

**Uitspraak Geschillencommissie Financiële Dienstverlening nr. 2013-343 d.d. 16 oktober 2013
(prof.mr. C.E. du Perron en mevrouw mr. M. van Pelt, secretaris)**

Samenvatting

Consument is telefonisch benaderd door een persoon die zich voordeed als een medewerker van de bank. Tijdens dit gesprek heeft Consument de beveiligingscodes van haar betaalrekening aan de medewerker doorgegeven. Later is gebleken dat hier geen sprake was van een bankmedewerker en dat er grote bedragen aan de rekening zijn onttrokken. Consument vordert de schade van de bank, omdat de bank toerekenbaar tekortgeschoten zou zijn in de nakoming van haar verplichtingen jegens Consument. Consument stelt onder meer dat zij niet wist dat de optie bestond om hoge bedragen naar het buitenland over te maken zonder extra controle en zij had deze mogelijkheid niet willen toestaan. De Commissie oordeelt dat Consument, hoewel zij slachtoffer is geworden van een gewiekste handelwijze van criminelen, door het mededelen van de beveiligingscodes met grove nalatigheid een of meer verplichtingen voor het veilig gebruik van het betrokken betaalinstrument niet is nagekomen. Zij neemt daarbij in aanmerking dat, zoals de Bank voldoende gemotiveerd en onvoldoende weersproken heeft gesteld, de Bank en de NVB consumenten voor deze en vergelijkbare vormen van fraude concreet en indringend hebben gewaarschuwd. Vervolgens overweegt de Commissie dat banken de zorgplicht hebben zich voortdurend in te spannen om consumenten tegen bestaande en nieuwe vormen van fraude te beschermen. De vordering wordt afgewezen.

Consument,

tegen

de coöperatie Coöperatieve Rabobank Twente Oost U.A., gevestigd te Oldenzaal, hierna te noemen Aangeslotene.

I. Procesverloop

De Commissie beslist met inachtneming van haar reglement en op basis van de volgende stukken:

- het dossier van de Ombudsman Financiële Dienstverlening;
- het door Consument ondertekende vragenformulier, ontvangen op 25 februari 2013;
- de brief van Consument van 30 januari 2013 met bijlagen;
- het verweerschrift van Aangeslotene.

Tussenkost van de Ombudsman Financiële Dienstverlening heeft niet tot oplossing van het geschil geleid.

Beide partijen zullen het advies van de Commissie als bindend aanvaarden.

Partijen zijn opgeroepen voor een mondelinge behandeling op vrijdag 20 september 2013. En zijn aldaar verschenen.

2. Feiten

De Commissie gaat uit van de volgende feiten:

- 2.1. Consument houdt bij Aangeslotene een rekening aan. Deze rekening is gekoppeld aan de overeenkomst Rabo Internetbankieren. Op het gebruik van Rabo Internetbankieren en de rekening zijn van toepassing de Algemene voorwaarden voor betaalrekeningen en betaaldiensten Rabobank 2011 (hierna: de Voorwaarden). Tevens zijn de Algemene Bankvoorwaarden van toepassing. Voor de rekening gold een kredietlimiet van circa 13.000 euro. De kredietlimiet stond vermeld op de rekeningafschriften die Consument van Aangeslotene ontving.
- 2.2. Uit het proces-verbaal van aangifte van 3 juni 2011 blijkt dat Consument op dinsdag 31 mei 2011 tussen 13.30 en 14.00 uur werd gebeld door een vrouw die zich voordeed als een medewerkster van Aangeslotene. De vrouw gaf zich uit als medewerkster van Rabobank Limburg. Consument vroeg toen: "Jullie zitten toch in Eindhoven?", waarop de vrouw bevestigend antwoordde. De vrouw vroeg vervolgens of het rekeningnummer xx.000 van Consument was, waarop Consument bevestigend antwoordde. De vrouw deelde Consument mee dat zij een nieuwe code zou krijgen op de zwarte strip van haar bankpas.
- 2.3. De vrouw vroeg Consument om haar bankpas in haar Random Reader te plaatsen en na het indrukken van de i-toets, de code in te voeren. De code die vervolgens in het scherm van de Random Reader tevoorschijn kwam, heeft Consument op verzoek van de vrouw aan de vrouw doorgegeven. Op dezelfde manier heeft Consument de s-code gegenereerd en doorgegeven. Consument heeft deze procedure drie keer herhaald. De pincode heeft Consument tijdens dit telefoongesprek niet aan de vrouw verstrekt.
- 2.4. Consument heeft meerdere keren aan de telefoon gezegd dat zij het niet vertrouwdde. De vrouw verzekerde haar dat het wel vertrouwd was. De vrouw zei in het gesprek ook dat Consument diezelfde dag voor 20.00 uur 's avonds niet mocht internetbankieren.
- 2.5. Op woensdag 1 juni 2011 omstreeks 14.30 uur heeft Consument met Aangeslotene gebeld om te vragen of het klopte dat zij gebeld was door een bankmedewerkster. Aangeslotene wees Consument er toen op dat er grote bedragen van haar rekening waren afgeschreven. Er had op dinsdag 31 mei 2011 een spoedoverboeking van €11.111,99 naar een buitenlandse bankrekening plaatsgevonden, alsmede een spoedoverboeking van € 6.000,- naar een binnenlandse bankrekening. Aangeslotene heeft van de binnenlandse overboeking nog € 4.876,- kunnen veiligstellen en heeft dit bedrag teruggestort aan Consument.
- 2.6. In de Algemene Bankvoorwaarden is – voor zover relevant – het volgende bepaald:

