Uitspraak Geschillencommissie Financiële Dienstverlening nr. 2020-629
(mr. E.L.A. van Emden, voorzitter en mr. M.A. Kleijer, secretaris)

Klacht ontvangen op	: 2 mei 2019
Ingediend door	: de heer [Consument 1] (de man) en mevrouw [Consument 2] (de vrouw), wonende te [plaatsnaam], samen te noemen Consumenten
Tegen	: ING Bank N.V., gevestigd te Amsterdam, verder te noemen de Bank
Datum uitspraak	: 29 juli 2020
Aard uitspraak	: Niet-bindend advies

Samenvatting

Microsoft-fraude. Consumenten zijn slachtoffer geworden van de Microsoft-fraude. Consumenten zijn benaderd door iemand die zich voordeed als Microsoft-medewerker. Op verzoek van deze 'Microsoft-medewerker' heeft de vrouw een aantal handelingen uitgevoerd waardoor de Microsoft-medewerker toegang heeft gekregen tot de computer van de vrouw. Ter authenticatie van een aantal betalingstransacties heeft de vrouw haar gebruikersnaam, wachtwoord en beveiligingscodes gebruikt en diverse bedragen overgemaakt. Naar het oordeel van de Commissie heeft de vrouw zich niet gehouden aan de veiligheidsvoorschriften van de Bank. Daardoor heeft de fraude kunnen plaatsvinden. Daarmee heeft zij grof nalatig in de zin van artikel 7:529 lid 2 (oud) BW gehandeld en zijn Consumenten zelf aansprakelijk voor de betalingstransacties. Er zijn naar het oordeel van de Commissie geen omstandigheden aanwezig die deze aansprakelijkheid van Consumenten zouden kunnen beperken. De vordering van Consumenten wordt afgewezen.

1. Procesverloop

De Commissie beslist met inachtneming van haar Reglement Geschillencommissie Financiële Dienstverlening (Kifid) Bemiddeling en bindend advies (verder: Reglement) en op basis van de volgende stukken en de daarbij behorende bijlagen:

- het door Consumenten ingediende klachtformulier en de aanvullingen daarop;
- het verweerschrift van de Bank;
- de repliek en de aanvulling daarop;
- de dupliek;
- de pleitaantekeningen van Consumenten;
- de e-mail van de Bank van 20 mei 2020 over de procedure van de limietverhoging in 2017.

Commissie stelt vast dat Consumenten hebben gekozen voor een niet-bindend advies. De uitspraak is daardoor niet-bindend. Partijen zijn opgeroepen voor een video-hoorzitting op 7 mei 2020 en hebben hieraan deelgenomen.

Wat de door Consumenten na de video-hoorzitting ingestuurde pleitnotities betreft wordt het volgende opgemerkt. Aan die notities is een *'extra noot naar aanleiding van de hoorzitting'* toegevoegd; een handelwijze die in strijd is met de goede procesorde: de Bank heeft hiervan immers geen kennis kunnen nemen en ook niet op kunnen reageren. Bovendien is hiervoor geen toestemming aan de Commissie gevraagd laat staan verkregen. Op het hiervoor genoemde onderdeel van de pleitnotities wordt geen acht geslagen.

Wat de door de Bank desgevraagd verstrekte informatie over de procedure van de limiet-vergoeding (e-mail van 20 mei 2020) betreft, wordt opgemerkt dat de Bank met hetgeen achter de vier liggende gedachtestreepjes is vermeld buiten de door de Commissie geboden gelegenheid te reageren is getreden. Een handelwijze die in strijd met de goede procesorde wordt geacht. Op de informatie die door dit handelen extra is vermeld wordt geen acht geslagen.

2. Feiten

De Commissie gaat uit van de volgende feiten.

2.1 Consumenten houden (en/of) betaal- en spaarrekeningen bij de Bank aan. Consumenten maken tevens gebruik van internetbankieren.

2.2 Op 13 december 2017 zijn Consumenten slachtoffer geworden van zogenoemde Microsoftfraude. Consumenten hebben op 21 december 2017 de Bank over het met de zogenaamde medewerkers van Microsoft gevoerde telefoongesprek, voor zover relevant, geschreven "*(…) Op woensdag 13 december 2017 werd mijn vrouw telefonisch benaderd door mensen die zich uitgaven als medewerkers van Microsoft. Op ondoorgrondelijke wijze hebben zij haar bewogen haar computer te openen om een volledige "crash" te voorkomen. Daarbij hebben ze op listige wijze de controle over haar computer over genomen en haar bewogen een aantal kleine betalingen te verrichten op uw betaalsite dan wel een copie daarvan. Middels deze truck hebben ze drie tot vier tancodes weten te ontvreemden voor een geheel ander set transacties. (…) Doordat de zogenaamde medewerkers van Microsoft aan gaven dat de behandeling van de computer wel even zou duren, en de computer in de tussentijd onbruikbaar was, begon mijn vrouw pas na langere tijd tot het besef te komen dat er iets niet pluis was.(…)".*

2.3 De hiervoor bedoelde betalingsopdrachten zijn op die dag ingevoerd tussen 11:08 en 12:16 uur en bevestigd door middel van TAN-codes.

