetsingskader opgesteld voor deze coulanceregeling. Uit dit toetsingskader volgt de volgende definitie van 'spoofing':

> *"(...) 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. (...)"*

3.3 Naar het oordeel van de commissie is de coulanceregeling niet van toepassing op de situatie van de consument. Vast staat immers dat de consument gebeld is door een fraudeur die zich voordeed als medewerker van ING Bank en niet van de bank. Uit het voorgaande volgt dat, in relatie tot de bank, niet is voldaan aan een belangrijk element voor toepasselijkheid van de coulanceregeling van de bank, namelijk dat de fraudeur misbruik heeft gemaakt van de naam van de bank en/of dat de fraudeur het telefoonnummer van de bank moet hebben misbruikt. Daarbij merkt de commissie op dat het niet aan haar is om (het toetsingskader van) de coulanceregeling, gelet op de aard daarvan, op te rekken.[1] Een eventuele koppeling tussen de rekening bij de bank en de rekening bij ING Bank (waarover meer in overweging 3.12) zou het oordeel van de commissie dat de coulanceregeling niet van toepassing is niet anders maken.

3.4 Gelet op het voorgaande zal de commissie nu ingaan op het relevante wettelijke kader. De wet maakt onderscheid tussen toegestane en niet-toegestane betalingstransacties.

Betalingstransactie: toegestane en/of niet-toegestane betalingstransactie

3.5 Bij toegestane betalingstransacties[2] geldt als uitgangspunt dat de consument daar zelf verantwoordelijk voor is. De bank is als betaaldienstverlener op grond van artikel 7:533 lid 4 van het Burgerlijk Wetboek (hierna: BW) verplicht om een betaalopdracht uit te voeren. De bank is niet aansprakelijk voor de schade. Bij niet-toegestane betalingstransacties[3] is de bank in beginsel wettelijk verplicht om de geleden schade te vergoeden.[4] Dit is slechts anders indien de consument frauduleus heeft gehandeld of opzettelijk of met grove nalatigheid een of meer verplichtingen uit hoofde van artikel 7:524 BW niet is nagekomen.[5]

[1] In gelijke zin: Geschillencommissie Kifid nrs. 2023-0171, 2022-0935, 2022-0953 en 2022-0959
[2] Artikel 7:522 lid 1 BW
[3] Artikel 7:522 lid 2 BW
[4] Artikel 7:528 lid 1 BW
[5] Artikel 7:529lid 1 BW

In dat artikel staat onder meer dat de consument zich dient te houden aan de veiligheids-regels die de bank stelt.

3.6 De bank dient te bewijzen dat de consument heeft ingestemd met de betalingstransactie, en dat sprake is geweest van fraude, opzet of grove nalatigheid.

3.7 De consument heeft gesteld – zo begrijpt de commissie – dat sprake is van een niet-toegestane betalingstransactie. De consument stelt de betalingstransactie niet (welbewust) te hebben geautoriseerd. Ook heeft hij niet actief (inlog) codes verstrekt aan derden, dus ook niet aan de fraudeur. De consument wist niet dat er betalingstransacties gedaan werden. De consument dacht bezig te zijn met "bereddingswerk". De bank heeft aangevoerd, en met stukken uit haar administratie onderbouwd, dat sprake is van een toegestane betalingstransactie, omdat de consument de transactie heeft geaccordeerd middels gebruikmaking van de Rabo scanner, betaalpas en pincode. Daarmee heeft de consument volgens de bank ingestemd met de uitvoering van de transactie. De consument heeft dit, in het licht van de door de bank gegeven onderbouwing, onvoldoende weersproken. Daarmee staat voor de commissie vast dat sprake is van een toegestane betalingstransactie. De bank is daarom niet gehouden het bedrag van de transactie aan de consument te vergoeden.

3.8 De commissie overweegt dat ook in het geval sprake zou zijn geweest van een niet-toegestane betalingstransactie, omdat de consument misleid is, de conclusie moet luiden dat de bank niet verplicht is het bedrag van de transactie aan de consument te vergoeden. Door het programma Anydesk te installeren, de oplichter toegang te geven tot zijn computer en telefoon en (daarmee) de internetbankierenomgeving en de transactie (al dan niet bewust) te accorderen, is de consument de veiligheidsregels voor (internet)bankieren, zoals opgenomen in artikel 45 van de voorwaarden, niet nagekomen. De consument heeft daarmee grof nalatig gehandeld in de zin van artikel 7:529 lid 1 BW. Daarom hoeft de bank het bedrag van de niet-toegestane transactie niet te vergoeden.

3.9 Daarnaast ziet de commissie geen aanleiding om de eigen aansprakelijkheid van de consument te beperken op grond van artikel 7:529 lid 2 BW.

De zorgplicht van de bank

3.10 De consument heeft verder gesteld dat de bank hem had behoren te waarschuwen dan wel. de betalingstransactie tegen had moeten houden. Zoals eerder geoordeeld is door de geschillencommissie van Kifid, is de rol van de bank jegens de consument als betaaldienst-verlener in beginsel beperkt tot het optimaliseren van het betalingsverkeer op de rekening van de consument.[6] De bank in haar rol van betaaldienstverlener kan geen verwijt worden gemaakt voor het uitvoeren van de transactie zonder nadere monitoring.