Artikel 18

"Tegenover de cliënt strekt een uittreksel uit de administratie van de bank tot volledig bewijs, behoudens door de cliënt gevoerd tegenbewijs. De bank behoeft haar administratie niet langer te bewaren dan de wettelijke bewaartermijnen."

Artikel 21 lid 1:

"De cliënt moet aan hem ter beschikking gestelde middelen zoals formulieren, informatiedragers, communicatie- en beveiligingsmiddelen, passen, pin- en toegangscode en wachtwoorden zorgvuldig bewaren en behandelen. De cliënt moet met persoonlijke pin- en toegangscode en dergelijke zorgvuldig omgaan en deze geheim houden voor andere personen. De cliënt houdt zich aan de door de bank gegeven beveiligingsvoorschriften."

In Hoofdstuk 4 van de Voorwaarden is – voor zover relevant – het volgende bepaald:

Artikel 7:

“I U bent gebonden aan alle (rechts)handelingen die met uw bankpas en/of uw beveiligingscode via een elektronische dienst zijn verricht. Rechtshandelingen zijn bijvoorbeeld het sluiten van een overeenkomst of het geven van een betaalopdracht.”

Artikel 9:

“I Rabo Internetbankieren kunt u gebruiken als wij dat met u hebben afgesproken.

2 Rabo Internetbankieren kunt u via internet gebruiken. U heeft daarom een verbinding met het internet nodig. En geschikte apparatuur en software om die verbinding te kunnen gebruiken.

3 U heeft een bankpas met bijbehorende pincode nodig om Rabo Internetbankieren te kunnen gebruiken. Wij delen u mee welke bankpas dit is.

4 Als u naar de beveiligde omgeving van Rabo Internetbankieren gaat, krijgt u aanwijzingen over hoe u kunt inloggen met de I-code, hoe u opdrachten kunt verzenden of over hoe u afspraken kunt bevestigen met de S-code. Als u elektronisch bankiert, moet u voortdurend controleren of de internetpagina nog is beveiligd. U kunt dat zien aan de adresbalk. Het adres moet beginnen met ‘https’. U kunt het ook zien aan het hangslotje op de balk onder aan de internetpagina. U mag de I-code en de S-code alleen gebruiken voor Rabo Internetbankieren en voor andere (bank)zaken die u met ons en derden doet via onze website. U mag deze (beveiligings)codes niet aan anderen (inclusief familie, vrienden) bekend maken, ook niet aan anderen die hun diensten aanbieden via internet en die om deze codes vragen. U moet ook zorgen dat anderen deze codes niet kunnen afkijken.”

In Hoofdstuk 5 van de Voorwaarden is – voor zover relevant – het volgende bepaald:

Artikel 7:

“I U kunt geld overboeken van uw rekening naar een rekening van een begunstigde door ons een betaalopdracht te geven. Dat kan een rekening zijn in Nederland of in het buitenland. (...)”

In Hoofdstuk 6 van de Voorwaarden is – voor zover relevant – het volgende bepaald:

Artikel 4 lid 5:

“Voor het geven van betaalopdrachten met Rabo Internetbankieren geldt een limiet van € 50.000,- per S-code, tenzij wij met u andere afspraken hebben gemaakt.”