2.4 De overschrijvingslimiet van de betaalrekening(en) is (zijn) tijdens het hiervoor onder 2.3 genoemde tijdvak verhoogd. Deze verhoging is via een TAN-code bevestigd.

2.5 In totaliteit is toen door middel van 6 overboekingen € 29.658,- naar 2 Engelse rekeningen overgeboekt.

2.6 Rond 16.30 uur die dag zijn de rekeningen van Consumenten na telefonisch contact tussen de vrouw en de Bank geblokkeerd.

2.7 Diezelfde dag rond 17.00 uur heeft de vrouw de alarmlijn van de Bank gebeld en melding gedaan van de diefstal. De Bank adviseerde haar aangifte bij de politie te doen en vertelde direct contact met de Engelse bank op te zullen nemen met als doel de gelden veilig te stellen. Dit laatste is niet gelukt.

2.8 Nadat de vrouw op 14 december 2017 bij de politie aangifte heeft gedaan, laat de politie enige tijd later weten dat het dossier wordt afgelegd.

2.9 Op 31 oktober 2018 is door de politie in samenwerking met Microsoft een nieuw proces-verbaal van aangifte opgemaakt; het resultaat daarvan is onbekend.

2.10 In de Algemene Bankvoorwaarden 2017 (ABV) in artikel 2 (Zorgplicht) is het volgende bepaald:
2."***Wij hebben een zorgplicht. U bent ook zorgvuldig tegenover ons en u mag van onze dienstverlening geen misbruik maken.***

1.Wij zijn bij onze dienstverlening zorgvuldig en houden hierbij zo goed mogelijk rekening met uw belangen. Dit doen wij op een manier die aansluit bij de aard van de dienstverlening. Deze regel geldt altijd. Andere regels in de ABV of in de voor producten en diensten geldende overeenkomsten en de daarbij behorende voorwaarden kunnen dit niet veranderen. (…).

2.11 In de Voorwaarden Betaalrekening is in artikel 16 (*Een betaalinstrument gebruiken*) bepaald: "*16.1Bij een betaalinstrument horen vaak gepersonaliseerde veiligheidskenmerken. Bijvoorbeeld een inlognaam, een wachtwoord, een pincode. Deze mogen alleen door u persoonlijk worden gebruikt. Houd deze geheim en neem alle denkbare maatregelen om fraude en misbruik te voorkomen. 16.2 ING geeft u via ing.nl en de productvoorwaarden instructies over hoe u veilig om moet gaan met gepersonaliseerde veiligheidskenmerken en betaalinstrumenten. Deze instructies moet u opvolgen.*

16.3 ING geeft u actuele informatie over maatregelen die u moet nemen om fraude en ander misbruik te voorkomen. Hiervan moet u maandelijks kennisnemen en u moet ernaar handelen."

2.12 In artikel 1 van de Uniforme Veiligheidsregels is voor zover relevant bepaald:
"1. ***Houd uw beveiligingscodes geheim***
Beveiligingscodes
wachtwoord *Mijn ING*
TAN – en PAC-codes *Mijn ING*
activeringscode *Mijn ING (…)*

- *Uw beveiligingscodes zijn persoonlijk: u laat ze nooit aan anderen zien en u vertelt anderen nooit wat uw codes zijn;(…)*
- *Als iemand u om een code vraagt, bijvoorbeeld telefonisch, op een website of in een app anders dan die via ING, via e-mail, sms, whatsapp, of persoonlijk, geef die nooit af".(…)*

2.13 In artikel 3 van de Uniforme Veiligheidsregels is, voor zover van belang, bepaald:
"***3. Zorg voor een goede beveiliging van de apparatuur die u gebruikt voor uw bankzaken***(…)
Zorg ervoor dat niemand anders uw Mijn ING of app de app kan gebruiken. Log altijd uit als u klaar bent met uw bankzaken".

