Uitspraak Geschillencommissie Kifid nr. 2023-0403

(mr. J. van der Groen, voorzitter, mr. A.M.T. Wigger, A.E. Tevel, leden en mr. E.H.C. Vos, secretaris)

Datum uitspraak	30 mei 2023
Klacht van	de heer [naam 1] en mevrouw [naam 2], verder te noemen de consumenten, of ieder afzonderlijk de heer en mevrouw
Tegen	Coöperatieve Rabobank U.A., gevestigd te Amsterdam, verder te noemen Rabobank
Aard uitspraak	Bindend advies
Uitkomst	Vordering afgewezen
Bijlage	Relevante bepalingen uit wet- en regelgeving en de algemene voorwaarden

Samenvatting

Spoofing. Bankhelpdeskfraude. De consumenten zijn slachtoffer geworden van bankhelpdeskfraude, met rekeningen van de twee banken waar zij bankieren. De ene bank heeft de schade vergoed. De klacht gaat over de andere bank. De commissie is van oordeel dat deze bank de schade niet hoeft te vergoeden. De coulanceregeling is niet van toepassing en de bank heeft haar zorgplicht niet geschonden. Verder is de commissie van oordeel dat de consumenten grof nalatig gehandeld hebben door onder meer hun betaalpassen en pincode af te geven. 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 consumenten en 2) het verweerschrift van Rabobank.

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 consumenten en Rabobank 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 consumenten houden samen een gezamenlijke rekening aan bij Rabobank (hierna: de betaalrekening). De consumenten hebben ieder een betaalpas van de betaalrekening.

Op het gebruik van de betaalrekening zijn Voorwaarden voor Betalen en online diensten 2022 van toepassing verklaard (hierna: de voorwaarden). Relevante artikelen uit de voorwaarden zijn in de bijlage opgenomen.

2.2 De consumenten hebben ook een rekening bij ING Bank. Op zaterdag 9 juli 2022 werden de consumenten rond 21:00 uur gebeld door iemand die zich voordeed als een medewerker van de afdeling Fraudebestrijding van ING Bank. Later bleek dat dit een fraudeur was (hierna: de fraudeur). De fraudeur zei dat er een afschrijving van € 1.704,50 vanaf de ING-rekening van de consumenten klaarstond en dat hij wilde verifiëren of de consumenten die afschrijving zelf wilden verrichten. De consumenten hadden die afschrijving niet opgegeven en de fraudeur concludeerde dat iemand dan waarschijnlijk de pincode van de consumenten had afgekeken en toegang had tot hun rekening. De fraudeur zei ook dat de mobiele telefoon van de heer waarschijnlijk geïnfecteerd was met malware. De fraudeur zou de consumenten helpen door hun rekening te blokkeren en een nieuwe pincode aan te maken. De consumenten zeiden daarop dat het enkele dagen duurt voordat een pincode gewijzigd is. De fraudeur wuifde dit echter weg met de opmerking dat sinds 1 juli een speciale procedure gevolgd moet worden. Hij zei ook dat een andere ING-medewerker langs zou komen bij de consumenten om hun passen door te knippen. De consumenten zouden die medewerker kunnen identificeren met behulp van een code.

2.3 Daarna hebben de consumenten op instructie van de fraudeur hun oude pincode ingesproken en een nieuwe pincode doorgegeven. Volgens de fraudeur zou een computer de pincodes ontvangen. Mevrouw gaf door de stress per ongeluk haar pincode van Rabobank door, in plaats van de pincode voor ING Bank. De heer hoorde dit en zei tegen zijn vrouw dat er dus iets niet klopte, want de computer had de verkeerde pincode geaccordeerd. De fraudeur redde zich hieruit met de verklaring dat de computer later pas de oude pincode controleert.

2.4 Enige tijd later die avond kwam een vrouw aan de deur bij de consumenten (hierna: de vrouw) en zij vroegen aan de vrouw of zij van Rabobank was. De vrouw bevestigde dat en zei dat zij ook voor ING Bank dit soort klusjes deed. De consumenten vonden het vreemd dat de vrouw bevestigd had voor Rabobank te werken, maar ook voor ING Bank klusjes zou doen, vroegen haar buiten te wachten en bespraken hun twijfels met de fraudeur aan de telefoon. De fraudeur haalde de consumenten over om de vrouw toch te vertrouwen, omdat zij de juiste code had doorgegeven. Op een gegeven moment was de vrouw verdwenen. Enige tijd later kwam een jongedame (hierna: de jongedame) de passen van de consumenten doorknippen en foto's maken van de startpagina's van de telefoons van de consumenten.