3. De vordering en grondslagen

- 3.1. Consument vordert dat Aangeslotene wordt veroordeeld tot vergoeding van de door haar geleden schade ten gevolge van telefonische “phishing”, ter grootte van een bedrag van €12.236,-, en te vermeerderen met de wettelijke rente vanaf 31 mei 2011.
- 3.2. Deze vordering steunt kort en zakelijk op de volgende grondslagen:
 - Aangeslotene is toerekenbaar tekortgeschoten in de nakoming van haar verplichtingen jegens Consument. Aangeslotene had als goed dienstverlener ervoor dienen te zorgen dat de gegevens uit haar systeem ontoegankelijk zijn voor onbevoegde derden, zodat klanten niet op het verkeerde been worden gezet en ten onrechte erop vertrouwen een medewerkster van Aangeslotene aan de telefoon te hebben.
 - Aangeslotene heeft een zorgplicht geschonden ten aanzien van de mogelijkheid om vanaf de rekening van Consument hoge bedragen naar het buitenland over te maken zonder enige extra controle. Consument wist niet dat deze optie bestond en had deze mogelijkheid niet willen toestaan.
 - Aangeslotene heeft een zorgplicht geschonden door de zeer hoge kredietlimiet te laten bestaan, terwijl Consument jaren geen gebruik hiervan had gemaakt en hiervan ook geen gebruik wilde maken.
 - Consument mocht gerechtvaardigd vertrouwen op de uitspraak van de NVB dat banken instaan voor vergoeding van de door hun cliënten geleden schade als gevolg van computercriminaliteit.
- 3.3. Aangeslotene heeft de stellingen van Consument gemotiveerd weersproken. Voor zover nodig zal de Commissie bij de beoordeling daarop ingaan.

4. Beoordeling

Juridisch kader

- 4.1. Volgens artikel 7:529 van het Burgerlijk Wetboek komen bij een geval van fraude zoals dat zich in deze zaak heeft voorgedaan de verliezen boven het eigen risico van €150,- alleen voor rekening van de betaler indien deze verliezen zijn veroorzaakt doordat de betaler frauduleus heeft gehandeld of opzettelijk of met grove nalatigheid – kort gezegd – een of meer verplichtingen voor het veilig gebruik van het betrokken betaalinstrument niet is nagekomen.
- 4.2. In artikel 21 lid 1 van de Algemene Bankvoorwaarden is bepaald dat een cliënt zorgvuldig dient om te gaan met de persoonlijke pin- en toegangscode en deze geheim dient te houden voor andere personen. In artikel 9 van hoofdstuk 4 van de toepasselijke Voorwaarden is bepaald dat de kaarthouder de (beveiligings)codes niet aan anderen bekend mag maken, ook niet aan anderen die om deze codes vragen. In artikel 7 van hoofdstuk 4 van de toepasselijke Voorwaarden is bepaald dat de consument gebonden is aan alle (rechts)handelingen die met zijn bankpas en/of zijn beveiligingscode via een elektronische dienst zijn verricht. Tegenover de cliënt geldt ingevolge artikel 18 van de Algemene Bankvoorwaarden de administratie van de bank als volledig bewijs, behoudens tegenbewijs.
- 4.3. Vaststaat dat Consument slachtoffer is geworden van fraude. De vraag die moet worden beantwoord is of deze fraude mogelijk is gemaakt doordat Consument met grove nalatigheid een of meer verplichtingen voor het veilig gebruik van het betrokken betaalinstrument niet is nagekomen. De Commissie stelt daarbij voorop dat van consumenten die gebruik maken van het betalingsverkeer mag worden verwacht dat zij voldoende zorgvuldigheid betrachten ten aanzien van de verstrekte betaalinstrumenten en veiligheidscodes. Bij de toepassing van deze maatstaf komt het aan op alle omstandigheden van het geval, waarbij de gemiddelde consument als maatstaf dient te worden genomen. Tevens dient er rekening mee te worden gehouden dat criminelen steeds nieuwe uiterst geraffineerde trucs bedenken om de beveiligingssystemen van banken te omzeilen, waarbij zij de medewerking van consumenten proberen te verwerven. Daarom is mede van belang of consumenten zijn voorgelicht over vormen van criminaliteit die zij zonder deze voorlichting niet hadden behoeven te doorzien.
Waarschuwing door Aangeslotene
- 4.4. Aangeslotene heeft gemotiveerd gesteld dat Aangeslotene haar klanten als sinds begin mei 2010 waarschuwt voor phishing. Zo worden er door Aangeslotene berichten op Rabo Internetbankieren geplaatst om klanten onder andere te wijzen op frauduleuze e-mails en de wijze waarop klanten benaderd kunnen worden door criminelen. Hierbij wordt gewaarschuwd voor personen die zich via de telefoon voordoen als bankmedewerker. Klanten zien dergelijke waarschuwingen wanneer zij inloggen op Rabo Internetbankieren. Enige tijd werd ook de volgende pop-up-melding getoond:
“Pas op dat u geen persoonlijke beveiligingscodes per telefoon afgeeft! U kunt namelijk worden benaderd door een persoon die zich uitgeeft voor een medewerk(st)er van de Rabobank. Ga niet in op telefonische verzoeken om bijvoorbeeld de I-code en S-code van uw Random Reader te verstrekken. Wanneer u de I-code en S-code verstrekt, geeft u criminelen de mogelijkheid om