[6] Zie o.a. Geschillencommissie Kifid 2019-531

Een algemene monitoringsverplichting zou het proces van geautomatiseerde gegevens-verwerking en het maatschappelijk belang dat daarmee gediend is, kunnen schaden.[7] Wel kan van de bank worden verwacht dat zij tot onderzoek zou overgaan indien zij wist van ongebruikelijk betalingsverkeer. Bepalend is datgene waarvan de bank zich daadwerkelijk bewust was. Bewustheid van het daaraan verbonden 'gevaar' bij de bank kan onder omstandigheden, gelet op haar positie en deskundigheid worden verondersteld.[8]

3.11 In het onderhavige geval is niet gesteld en ook niet gebleken dat de bank ten tijde van de overboeking van € 3.008,- ervan op de hoogte was dat de consument opgelicht werd of de transactie niet vrijwillig door de consument werd gedaan. Dat de tweede overboeking (van € 1.789,-) is gesignaleerd en tegengehouden door het detectiesysteem van de bank, maakt niet dat het detectiesysteem van de bank ook de eerste transactie had moeten signaleren en tegenhouden, dan wel dat de bank op dat moment anderszins wist dat er sprake was van fraude/oplichting. De bank heeft dus niet verwijtbaar gehandeld door de consument niet (tijdig) te waarschuwen of de betalingstransactie te blokkeren.

Koppeling van de rekening bij de bank met de rekening bij ING Bank

3.12 De consument stelt verder nog dat de fraude plaats heeft kunnen vinden door de koppeling van de rekening bij de bank met de rekening bij ING Bank. Door de bank wordt betwist dat er sprake is van een dergelijke koppeling. De consument heeft niet aangetoond dat er wel sprake is van een dergelijke koppeling. Ook heeft de consument niet onderbouwd op welke wijze een dergelijke koppeling geleid zou hebben tot c.q. invloed zou hebben gehad op de fraude.

Conclusie

3.13 De conclusie is dat de schade die de consument heeft geleden voor zijn eigen rekening en risico blijft. De bank hoeft geen schadevergoeding aan de consument te betalen.

Ambtshalve toetsing

3.14 De overeenkomst die in deze klachtprocedure centraal staat is gesloten tussen de financiële dienstverlener die bedrijfsmatig handelt en een consument. In dat geval vindt ook ambtshalve toetsing plaats aan het Europese en Nederlandse (consumenten)recht. Het beding dat voor de beoordeling van de klacht van de consumenten relevant is, te weten artikel 45 van de voorwaarden, is door de commissie getoetst en niet oneerlijk bevonden.

[7] Zie o.a. Geschillencommissie Kifid 2019-759
[8] Hoge Raad 27 november 2015, ECLI:NL:HR:2015:3399 'Van den Berg'. Dit arrest is te vinden op www.rechtspraak.nl.

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 2022, 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 2022, 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 / de algemene voorwaarden

In deze bijlage zijn opgenomen de relevante bepalingen uit het Burgerlijk Wetboek en de Voorwaarden betalen en online diensten 2022

Voorwaarden betalen en online diensten 2022

Uniforme veiligheidsregels

(...)

45. Waarom is het belangrijk dat u zich houdt aan deze regels? U vermindert de kans dat u het slachtoffer wordt van fraudeurs sterk als u de regels opvolgt. Het is voor consumenten wettelijk geregeld dat een bedrag, dat zonder uw toestemming van uw rekening is afgeboekt, door ons wordt vergoed. Wij zijn echter niet altijd verplicht dat bedrag aan u te vergoeden. Wanneer u zich aan de onderstaande vijf veiligheidsregels houdt, loopt u niet het risico dat de gehele schade voor uw eigen rekening komt.

Wat moet u doen?

1) Houd uw beveiligingscodes geheim.

2) Zorg ervoor dat een ander uw betaalpas, creditcard en digitale pas nooit gebruikt.

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

4) Controleer uw rekening.

5) Meld incidenten direct aan ons en volg onze aanwijzingen op.

Elk van deze veiligheidsregels wordt hieronder toegelicht.

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/Scode, 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.

U kunt uw betaalpas, digitale pas of creditcard vaak ook blokkeren via internetbankieren of de Rabo App. Maar ook dan neemt u direct contact met ons op.

Burgerlijk Wetboek, Boek 7

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.

3. De instemming kan te allen tijd, 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 niettoegestane 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 niettoegestane 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. 9

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.

Artikel 7:533

1. Indien de betaaldienstverlener weigert een opdracht uit te voeren of een betalingstransactie te initiëren, wordt de betaaldienstgebruiker in kennis gesteld van deze weigering en, indien mogelijk, van de redenen daarvoor en van de procedure voor de correctie van eventuele feitelijke onjuistheden die tot de weigering hebben geleid, tenzij ander toepasselijk Unierecht op toepasselijk nationaal recht dit verbiedt.

2. De betaaldienstverlener verstrekt zo spoedig mogelijk de kennisgeving – of stelt deze ter beschikking – op de overeengekomen wijze, en in elk geval binnen de in artikel 537 vermelde termijnen.

3. In de raamovereenkomst kan de voorwaarde worden gesteld dat de betaaldienstverlener voor die kennisgeving een redelijke vergoeding in rekening mag brengen indien de weigering objectief gerechtvaardigd is.

4. Indien alle in de raamovereenkomst van de betaler gestelde voorwaarden vervuld zijn, weigert de rekeninghoudende betaaldienstverlener van de betaler niet een toegestane betaalopdracht uit te voeren, ongeacht of de betaalopdracht door een betaler zelf, onder meer door een betaalinitiatiedienstverlener, dan wel door of via een begunstigde is geïnitieerd, tenzij ander toepasselijk Unierecht of toepasselijk nationaal recht dit verbiedt.

5. Een betaalopdracht waarvan de uitvoering is geweigerd, wordt geacht niet ontvangen te zijn voor de toepassing van de artikelen 537, 543, 544 en 545.