Uitspraak Geschillencommissie Financiële Dienstverlening nr. 2022-0325
(mr. E.L.A. van Emden, voorzitter en mr. P.V. Remmerswaal, secretaris)

Klacht ontvangen op	: 6 december 2021
Ingediend door	: De consument
Tegen	: Coöperatieve Rabobank U.A., gevestigd te Amsterdam, verder te noemen de bank
Datum uitspraak	: 20 april 2022
Aard uitspraak	: Niet-bindend advies
Uitkomst	: Vordering afgewezen
Bijlage	: Relevante bepalingen uit de algemene voorwaarden

Samenvatting

Helpdeskfraude. De consument is telefonisch benaderd door een persoon die zich voordeed als medewerker van Apple. Op verzoek van deze medewerker heeft hij hen toegang verleend tot zijn computer en een kleine betaling verricht. Na afloop bleek er in totaal een bedrag van € 13.201,- van zijn rekening te zijn afgeschreven. Naar het oordeel van de commissie heeft de consument zich niet gehouden aan de veiligheidsvoorschriften. Daarmee heeft hij grof nalatig gehandeld in de zin van artikel 7:529 lid 1 BW. Hij is daarom zelf aansprakelijk voor de schade. Dat de bank haar zorgplicht zou hebben geschonden is niet komen vast te staan. De vordering wordt afgewezen.

1. De procedure

1.1 De commissie beslist op basis van haar 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 en 4) de repliek van de consument.

1.2 De commissie is van oordeel dat dit geschil zich leent voor verkorte behandeling als bedoeld in artikel 32 van haar reglement. Dit betekent dat de uitspraak niet bindend is en dat partijen elkaar dus niet aan de uitspraak kunnen houden.

2. Het geschil

Wat is er gebeurd?

2.1 De consument houdt een betaalrekening aan bij de bank. Op de overeenkomst tussen partijen zijn de Algemene voorwaarden voor betalen en online diensten van de Rabobank 2020 (hierna: de algemene voorwaarden) van toepassing.

Voor de relevante bepalingen uit de algemene voorwaarden wordt verwezen naar de bijlage bij deze uitspraak.

2.2 Op 3 februari 2021 is de consument gebeld door een persoon die zich voordeed als medewerker van de helpdesk van Apple. Volgens deze persoon was er een datalek op de computer van de consument. De zogenaamde helpdeskmedewerker heeft de consument overgehaald om hem via Teamviewer toegang te geven tot zijn computer, zodat hij het probleem zou kunnen verhelpen. Vervolgens heeft hij de consument ertoe bewogen om een kleine betaling te verrichten. Daarbij heeft de consument op de website van de bank, dan wel een kopie daarvan, ingelogd. Vervolgens is in vier transacties in totaal € 13.201,- overgeboekt van de betaalrekening van de consument naar het betaalplatform PPRO Payment Service S.A. Ook heeft er een bijschrijving van € 2.000,- van een voor de consument onbekende betaalrekening plaatsgevonden. De consument zou zijn geld volgens de zogenaamde helpdeskmedewerker de volgende dag terugkrijgen. Het telefoongesprek heeft in totaal 3 tot 4 uren geduurd.

2.3 De fraudeafdeling van de bank heeft de consument op 3 februari 2021 geprobeerd te bellen vanwege een vermoeden van fraude, maar de consument nam niet op. Uit voorzorg is de betaalrekening geblokkeerd. Op 4 februari 2021 heeft de bank de consument opnieuw gebeld, dit keer met succes. Tijdens het telefoongesprek is besproken dat de consument het slachtoffer is geworden van fraude.

2.4 De consument heeft op 6 februari 2021 aangifte gedaan van het voorval. Op 15 maart 2021 heeft hij een klacht ingediend bij de bank en haar verzocht de schade te vergoeden. Dat verzoek is door de bank definitief afgewezen op 8 april 2021.

De klacht en vordering

2.5 De consument is het niet eens met het besluit van de bank om de door hem geleden schade niet te vergoeden. De bank weet dat dit soort fraude vaker voor komt, maar heeft er in het geval van de consument niets aan gedaan. De bank hoort haar klanten te beschermen tegen fraude en had de betalingen vanwege haar kennis over dit soort fraude moeten blokkeren. De consument vordert vergoeding van de schade, door hem begroot op een bedrag van € 11.000,-.

Het verweer

2.6 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

Algemeen

3.1 De vraag die centraal staat is of de schade die de consument heeft geleden door de oplichting voor rekening van de bank moet komen. De commissie beantwoordt die vraag ontkennend en licht dat hieronder toe.

Onderscheid toegestane en niet toegestane betalingstransacties

3.2 Juridisch gezien wordt een onderscheid gemaakt tussen toegestane betalingstransacties en niet-toegestane betalingstransacties. Bij een toegestane betalingstransactie is het uitgangspunt dat de consument daar zelf verantwoordelijk voor is. De bank is verplicht een betalingsopdracht die volgens de juiste voorwaarden is gegeven uit te voeren. Dit volgt uit artikel 7:533 lid 4 van het Burgerlijk Wetboek (BW).