geld van uw rekening(en) over te schrijven. Vraag in dat geval de naam van deze personen en bel zelf uw Rabobank terug. Gebruik voor het zoeken van het telefoonnummer van uw Rabobank de informatiepagina op deze website of gebruik het telefoonboek. Het telefoonnummer van uw Rabobank kan nooit een mobiel (06) nummer zijn!”

- 4.5. Ook verwijst Aangeslotene naar de publiekscampagnes van de Nederlandse Vereniging voor Banken (hierna: NVB). In de landelijke campagne ‘3x kloppen’ zijn consumenten gewezen op internetcriminaliteit.
Grove nalatigheid Consument
- 4.6. Consument heeft tijdens de zitting erkend niet overeenkomstig de toepasselijke voorwaarden te hebben gehandeld door de beveiligingscodes (telefonisch) aan een derde door te geven. Met de door Consument verstrekte beveiligingscodes heeft de onbekende vrouw immers kunnen inloggen in Rabo Internetbankieren en gelden van de rekening van Consument kunnen overboeken naar rekeningen van derden. De Commissie oordeelt dat Consument, hoewel zij slachtoffer is geworden van een gewiekste handelwijze van criminelen, door het mededelen van de beveiligingscodes met grove nalatigheid een of meer verplichtingen voor het veilig gebruik van het betrokken betaalinstrument niet is nagekomen. Zij neemt daarbij in aanmerking dat, zoals Aangeslotene voldoende gemotiveerd en onvoldoende weersproken heeft gesteld, Aangeslotene en de NVB consumenten voor deze en vergelijkbare vormen van fraude concreet en indringend hebben gewaarschuwd.
Gegevens van Consument
- 4.7. Ter zitting is niet duidelijk geworden hoe de criminelen in kwestie de beschikking hebben gekregen over het juiste rekeningnummer en de naam van Consument, wat hen in staat stelde vertrouwen bij Consument te wekken. Consument stelt deze gegevens niet met derden gedeeld te hebben. Aangeslotene betwist dat de gegevens van haar afkomstig zijn en merkt op dat bijvoorbeeld adresgegevens, geboortedata en rekeningnummers geen geheime gegevens zijn. Naar het oordeel van de Commissie kunnen dergelijke gegevens inderdaad ook ter kennis van de criminelen gekomen zijn zonder dat sprake was van een lek in het systeem van Aangeslotene. Dat geldt niet in dezelfde mate voor andere gegevens waarover de vrouw aan de telefoon volgens Consument beschikte, te weten het actuele saldo van de rekeningen van Consument en het nummer van haar spaarrekening. Ter zitting is echter gebleken dat de vrouw aan de telefoon pas opmerkte hoe hoog het saldo was en het nummer van de spaarrekening noemde, nadat Consument haar de i-code had doorgegeven. Daarmee had de vrouw toegang tot de gegevens van Consument verkregen. Het is dan ook niet komen vast te staan dat Aangeslotene een verwijt valt te maken van het feit dat deze gegevens bij de criminelen bekend waren.
Mogelijkheid tot buitenlandse overboekingen
- 4.8. Consument voert verder aan dat Aangeslotene een zorgplicht heeft geschonden ten aanzien van de mogelijkheid om, zonder enige extra controle, vanaf de rekening van Consument hoge bedragen naar het buitenland over te maken. Consument wist niet dat deze optie bestond en had dit niet willen toestaan. Aangeslotene betwist dit en voert aan dat in artikel 7 lid 1 van hoofdstuk 5 van de Voorwaarden is bepaald dat Consument de mogelijkheid heeft om gelden over te boeken naar rekeningen in binnen- en

