

**Uitspraak Geschillencommissie Financiële Dienstverlening nr. 2013-240
d.d. 23 juli 2013
(mr. C.E. du Perron, voorzitter en mevrouw mr. M. Nijland, secretaris)**

Samenvatting:

Consument heeft een e-mailbericht ontvangen waarvan hij dacht dat het afkomstig was van de bank. In het bericht heeft hij op een link geklikt, waarna hij werd doorverwezen naar een scherm dat leek op het inlogscherf van Rabo Internetbankieren. In dit scherm verscheen het verzoek zijn naam, geboortedatum en telefoonnummer in te vullen. Dit heeft hij gedaan. Vervolgens is Consument telefonisch benaderd door een persoon die zich voordeed als een medewerker van de bank. Tijdens dit gesprek heeft Consument de beveiligingscodes van zijn 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 had niet eerder van deze vorm van fraude gehoord en vordert de schade van de bank. De Commissie overweegt als volgt. Gelet op de vertrouwensbeschermende functie van de aansprakelijkheidsverdeling kan de schade boven het eigen risico uitsluitend ten laste van Consument gebracht worden als deze het gevolg is van zijn grove nalatigheid. Daarbij dient de gemiddelde consument als maatstaf te worden genomen. De omstandigheden van het geval zijn hierbij van belang, waarbij het een rol speelt in hoeverre consumenten zijn voorgelicht over vormen van criminaliteit die zij zonder deze voorlichting niet hadden hoeven te voorzien. In dit geval heeft de bank voldoende aangetoond dat Consument onmiskenbaar gewaarschuwd is voor deze vorm van criminaliteit. Dat hij geen kennis heeft genomen van de waarschuwingen is een omstandigheid die voor zijn eigen rekening en risico dient te blijven. De vordering wordt afgewezen.

Consument,

en

de Coöperatieve Rabobank De Kempen West U.A., gevestigd te Bladel, 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 verzoek tot geschilbeslechting van 19 juni 2012;
- het verweerschrift van Aangeslotene;
- de repliek van Consumenten;
- de dupliek van Aangeslotene;
- de brief van Consument van 6 mei 2013;
- de brief van Aangeslotene van 24 mei 2013; en
- de reactie daarop van Consument van 11 juni 2013.

De Commissie stelt vast dat tussenkomst van de Ombudsman Financiële Dienstverlening niet tot oplossing van het geschil heeft geleid en dat partijen het advies van de Commissie als bindend aanvaardden.

Partijen zijn opgeroepen voor een mondelinge behandeling op vrijdag 12 april 2013 en zijn aldaar verschenen.

2. Feiten

De Commissie gaat uit van de volgende feiten:

- 2.1. Een vereniging houdt een bankrekening aan bij Aangeslotene. Bij deze rekening hoort een betaalpas welke Consument, in zijn hoedanigheid van penningmeester, in zijn bezit heeft.
- 2.2. Op 1 juni 2011 heeft Consument een e-mailbericht ontvangen waarvan hij dacht dat het afkomstig was van Aangeslotene. In het bericht heeft hij op een link geklikt, waarna hij werd doorverwezen naar een scherm dat leek op het inlogscherf van Rabo Internetbankieren. In dit scherm verscheen het verzoek zijn naam, geboortedatum en telefoonnummer in te vullen. Dit heeft Consument vervolgens gedaan.
- 2.3. Op 7 juni 2011 is Consument 's morgens telefonisch benaderd door een vrouw die zich voordeed als een medewerkster van Aangeslotene. Op verzoek van de vrouw heeft Consument de betaalpas van de vereniging in de Random Reader geplaatst. Vervolgens heeft hij de pincode ingetoetst, waarna de I-code verscheen. Deze inlogcode heeft hij doorgegeven aan de vrouw. Op dezelfde manier heeft Consument een S-code gegenereerd die hij ook aan de vrouw heeft doorgegeven.
- 2.4. Om 13:21 uur van diezelfde dag heeft een medewerker van Aangeslotene telefonisch contact opgenomen met Consument en hem erop gewezen dat er een aantal transacties ten laste van de rekening van de vereniging was verricht. Om 12:30 uur twee binnenlandse overboekingen van elk € 5.130,- en om 13:10 uur een spoedoverboeking naar het buitenland van € 9.753,-.
- 2.5. Omdat Consument niet op de hoogte was van deze transacties heeft de afdeling Crisismanagement & Fraudebestrijding van Aangeslotene de overboekingen proberen te annuleren. Bij de twee binnenlandse overboekingen is zij hierin geslaagd en heeft zij de bedragen kunnen veiligstellen. Voor de buitenlandse overboeking heeft zij om 15:41 uur een zogenoemd SWIFT-bericht aan de begunstigde bank van de overboeking verzonden en verzocht de betrokken rekening te blokkeren. Op 20 juni 2011 heeft de buitenlandse bank medegedeeld dat het geld reeds was opgenomen.
- 2.6. Op de overeenkomst zijn van toepassing de Algemene voorwaarden voor betaalrekeningen en betaaldiensten van de Rabobank 2011 (hierna: de Voorwaarden), alsmede de Algemene Bankvoorwaarden.