2.5 De fraudeur aan de telefoon vroeg daarna of de consumenten nog bij andere banken rekeningen hadden De consumenten denken dat hij op dit spoor gezet is door de eerste vrouw die bij hen aan de deur was geweest. Dit alles gebeurde nog steeds op dezelfde avond.

De consumenten bevestigden toen dat zij ook rekeningen bij Rabobank hadden. De fraudeur zei dat hij ging overleggen met Rabobank en belde na 20 minuten, rond 23:55 uur terug en zei dat hij ook gemachtigd was om dit voor Rabobank te regelen. Daarop hebben de consumenten dezelfde stappen doorlopen voor hun passen bij Rabobank: pincodes veranderen door ze telefonisch in te spreken en de betaalpassen en creditcard van Rabobank laten doorknippen door de jongedame, die weer op bezoek kwam. Ook hebben de consumenten de telefoon van de heer afgegeven aan de jongedame, omdat die geïnfecteerd zou zijn met malware.

2.6 Op 10 juli 2022 om 00:25 uur is € 4.000,- opgenomen van de spaarrekening van de consumenten bij de bank en op de betaalrekening bijgeschreven. Vervolgens zijn die nacht drie geldopnames van ieder € 1.240,- verricht vanaf de betaalrekening: om 00:29 uur, 00:30 uur en 00:37 uur, in totaal € 3.720,-. Om 00:38 uur is geprobeerd nog een opname van € 990,- te verrichten, maar die opname is niet gelukt. Tussentijds is om 00:34 uur de opnamelimiet van de betaalpas van de heer verhoogd naar € 2.300,-, via de bankierenapp van de heer. Rabobank heeft de wijziging van de paslimiet bevestigd met een e-mail van 00:34 uur aan de heer.

2.7 Op maandagochtend belden zowel ING Bank als Rabobank naar de consumenten. Toen begrepen de consumenten dat zij waren opgelicht door de fraudeur en de personen die bij hen aan de deur verschenen waren. Bij ING Bank was een bedrag van € 800,- afgeschreven en die bank heeft dit bedrag aan de consumenten vergoed. In een brief van ING Bank aan de consumenten is opgenomen dat de consumenten slachtoffer zijn van bankhelpdeskfraude (spoofing) en dat ING Bank het geld uit coulance aan de consumenten vergoedt.

De klacht en vordering

2.8 De consumenten vorderen dat Rabobank het van hun betaalrekening afgeschreven bedrag van € 3.720,- aan hen vergoedt, of in elk geval voor een deel. De consumenten hebben deze klacht ingediend omdat ING Bank hun schade bij die bank wel vergoedde. De consumenten vinden dat Rabobank dat ook moet doen. Daarnaast hebben de consumenten erop gewezen dat zij meer dan 30 jaar trouwe klanten zijn, zonder problemen. De consumenten zijn zich er bewust van dat zij ontzettend nalatig zijn geweest, maar hun vertrouwen in mensen en in Rabobank moet hersteld worden.

2.9 Bovendien heeft mevrouw geen e-mail ontvangen over de paslimietverhoging, terwijl het een gezamenlijke rekening betreft. De heer kon de e-mail die naar hem gestuurd is niet lezen, omdat hij zijn telefoon ook, onder valse voorwendselen, had afgegeven aan de jongedame. Volgens de consumenten hadden zij, als zij de e-mail opgemerkt hadden, onraad geroken en kunnen ingrijpen om de schade te beperken.

2.10 Tot slot vinden de consumenten het opvallend dat er binnen 12 minuten 5 handelingen werden verricht: 4 transacties en de paslimietwijziging. Volgens de consumenten moet er dan toch een melding binnenkomen bij Rabobank, op basis van een algoritme. Ook hebben de consumenten erop gewezen dat andere banken een wachttijd hanteren voor een paslimietwijziging.

Het verweer

2.11 Rabobank heeft verweer gevoerd tegen de stellingen van de consumenten. Voor zover relevant zal de commissie bij de beoordeling daarop ingaan.

3. De beoordeling

Te beoordelen vragen

3.1 Aan de commissie is ter beoordeling voorgelegd of Rabobank de schade van de consumenten moet vergoeden. De commissie heeft deze vraag beoordeeld aan de hand van drie aspecten. Het eerste is de vergoeding van de schade door ING bank, het tweede aspect is de zorgplicht van Rabobank en ten derde het wettelijke kader voor niet-toegestane transacties. Het oordeel luidt dat de schade van de consumenten niet vergoed hoeft te worden en deze conclusie wordt als volgt toegelicht.