buitenland. Gelet op deze bepaling in de Voorwaarden treft dit betoog van Consument geen doel. Dit wordt niet anders doordat banken als Aangeslotene de zorgplicht hebben zich voortdurend in te spannen om Consumenten tegen bestaande en nieuwe vormen van fraude te beschermen. Daarbij is niet uitgesloten dat deze verplichting meebrengt dat banken fraude door ongewenste buitenlandse transacties moeten voorkomen of bemoeilijken door deze transacties, al dan niet in bepaalde gevallen, te blokkeren, of door het voor klanten mogelijk te maken een blokkade in te stellen. Waartoe banken gehouden zijn, zal onder meer afhangen van de omvang van dit type van fraude, de bezwaarlijkheid van de veiligheidsmaatregelen, de mogelijkheden voor criminelen om eventuele veiligheidsmaatregelen te omzeilen en de mogelijkheden voor Consumenten om de bewuste fraude zelf te voorkomen. Bij de benodigde afweging moet bovendien voorkomen worden dat op basis van inzichten van nu verplichtingen tot het treffen van veiligheidsmaatregelen in het verleden worden aangenomen. In het licht hiervan, en gelet op hetgeen partijen hebben aangevoerd, oordeelt de Commissie dat onvoldoende gronden zijn gebleken om aan te nemen dat de door Consument verdedigde blokkadeplicht ten tijde van de fraude op Aangeslotene rustte.

Hoge kredietlimiet

- 4.9. Consument betoogt dat Aangeslotene een zorgplicht heeft geschonden door de zeer hoge kredietlimiet te laten bestaan, terwijl Consument hiervan al jaren geen gebruik had gemaakt en hiervan ook geen gebruik meer wilde maken. Aangeslotene wijst erop dat Consument zelf de kredietlimiet heeft aangevraagd en derhalve zelf deze limiet had moeten beperken of opzeggen. Aangeslotene stelt dat de limiet zichtbaar is op de rekeningoverzichten en bij elke geldopname bij een geldautomaat van Aangeslotene. Ter zitting is gebleken dat de kredietlimiet vermeld stond op de rekeningafschriften die Aangeslotene aan Consument zond. De Commissie oordeelt dat nu Consument de kredietlimiet zelf heeft aangevraagd, en de hoogte daarvan uit de afschriften kon kennen, het op haar weg had gelegen deze kredietlimiet naar beneden aan te passen. De Commissie zijn thans onvoldoende gronden gebleken om een verplichting voor Aangeslotene aan te nemen om Consument tegen het frauderisico van een hoge kredietlimiet te beschermen.

Mededeling NVB

- 4.10. Consument beroept zich op de mededeling van de NVB dat de banken instaan voor vergoeding van de door hun cliënten geleden schade als gevolg van computercriminaliteit. De Commissie overweegt als volgt. Naar ook in latere nuanceringen door de NVB is bevestigd, moet deze uitlating in redelijkheid aldus worden volstaan, dat banken de schade zullen vergoeden, behalve indien consumenten een ernstig verwijt van de fraude gemaakt kan worden. (Zie Geschillencommissie Kifid 2013/117, ro. 4.3. en 2013/240, r.o. 4.12 en Rechtbank Breda 23 maart 2011, HA-ZA 10-1582, r.o. 3.7). Een en ander is in overeenstemming met de wettelijke regeling. Nu Consument in deze zaak grof nalatig heeft gehandeld in het licht van de voorwaarden, kan in het midden blijven of zij aan uitlatingen van de NVB rechten tegenover Aangeslotene zou kunnen ontlenuen.
- 4.11. Gelet op het hiervoor overwogene dient de vordering van Consument te worden afgewezen.

5. Beslissing

De Commissie wijst bij bindend advies de vordering van Consument af.

In artikel 5 van het Reglement van de Commissie van Beroep Financiële Dienstverlening is bepaald in welke gevallen beroep openstaat van beslissingen van de Geschillencommissie Financiële Dienstverlening bij de Commissie van Beroep Financiële Dienstverlening. Daarbij geldt een termijn van zes weken na verzending van deze uitspraak. Op de website van Kifid vindt u praktische informatie over het instellen van beroep. Zie hiervoor kifid.nl/consumenten/wie-behandelt-mijn-klacht/4#stappen-plan.