2.14 Op de website van de Bank (De ING> Veilig bankieren> Belangrijke mededelingen> Toename fraude via de telefoon) is vermeld:
"***Toename fraude via de telefoon***

Voorkom dat u slachtoffer wordt

Steeds vaker wordt melding gemaakt van fraudetrucs via de telefoon. Bijvoorbeeld met betrekking tot 'Microsoft Windows'. We vertellen u graag hoe u zich ertegen kunt beschermen.

Fraudetruc via de telefoon
Een fraudeur doet zich voor als een medewerker van Microsoft en belt u met het bericht dat uw Windows computer in gevaar is. Deze zogenaamde medewerker vraagt u om naar een onbekende website te gaan om antivirussoftware op uw computer te installeren. Hij kan u ook vragen om toestemming te geven om uw computer op afstand door hem te laten overnemen. Voor de hulp die u ontvangt, betaalt u een klein bedrag via internetbankieren.

In werkelijkheid manipuleert de fraudeur uw overschrijving en maakt u, zonder dat u zich daar bewust van bent, veel geld over naar de fraudeur.

Dit doen wij
Het is onze kerntaak om uw geld veilig te bewaren. Wij doen er dan ook alles aan om internetcriminelen een stap voor te blijven en internetbankieren zo veilig mogelijk te houden.

Zo gebruikt ons team van veiligheidsexperts de laatste technieken om verdachte transacties en handelingen op te sporen en continue te analyseren, ook met betrekking tot deze vorm van fraude.

Dit kunt u doen

- ***Bescherm uw codes***

Geef codes zoals uw (mobiele) pincode, gebruikersnaam, wachtwoord, activeringscode, TAN- of PAC-codes voor Mijn ING nooit af. Onthoud dat medewerkers van de ING, u nooit per e-mail, sms of telefoon naar deze persoonlijke gegevens vragen.

- ***Hang direct op als u het telefoontje niet vertrouwt***

- ***Kijk uw overboekingen altijd goed na en lees uw SMS TAN-bericht zorgvuldig***

Controleer of het bedrag in het bericht overeenkomt met het totaalbedrag van uw overboekingen op de verzendlijst."(…)

2.15 In de Voorwaarden Betaalrekening is in artikel 11 (Een opdracht intrekken), voor zover van belang, bepaald:

11.1(…) Een opdracht die u via Mijn ING verzendt, is na autorisatie met de TAN-code onherroepelijk. (…)

3. Vordering, klacht en verweer

Vordering Consumenten

3.1 Consumenten vorderen betaling van € 29.658,- alsmede van € 500,- wegens schade aan de computer, te vermeerderen met de wettelijke rente daarover vanaf 13 december 2017.

Grondslagen en argumenten daarvoor

3.2 Op onterechte gronden weigert de Bank de door Consumenten geleden schade te vergoeden. Consumenten voeren hiertoe, kort en zakelijk samengevat, het volgende aan.

- De zes transacties van min of meer gelijke grootte zijn binnen een kort tijdsbestek zonder autorisatie naar twee voor Consumenten onbekende rekeninghouders in Engeland uitgevoerd.
- De hieruit voortgevloeide schade is te wijten aan een door criminelen gemakkelijk en snel te wijzigen daglimiet van de rekeningen.
- De Bank handelt in strijd met haar zorgplicht dan wel grof nalatig dan wel onrechtmatig door hiertegen geen technische maatregelen te nemen.

Naast het feit dat het gebruik van papieren TAN-codes fraudegevoelig is, is niet in te zien waarom voor de authenticatie van een overboeking en de procedure voor de wijziging van de daglimiet, een zelfde procedure wordt gehanteerd; voor beide handelingen wordt namelijk gebruik gemaakt van TAN-codes. Consumenten wijzen nog op een uitspraak van de Commissie (2017-476) waarin, voor zover van belang, bank XXX de aanbeveling wordt gedaan voor de wijzigingsprocedure van de daglimiet van internetoverboekingen maatregelen te nemen.