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

Artikel 7:

“1 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:

“1 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 7 van de Voorwaarden is – voor zover relevant – het volgende bepaald:

Artikel 9:

“1 U bent aansprakelijk voor de gevolgen van het gebruik van een kaart.

2 Bij onbevoegd gebruik na verlies of diefstal van de kaart bent u in ieder geval aansprakelijk tot € 150,- per kaart voor onbevoegde transacties die zijn gedaan tot het moment van melding van een incident.

3 Daarnaast bent u aansprakelijk:

a als blijkt dat u een incident met de kaart niet meteen heeft gemeld toen u van dat incident wist. Voor alle onbevoegde transacties die vanaf dat moment tot aan het moment van melding zijn gedaan, bent u aansprakelijk;

b als blijkt dat de onbevoegde transacties konden gebeuren omdat u uw pincode niet geheim heeft gehouden. Of doordat een mederekeninghouder of de gevolmachtigde zijn pincode niet geheim heeft gehouden. U bent dan aansprakelijk voor alle onbevoegde transacties die vóór de melding zijn gedaan;

c voor onbevoegde transacties die zijn gedaan vanaf de derde werkdag waarop deze transacties op een rekeningoverzicht of transactieoverzicht zijn vermeld, tot het moment waarop u een incident met de kaart heeft gemeld.

4 U bent in ieder geval aansprakelijk als het gebruik heeft kunnen plaatsvinden door opzet, grove schuld of grove nalatigheid van u, een andere rekeninghouder of een gevolmachtigde. Of als u, een andere rekeninghouder of gevolmachtigde frauduleus heeft gehandeld.”

In artikel 21 lid 1 van de Algemene Bankvoorwaarden is bepaald:

“De cliënt moet aan hem ter beschikking gestelde middelen zoals formulieren, informatie-dragers, 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.”

3. Geschil

- 3.1. Consument vordert dat Aangeslotene wordt veroordeeld een bedrag van € 9.753,- te betalen. Aan deze vordering legt Consument ten grondslag dat Aangeslotene gehouden is tot nakoming van de rekening-courant overeenkomst. Consument erkent dat hij de I-en S-codes aan de onbekende vrouw heeft verschaft, maar vindt dat Aangeslotene hem onvoldoende voor deze vorm van criminaliteit heeft gewaarschuwd. Pas twee uur na de onbevoegde transacties heeft Aangeslotene een SWIFT-bericht aan de buitenlandse bank verzonden. Bovendien heeft Aangeslotene geweigerd de bankgegevens van de buitenlandse bank aan hem te verstrekken waardoor het hem belemmerd werd om zelf actie te ondernemen.
- 3.2. Aangeslotene heeft de stellingen van Consument gemotiveerd weersproken. Voor zover nodig zal de Commissie bij de beoordeling daarop ingaan.

4. Beoordeling

- 4.1. Naar aanleiding van het over en weer door partijen gestelde overweegt de Commissie als volgt.
- 4.2. Volgens art. 7:529 BW 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 Consument indien deze verliezen zijn veroorzaakt doordat Consument 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.
- 4.3. 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. Voorts is in artikel 5 van hoofdstuk 7 van de Voorwaarden bepaald dat een kaarthouder zorgvuldig met zijn bankpas en pincode dient om te gaan. Van zorgvuldig gebruik is sprake als de betaalpas zo wordt opgeborgen dat anderen hem niet ongemerkt kunnen pakken. In artikel 9 van ditzelfde hoofdstuk is bepaald dat een kaarthouder bij onbevoegd gebruik van de betaalpas of pincode in ieder geval aansprakelijk is tot € 150,-, tot het moment van melding van het incident. De beperking van de aansprakelijkheid vervalt volgens de voorwaarden indien het gebruik heeft kunnen plaatsvinden door opzet, grove schuld of grove nalatigheid van de rekeninghouder of gevolmachtigde.