3.3 Een transactie waarmee de consument niet heeft ingestemd, wordt volgens artikel 7:522 lid 2 van het Burgerlijk Wetboek (BW) als niet toegestaan aangemerkt. Op grond van artikel 7:528 lid 1 BW moet de bank in geval van een niet-toegestane betalingstransactie de consument onmiddellijk het bedrag van de niet-toegestane betalingstransactie terugbetalen. Op die regel bestaat een uitzondering. Volgens artikel 7:529 lid 1 BW hoeft de bank de niet-toegestane betalingstransacties niet terug te betalen als de consument frauduleus heeft gehandeld of in juridische zin opzettelijk of met grove nalatigheid één of meer verplichtingen uit hoofde van artikel 7:524 BW niet is nagekomen.[1]

3.4 De commissie zal daarom eerst vaststellen of de betreffende betalingstransacties moeten worden gekwalificeerd als toegestane of niet-toegestane betalingstransacties. De bank heeft zich onder meer verweerd door te stellen dat de consument op instructie van de oplichter zelf opdracht heeft gegeven voor en heeft ingestemd met de betalingstransacties. Derhalve is sprake van een toegestane betalingstransactie, aldus de bank.

3.5 De commissie overweegt dat uit de aangifte blijkt dat hij op instructie van de oplichter heeft ingelogd om een betaling te doen van € 7,-. Vervolgens zag hij dat er grote bedragen van zijn betaalrekening waren afgeschreven. Hieruit leidt de commissie af dat de consument niet heeft ingestemd met de betalingstransacties.

[1] Zie Commissie van Beroep Kifid, nr. 2020-027.

De omstandigheid dat de betaalopdrachten zijn gegeven volgens de met de bank afgesproken vorm en procedure, bijvoorbeeld met gebruik van bepaalde bankgegevens van de consument, staat er niet aan in de weg dat de betalingstransacties worden aangemerkt als niet toegestaan.[2] De consument heeft weliswaar verklaard te hebben ingelogd om een betaling te doen van € 7,-, maar heeft niet ingestemd met het afschrijven van een bedrag van in totaal € 13.201,-. De commissie neemt daarom tot uitgangspunt dat sprake is geweest van niet toegestane betalingstransacties.

Moet de bank het bedrag van de niet toegestane betalingstransacties vergoeden?

3.6 Zoals hiervoor onder 3.3 is overwogen, geldt als hoofdregel voor niet toegestane betalingstransacties dat de bank het bedrag van de niet toegestane betalingstransacties moet terugbetalen, tenzij de consument frauduleus heeft gehandeld of opzettelijk of met grove nalatigheid één of meer verplichtingen uit hoofde van artikel 7:524 BW niet is nagekomen. Volgens artikel 7:524 lid 1 BW moet de consument zijn betaalpas gebruiken overeenkomstig de voorwaarden die op het gebruik daarvan van toepassing zijn. In hoofdstuk 4 van de algemene voorwaarden zijn bepalingen opgenomen die betrekking hebben op de veiligheid van de betaalrekening. Daarin is onder meer opgenomen dat beveiligingscodes geheim moeten worden gehouden en dat beveiligingscodes nooit mogen worden doorgegeven per telefoon, e-mail of op een andere manier dan uitdrukkelijk door de bank voorgeschreven. Dat geldt ook als de consument telefonisch, per e-mail of persoonlijk door iemand wordt benaderd die aangeeft medewerker van de bank of andere dienstverlener te zijn. Daarnaast moet de consument zorg dragen voor een goede beveiliging van de apparatuur die hij gebruikt voor zijn bankzaken.

3.7 De commissie moet beoordelen of de consument – in juridische zin – grof nalatig heeft gehandeld met betrekking tot het naleven van deze veiligheidsvoorschriften. Vast staat dat de consument de persoon die zich voordeed als een medewerker van Apple de toegang heeft verleend tot zijn computer. Ook staat vast dat de consument op verzoek van deze persoon heeft ingelogd op een door hem klaargezette website. Daarmee heeft de consument de hierboven genoemde veiligheidsvoorschriften niet in acht genomen. Het gevolg daarvan is dat de consument – in juridische zin – grof nalatig heeft gehandeld met betrekking tot het naleven van de veiligheidsvoorschriften. Hij is daarom zelf aansprakelijk voor de schade die hij heeft geleden door de betalingstransacties.[3]

---

[2] Hoge Raad 21 mei 2021, ECLI:NL:HR:2021:749, r.o. 3.2.2.
[3] Zie ook Geschillencommissie Kifid, nrs. 2022-0172 en 2022-0031.

Schending zorgplicht?