- De Bank heeft niet het nodige en mogelijke gedaan om de schade te herstellen; de Bank heeft niet de zogenoemde 'SCT recall', waarmee de overboekingen konden worden gestopt en/of worden teruggedraaid, uitgevoerd; als dit wel is gedaan dan dient de Bank daarvan bewijs te leveren; op onterechte gronden gaat de Bank ervan uit dat de met de TAN-codes bevestigde betalingsopdrachten onherroepelijk zijn. Dat de Bank weigert informatie over de rekeninghouders in Engeland te geven bestempelen Consument als grof nalatig.
- Consumenten hebben de in de contractuele relatie van partijen vastgelegde veiligheidsregels opgevolgd en hebben de criminelen geen toegang tot de computer verschaft. Dit heeft als gevolg dat de Bank overeenkomstig hetgeen contractueel is bepaald Consumenten schadeloos (exclusief het eigen risico van € 50,-) dient te stellen.
- Consumenten waren destijds niet bekend met deze vorm van fraude. De Bank heeft hierover geen dan wel onvoldoende dan wel geen adequate voorlichting verstrekt en/of voor gewaarschuwd, dit terwijl zij van die oplichtingstruc wél op de hoogte was. Ook de publieke aandacht voor deze vorm van fraude schoot tekort omdat daarin niet duidelijk werd gemaakt hoe de fraude in zijn werk ging en dat het een inbreuk op de betaalrekening betrof. Dat de voorlichting niet effectief was blijkt uit de toename van deze fraude in de periode 2014-2018.
- De Bank is haar wettelijke verplichting zoals neergelegd in artikel 16 Wwft niet dan wel niet naar behoren nagekomen; de transacties hadden als mogelijke witwastransactie gedetecteerd dienen te worden waarmee de schade te voorkomen was geweest.
- Consumenten voelen zich niet als klant maar als potentiële schadepost behandeld.
- Het coulance beleid van de Bank is te omschrijven als 'penny wise' maar 'pound foolish'. Consumenten stellen dat hen is gebleken dat de Bank kleine schadegevallen compenseert maar bij omvangrijke schades zich uiterst terughoudend opstelt en vanuit een juridisch kader opereert.
- De computer is naar aanleiding van het incident beschadigd geraakt; de geschatte schade is op € 500,- gesteld.

Verweer Bank

3.3 De Bank heeft de stellingen van Consumenten gemotiveerd weersproken. Voor zover nodig zal de Commissie bij de beoordeling daarop ingaan.

4. Beoordeling

4.1 De Commissie stelt vast dat Consumenten in de afgelopen jaren veel tijd in het bepleiten van hun standpunt tegenover de Bank hebben gestoken. Daarbij hebben ze stellingen betrokken die ver verwijderd liggen van de kern van de klacht. In de kern dient beoordeeld te worden of de Bank bij het weigeren de schade te vergoeden een juiste maatstaf heeft gehanteerd. De Commissie zal in het hierna volgende niet ingaan op die argumenten die de kern van de klacht niet raken.

4.2 De door Consumenten opgeworpen vraag of de vanwege oplichting geleden schade voor rekening van de Bank dient te komen, beantwoordt de Commissie ontkennend. Dit oordeel wordt hieronder toegelicht.

4.3 In het Burgerlijk Wetboek (BW) is in artikel 7:522 en volgende een regeling over betaaldiensten opgenomen. De feiten in deze casus spelen zich af vóór de wijziging van de nummering van deze bepalingen in februari 2019. In de volgende overwegingen wordt verwezen naar de tijdens de overboekingen geldende wettekst.

4.4 De in dit geval toe te passen maatstaf is de volgende. In artikel 7:529 lid 2 (oud) BW is bepaald dat de betalers - in dit geval dus Consumenten - alle verliezen die voortvloeien uit niet-toegestane betalingstransacties dienen te dragen voor zover zij frauduleus hebben gehandeld of opzettelijk of met grove nalatigheid een of meer verplichtingen uit hoofde van artikel 7:524 (oud) BW, niet zijn nagekomen. Zo is in artikel 7:524 (oud) BW onder meer bepaald dat de betaler zich moet houden aan de veiligheidsregels, zoals de Uniforme Veiligheidsregels, die de Bank stelt. De Commissie overweegt als volgt.

4.5 Met de Bank is de Commissie van oordeel dat is komen vast te staan dat Consumenten (dan wel de vrouw) na de Microsoftmedewerker(s) toegang tot hun computer te hebben verschaft, op de eigen digitale bankomgeving hebben ingelogd en de transacties hebben verricht. Transacties die door middel van de TAN-codes zijn geautoriseerd en daarmee definitief werden, zie hiervoor hetgeen onder 2.15 is vermeld. Dit is een handelwijze waarmee Consumenten de contractuele voorwaarden waaronder de veiligheidsinstructies van de Bank niet in acht hebben genomen hetgeen, in juridische zin, als grove nalatigheid moet worden gekwalificeerd. Gelet hierop en op hetgeen hiervoor onder 4.4 is overwogen, is de schadevordering door de Bank op terechte gronden afgewezen.

4.6 De hiervoor beschreven handelwijze van Consumenten wordt gedragen door datgene wat door hen over de oplichting is geschreven.