- 4.4. Vaststaat dat Consument slachtoffer is geworden van fraude. De vraag die moet worden beantwoord is of deze fraude mogelijk is gemaakt doordat Consument grof nalatig heeft gehandeld ten aanzien van de veiligheidsvoorwaarden. 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 in hoeverre consumenten zijn voorgelicht over vormen van criminaliteit die zij zonder deze voorlichting niet hadden behoeven te doorzien.
- 4.5. Op verzoek van de Commissie heeft Aangeslotene bij brief van 24 mei 2013 een overzicht verstrekt van de waarschuwingen voor het gevaar van phishing en de wijze waarop consumenten daar kennis van konden nemen. Uit het overzicht blijkt dat klanten die binnen een bepaalde periode inlogden in hun persoonlijke Rabo Internetbankierenomgeving, een waarschuwing te zien kregen in de vorm van een pop-up bericht. Deze pop-up diende de klant eerst weg te klikken (button “ga verder”) alvorens verder gebruik te kunnen maken van Rabo Internetbankieren. De betwiste transacties hebben plaatsgevonden op 7 juni 2011. De pop-ups werden vanaf 15 juni 2010 regelmatig ververs.
- 4.6. Verder blijkt uit het overzicht dat op 8 februari 2011 het volgende pop-up bericht met het onderwerp “Fraude via telefoon en e-mail” is geplaatst:
“Let op dat u nooit uw persoonlijke beveiligingscodes per telefoon afgeeft! Ook niet aan personen die zich uitgeven als Rabobankmedewerker. De Rabobank zal ook nooit via e-mail vragen naar uw (persoonlijke) beveiligingscodes: dit zijn bijvoorbeeld de I-code en S-code van uw Random Reader of pincode van uw bankpas. Wanneer u deze gegevens verstrekt, geeft u criminelen de mogelijkheid om geld van uw rekening(en) af te schrijven. <i> Houd beveiligingscodes altijd voor uw zelf!</i> Lees meer.”
Dit bericht werd in iedere geval geactualiseerd op 18 februari 2011, 28 maart 2011 en 30 mei 2011.
- 4.7. Tegelijkertijd met bovenstaande melding, werd het hierna vermelde pop-up bericht vanaf 10 maart 2011 getoond:
“Als u een vreemde e-mail heeft ontvangen waarin bijvoorbeeld – de Rabobank wordt genoemd – de tekst in de e-mail taalkundig niet juist is – u wordt gevraagd om direct uw account te updaten – u op een link in de e-mail kunt klikken stuur deze e-mail dan op naar: [valse-email@rabobank.nl](mailto:valse-email@rabobank.nl"). Kijk voor meer informatie het nieuwsbericht over valse email bij Nieuws op [www.rabobank.nl](www.rabobank.nl") ‘Fraude via telefoon en e-mail’.”
Dit bericht is ververs op 17 maart 2011 en 24 maart 2011 en eindigde op 1 april 2011 en werd gelijktijdig met de waarschuwing van 8 februari 2011 en later genoemd. Voorts werden (en worden) klanten vanaf 2010 door Aangeslotene gewaarschuwd door berichten op haar website. Op 7 mei 2010 is de waarschuwing verscherpt en is de volgende tekst op haar website opgenomen: “(...) Afgelopen maand zijn er diverse

valse e-mails in omloop gekomen. In deze e-mails wordt u gevraagd door te klikken naar een frauduleuze website die erg op de site van de Rabobank lijkt. Op deze website wordt u gevraagd persoonlijke gegevens in te voeren. Doe dit nooit! Medewerkers van de Rabobank vragen nooit naar uw (persoonlijke) inloggegevens (pincode, I-code of S-code). Niet per e-mail, per telefoon, of op welke andere manier dan ook. Klik hier voor meer informatie over deze vorm van fraude en voorkom dat uzelf slachtoffer wordt. (...)” Ook verwijst Aangeslotene naar de publiekscampagnes van de Nederlandse Vereniging voor Banken (hierna: NVB) welke in het najaar van 2007 en 2010 zijn gestart. In deze campagnes zijn klanten eveneens gewaarschuwd voor phishing.