Vergoeding door ING Bank, coulanceregeling spoofing

3.2 De consumenten hebben gesteld dat ING Bank hun schade bij die bank vergoed heeft en zij menen dat Rabobank hun schade bij die bank ook aan hen zou moeten vergoeden. ING Bank heeft het bedrag van € 800-,- aan de consumenten vergoed uit coulance. Dat ING Bank dit gedaan heeft, maakt op zichzelf niet dat Rabobank ook een schadevergoeding moet betalen aan de consumenten. Coulance is namelijk niet afdwingbaar en verschillende banken hoeven niet hetzelfde om te gaan met verzoeken tot vergoeding.

3.3 Mogelijk heeft ING Bank de schade vergoed in verband met de coulanceregeling voor slachtoffers van bankhelpdeskfraude, ook wel spoofing genoemd. Deze coulance-regeling hebben de vier grootbanken, waaronder ING Bank en Rabobank, vastgesteld. Deze vier grootbanken zijn lid van de Nederlandse Verenging van Banken (NVB) en de NVB heeft een toetsingskader opgesteld voor de coulanceregeling. Uit het toetsings-kader van de NVB van 2 juni 2021 voor de coulanceregeling 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."*

3.4 Omdat de consumenten de vergelijking gemaakt hebben tussen de bereidheid van ING Bank om de schade te vergoeden en de weigering van Rabobank om dat te doen, heeft de commissie beoordeeld of in het geval van Rabobank voldaan is aan de criteria zoals opgenomen in het toetsingskader. De commissie is van oordeel dat daar niet aan voldaan is. In het toetsingskader is namelijk bepaald dat de consument moet zijn benaderd door iemand die zich voordoet als een medewerker van Rabobank. In dit geval zijn de consumenten gebeld door een zogenaamde medewerker van ING Bank. Op een gegeven moment heeft de vrouw aan de deur weliswaar bevestigd dat zij voor Rabobank werkte (zie overweging 2.4), maar dat was slechts een keer, in de loop van de avond, nadat de consumenten dat per ongeluk vroegen. Omdat de consumenten benaderd zijn door iemand die zich voordeed als medewerker van ING Bank en niet van Rabobank, is in elk geval aan een van de voorwaarden van het toetsingskader van de NVB niet voldaan en is dat toetsingskader niet van toepassing op de situatie van de consumenten in relatie tot Rabobank.

De zorgplicht van Rabobank

3.5 De consumenten hebben verschillende kanttekeningen geplaatst bij het optreden van Rabobank. Ten eerste hebben de consumenten gesteld dat Rabobank weliswaar een e-mail gestuurd heeft naar de heer om hem erop te attenderen dat de paslimiet verhoogd was, maar niet naar mevrouw. De heer heeft de e-mail niet op tijd gezien omdat hij zijn telefoon meegegeven had aan de jongedame. Volgens de consumenten hadden zij, als Rabobank mevrouw ook een e-mail gestuurd had, maatregelen kunnen nemen om te voorkomen dat de schade verder zou oplopen.

3.6 Rabobank heeft hierop gereageerd dat zij geen e-mail gestuurd heeft naar het e-mailadres van mevrouw, omdat haar e-mailadres niet gekoppeld was aan de betaalpas waarvan de limiet verhoogd is. Dat is dan weer te verklaren door het feit dat dit de betaalpas van de heer was. De commissie is op basis hiervan van oordeel dat Rabobank niet tekortgeschoten is door alleen een e-mail naar de heer te sturen.

3.7 Ten tweede hebben de consumenten gesteld dat het Rabobank had moeten opvallen dat in korte tijd vier transacties en een limietverhoging plaatsvonden. Zoals eerder geoordeeld is door de geschillencommissie van Kifid, is de rol van Rabobank jegens de consumenten als betaaldienstverlener in beginsel beperkt tot het optimaliseren van het betalingsverkeer op de rekening van de consument.[1] Rabobank in haar rol van betaaldienstverlener kan geen verwijt worden gemaakt voor het uitvoeren van de opnames zonder nadere monitoring. Een algemene monitoringsverplichting zou het proces van geautomatiseerde gegevensverwerking en het maatschappelijk belang dat daarmee gediend is, kunnen schaden.[2] Wel kan van Rabobank worden verwacht dat zij tot onderzoek zou overgaan indien zij wist van ongebruikelijk betalingsverkeer.

[1] Zie GC Kifid 2019-531. Deze en andere uitspraken zijn te vinden op www.kifid.nl.
[2] Zie GC Kifid 2019-759 onder 4.3.