3.8 Naar de commissie begrijpt heeft de consument verder gesteld dat de bank een op haar rustende zorgplicht heeft geschonden door hem niet te behoeden voor de fraude. De commissie overweegt dat de bank is opgetreden als betaaldienstverlener. De rol van de bank als betaaldienstverlener is in beginsel beperkt tot het optimaliseren van het betalingsverkeer. De op de bank rustende zorgplicht strekt niet zo ver dat zij verplicht is om in het algemeen betalingstransacties te monitoren. Ook is zij niet verplicht onderzoek te doen naar de begunstigde van een betaling. Wel kan van de bank worden verwacht dat zij tot onderzoek zou overgaan indien zij op de hoogte was van ongebruikelijk betalingsverkeer, alsmede het daaraan verbonden gevaar. Bepalend is datgene waar de bank zich daadwerkelijk van bewust was.[4] Het is de commissie niet gebleken dat de bank zich daadwerkelijk bewust was van enig gevaar op het moment dat zij de betalingstransacties uitvoerde. Voor de bank bestond daarom geen aanleiding om in te grijpen door de betalingen te blokkeren. Dat de bank haar zorgplicht zou hebben geschonden is daarom niet komen vast te staan.

Conclusie

3.9 Hoewel de commissie betreurt dat de consument zijn geld kwijt is, is zij van oordeel dat de klacht ongegrond is. De vordering wordt afgewezen.

4. De beslissing

De commissie wijst de vordering af.

Deze uitspraak is een niet-bindend advies, omdat deze beslissing is genomen in een verkorte procedure. Meer informatie hierover staat in artikel 32 van het reglement, te vinden op de website van Kifid (www.kifid.nl/reglementen-en-statuten).. Tegen deze uitspraak staat geen hoger beroep open bij de Commissie van Beroep Financiële Dienstverlening. U kunt de zaak nog wel aan de rechter voorleggen.

Binnen twee weken na de verzenddatum van deze uitspraak kunt u een schriftelijk verzoek indienen tot herstel van vergissingen in de uitspraak zoals schrijffouten, een verkeerde naam/datum of rekenfouten. De beslissing van de geschillencommissie in de uitspraak kan hiermee niet ter discussie worden gesteld. Binnen een maand na de verzenddatum van de uitspraak kunt u een schriftelijk verzoek indienen om de uitspraak aan te vullen als u vindt dat de geschillencommissie niet heeft beslist over alle onderdelen van uw vordering. Dit ziet niet op de situatie waarin u meent dat de geschillencommissie in haar uitspraak niet uitdrukkelijk al uw argumenten, ter onderbouwing van uw vordering, heeft behandeld. Meer informatie hierover staat in artikel 40 van het reglement van de geschillencommissie, te vinden op de website www.kifid.nl/reglementen-en-statuten.

[4] Zie Hoge Raad 27 november 2015, ECLI:NL:HR:2015:3399. Zie ook Geschillencommissie Kifid, nrs. 2019-531, 2020-086, 2020-150, 2021-0502, 2021-0957.

Bijlage - Relevante bepalingen uit de algemene voorwaarden

Boek 7 van het Burgerlijk Wetboek Artikel 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 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 529 lid 1

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.

De Algemene voorwaarden voor betalen en online diensten van de Rabobank 2020

Hoofdstuk 4
Veiligheid

1. Inleiding - waarover gaan deze regels?
Elektronisch bankieren en elektronisch betalen moeten veilig zijn. Denk aan Rabo Online Bankieren, Rabofoon, betalen bij betaalautomaten in winkels en geld opnemen bij de geldautomaat. Dit geldt ook voor het gebruik van online diensten, zoals iDIN. Wij hebben hierin een belangrijke taak, maar u ook. Wat u moet doen, vindt u in deze veiligheidsregels.

2. Waarom is het belangrijk dat u zich houdt aan deze regels?
U vermindert de kans dat u het slachtofer 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.

3. Wat moet u doen?
1 Houd uw beveiligingscodes geheim
2 Zorg ervoor dat een ander uw betaalpas, creditcard en NFC-telefoon 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 mPIN die u in combinatie met de betaalpas, creditcard of NFC-telefoon 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, de Rabo Wallet 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 en de driecijferige code achterop uw creditcard (de CVC-code).

• U mag deze beveiligingscodes alleen zelf gebruiken. U moet dat doen op de manier die wij aangeven.

• 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 NFC-telefoon 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 mPIN, maar ook om alle andere codes die u moet gebruiken om elektronische betalingen te doen en/ of gebruik te maken van Rabo Online Bankieren, de Rabo Wallet en Rabofoon.

• Geef nooit een beveiligingscode door per telefoon, e-mail, op een website of in een app anders dan die van de 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 van de bank te zijn. Wij zullen u op deze wijze nooit om beveiligingscodes vragen.

• Zorg er ook voor dat iemand anders geen vingerafdruk of gezicht kan toevoegen die gebruikt kan worden voor Rabo Online Bankieren of de Rabo Wallet (in de toekomst).

2 Zorg ervoor dat een ander uw betaalpas, creditcard en NFC-telefoon nooit gebruikt Denk hierbij aan het volgende:
• Laat u niet afeiden als u uw betaalpas, creditcard of NFC-telefoon gebruikt en controleer of u uw eigen betaalpas, creditcard of NFC-telefoon daarna terugkrijgt.

• Berg de betaalpas, creditcard en NFC-telefoon altijd op een veilige plaats op en zorg ervoor dat u deze niet gemakkelijk kunt verliezen.

• Controleer regelmatig of u de betaalpas, creditcard en NFC-telefoon 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.