- 4.8. Het voorgaande brengt mee dat een klant in beginsel afdoende gewaarschuwd is voor phishing; hetzij in de persoonlijke Rabo Internetbankierenomgeving, hetzij via de website van Aangeslotene, hetzij via de media. Onweersproken is dat Consument in de periode voorafgaand aan de phishing verschillende transacties heeft verricht via zijn persoonlijke Internetbankierenomgeving. Daarbij heeft hij – als blijkt uit de administratie van Aangeslotene – ten minste op 26 februari 2011, 4 maart 2011 en 17 april 2011 waarschuwingmeldingen moeten zien en heeft hij deze meldingen moeten wegklikken om de betalingen te kunnen verrichten.
- 4.9. Naar het oordeel van de Commissie heeft Aangeslotene voldoende aannemelijk gemaakt dat het in haar systeem onmogelijk is om betalingen te verrichten in de persoonlijke Internetbankierenomgeving zonder daarbij gewaarschuwd te worden voor phishing. De Commissie stelt dan ook vast dat Consument indringend is voorgelicht en gewaarschuwd voor deze vorm van criminaliteit. Dat Consument de inhoud van de pop-up berichten niet tot zich heeft genomen, is een omstandigheid die voor zijn rekening en risico dient te blijven.
- 4.10. Gelet op het voorgaande treft het argument van Consument dat hij nooit van phishing heeft gehoord en ook geen pop-up scherm in zijn Internetbankierenomgeving heeft gezien, geen doel. Nu Consument ondanks de adequate waarschuwingen voor phishing en in strijd met de verstrekte veiligheidsinstructies, de beveiligingscodes aan een ander heeft afgegeven, leidt dit tot de conclusie dat hij grof nalatig in de zin van artikel 9 lid 4 van de Voorwaarden heeft gehandeld. Ten overvloede merkt de Commissie op dat dit oordeel uitsluitend betrekking heeft op de verhouding tussen Consument en Aangeslotene en de daarin geldende voorwaarden en niet inhoudt dat Consument in zijn functie van penningmeester grof nalatig heeft gehandeld ten opzichte van de vereniging.
- 4.11. Consument heeft nog betoogd dat Aangeslotene het SWIFT-bericht te laat aan de buitenlandse bank van de begunstigde rekeninghouder heeft toegezonden, waardoor hij de schade niet meer heeft kunnen beperken. Naar het oordeel van de Commissie kon van Aangeslotene echter niet worden verlangd dat zij voortvarender handelde dan zij heeft gedaan. Het is de Commissie niet gebleken dat fraude met internationale betalingen zo regelmatig plaatsvindt dat van de Aangeslotene gevergd kan worden dat zij haar systemen en procedures zo inricht dat zij bij signalen van fraude onmiddellijk een SWIFT-bericht aan de correspondentbank kan versturen. Daarbij neemt de Commissie in aanmerking dat Aangeslotene er in beginsel op mag vertrouwen dat fraude is uitgesloten als Consumenten de veiligheidsvoorschriften naleven. Ten overvloede tekent de Commissie aan dat niet is komen vast te staan dat het geld

teruggehaald had kunnen worden wanneer Aangeslotene het SWIFT-bericht direct zou hebben had verzonden, mede doordat Aangeslotene hierbij afhankelijk is van de medewerking van de correspondentbank. Aangeslotene was ook niet gehouden de naam van de begunstigde bank aan Consument bekend te maken, maar mocht verlangen dat de daartoe geëigende procedures werden gevolgd.

- 4.12. Wat betreft het beroep van Consument op de mededeling van de NVB dat de banken instaan voor vergoeding van de door hun cliënten geleden schade als gevolg van computercriminaliteit, overweegt de Commissie 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. Een en ander is in overeenstemming met de wettelijke regeling. Nu Consument in deze zaak grof nalatig heeft gehandeld in strijd met de voorwaarden, kan in het midden blijven of Consument aan de uitlatingen van de NVB rechten tegenover Aangeslotene kan ontleen.
- 4.13. Gelet op het hiervoor overwogene dient de vordering van Consument te worden afgewezen.

5. Beslissing

De Commissie wijst de vordering bij bindend advies 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.