Bepalend is datgene waarvan Rabobank zich bewust was. Bewustheid van het daaraan verbonden 'gevaar' bij Rabobank kan onder omstandigheden, gelet op haar positie en deskundigheid worden verondersteld.[3] In het onderhavige geval is niet gesteld en ook niet gebleken dat Rabobank ten tijde van de opnames ervan op de hoogte was dat de consumenten opgelicht werden. Rabobank heeft dus niet verwijtbaar gehandeld door de consumenten niet te waarschuwen.

3.8 Ten derde hebben de consumenten naar voren gebracht dat andere banken limiet-verhogingen pas na een wachttijd doorvoeren. Rabobank heeft hierop gereageerd dat zij het voorkomen van misbruik van de betaalrekening ent op het gebruik van de betaalpas en pincode. Het is aan de consumenten om hier zorgvuldig mee om te gaan, volgens Rabobank. De commissie volgt Rabobank hierin en is van oordeel dat Rabobank niet tekortgeschoten is door geen wachttijd te hanteren voor het verhogen van de limiet van de betaalpas.

Niet-toegestane transacties

3.9 Omdat de consumenten zelf niet hebben ingestemd met de opnames, zijn de bepalingen over niet-toegestane transacties in het Burgerlijk Wetboek van toepassing. Het uitgangspunt is dat Rabobank het bedrag van niet-toegestane betalingstransacties onmiddellijk aan de consumenten moet terugbetalen (artikel 7:528 BW). Rabobank hoeft dit echter niet te doen als komt vast te staan dat de consumenten één of meer verplichtingen uit artikel 7:524 BW met grove nalatigheid niet zijn nakomen (artikel 7:529 lid 1 BW). Artikel 7:524 BW bepaalt onder meer dat de consumenten zich moeten houden aan de veiligheidsregels van Rabobank.

3.10 Rabobank heeft gesteld dat de consumenten op 9 juli 2022 meerdere veiligheidsregels niet nageleefd hebben en daarmee grof nalatig gehandeld hebben, zodat de schade voor rekening van de consumenten moet blijven (zie de veiligheidsregels in de bijlage). Zo mochten zij hun beveiligingscodes, betaalpassen en creditcard niet afstaan of doorgeven aan anderen. Zij mochten die alleen zelf gebruiken.

3.11 De consumenten hebben inderdaad in strijd met deze veiligheidsregels gehandeld toen zij hun betaalpassen, creditcard en mobiele telefoon afgaven terwijl kennelijk de code voor de bankierenapp bekend was bij de jongedame en toen zij hun pincode telefonisch doorgaven. De commissie is van oordeel dat de consumenten hierbij grof nalatig gehandeld hebben, vanwege de volgende omstandigheden.

3.12 Ten eerste hebben de consumenten in strijd met meerdere veiligheidsmaatregelen gehandeld (het aan derden verstrekken van passen en pincodes).

[3] Hoge Raad 27 november 2015, ECLI:NL:HR:2015:3399 'Van den Berg'. Dit arrest is te vinden op www.rechtspraak.nl.

Ten tweede hebben de handelingen veel tijd in beslag genomen en was er daardoor gelegenheid om tot het inzicht te komen dat er iets mis was. Dit geldt des te meer omdat de consumenten zelf meermaals twijfels hadden. Zo waren de consumenten zich ervan bewust dat het normaal gesproken een aantal dagen duurt voordat een pincode gewijzigd is, hadden zij twijfels toen de 'computer' de pincode van Rabobank accepteerde terwijl zij de pincode van ING Bank moesten doorgeven, en hadden zij wederom hun bedenkingen toen de vrouw bevestigde voor Rabobank te werken, terwijl iemand van ING Bank zou langskomen. Tot slot zijn de betaalpassen weliswaar doorgeknipt voordat zij werden meegenomen[4], maar in dit geval heeft de jongedame dat gedaan. De consumenten hebben de passen niet zelf doorgeknipt met het idee dat de betaalpas daarna onbruikbaar zou zijn. Dit maakt het voorgaande daarom niet anders.

Ambtshalve toetsing

3.13 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.

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

[4] Vergelijk GC Kifid 2022-1032.

Bijlage - Relevante bepalingen uit wet- en regelgeving en de algemene voorwaarden

In deze bijlage zijn opgenomen 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/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.

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

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 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 persoonlijke beveiligingsgegevens ervan te waarborgen.

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

Artikel 7:528

1. Onverminderd artikel 526, betaalt de betaaldienstverlener van de betaler, in geval van een niet-toegestane betalingstransactie, de betaler onmiddellijk het bedrag van de niet-toegestane betalingstransactie terug en in elk geval uiterlijk aan het einde van de eerstvolgende werkdag, nadat hij bekend is geworden met de transactie of daarvan in kennis is gesteld.

2. 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.