Zo is door Consumenten in hun hiervoor onder 2.2 geciteerde deel van de brief geschreven dat oplichters de vrouw hebben bewogen haar computer te openen, de controle daarvan hebben overgenomen en haar hebben bewogen op de (fake) site van de Bank enkele betalingen te doen.

4.7 Verder is door Consumenten over de oplichting in bijlage 5 van hun brief van 8 maart 2019 (*Toetsing van ons internetbankier gedrag aan* de *veiligheidsregels*), voor zover relevant, geschreven:
"(…) Geconstateerd kan worden dat de criminelen vermoedelijk hebben meegekeken toen mijn vrouw betaalgegevens invulde op haar beeldscherm, doordat ze een programma geïnstalleerd waarmee ze konden meekijken. (…)"

4.8 Voorts is door Consumenten over de oplichting in de hiervoor genoemde bijlage, onderdeel '**5 B's van veilig bankieren',** onder het kopje '**Laat niemand meekijken',** voor zover van belang geschreven:
"(…)Mijn vrouw heeft niemand laten meekijken er was niemand in de kamer. Kennelijk hebben de scammers wel stiekem meegekeken via naar wat we later hoorden een web viewer was. Dat is wat anders dan dat mijn vrouw ze heeft laten meekijken".

4.9 En ook omdat door Consumenten over de uitvoering van de transacties in de tijd dat de Microsoft medewerkers toegang tot de computer was verleend onder het kopje '**Voer uw codes alleen in op ING.nl'** in het zelfde onderdeel van de meer genoemde bijlage 5, voor zover van belang, hebben geschreven:
"(…)De codes zijn door mijn vrouw op de ING site op haar computer ingevoerd.(…)".

4.10 Hier bovenop komt hetgeen door Consumenten in hun repliek over de aanleiding van de oplichting, voor zover relevant, is geschreven: "(…) *Maar net zoals vele slachtoffers voor en na haar, werd zij door de scammers overvallen op een moment waarop zij haar computer niet kon missen. Toen zij de vele foutmeldingen in haar computer zag waarop de "medewerkers van Microsoft" haar telefonisch wezen kon de scam zich verder ontplooien. (…) Wel had ze eerder gezien dat Microsoft op magische wijze op afstand alerlei updates van haar computer kon plegen. Ze was daardoor ook niet argwanend toen Microsoft belde dat zij een crash van haar computer aan zagen komen en herstel wilde plegen. Uiteraard had ze beter kunnen ophangen of de sessie kunnen afbreken zeker toen er betalingen werden gevraagd. (…) Helaas heeft mijn vrouw niet opgehangen en ook de sessie niet afgebroken en helaas heeft ze een 4-tal betalingen van 3 Euro verricht aan oplichters voor niet geleverde service. Achteraf is uiteraard duidelijk dat ze voor dat bedrag opgelicht was. (…)"*

4.11 Aanleiding om de aansprakelijkheid van Consumenten in te perken, zoals neergelegd in artikel 7: 529 lid 3 (oud) BW, is er naar het oordeel van de Commissie niet hetgeen hierna wordt toegelicht.

4.12 De Commissie gaat voorbij aan al datgene dat Consumenten over de voorlichting door de Bank in relatie tot (de omvang van) deze fraude hebben aangevoerd. Ten eerste omdat uit de door de Bank overgelegde uitdraai van haar website (zie het citaat hiervoor onder 2.14) de modus operandi van de zogenaamde Microsoftmedewerkers in heldere en voor één uitleg vatbare bewoordingen is uitgelegd; een modus operandi waarvan ook in dit geval sprake was. Immers: de fraudeurs deden zich voor als medewerkers van Microsoft, belden op met de mededeling dat de computer van de vrouw in gevaar was. De fraudeurs hebben de vrouw bewogen om de computer op te starten en op afstand over te laten nemen voor welke hulp enkele kleine bedragen via internetbankieren zijn betaald. Betalingen die door de fraudeurs zijn gemanipuleerd.

4.13 De Commissie volgt de Bank in haar standpunt dat deze vorm van fraude als algemeen bekend mag worden verondersteld en Consumenten daarop in alle redelijkheid bedacht hadden kunnen en moeten zijn. Door de Bank is onbetwist gemotiveerd aangevoerd dat aan deze vorm van fraude sinds 2012 vanuit diverse media en consumentenprogramma's en sinds 2013 vanuit de NVB gestarte campagne "Hang op, klik weg, bel uw Bank", aandacht wordt gegeven. Al hetgeen door Consumenten over (de effectiviteit van) de voorlichting is gesteld, maakt dit niet anders.

4.14 De Commissie gaat voorbij aan al datgene dat Consumenten over de techniek van het internetbankieren waaronder de wijzigingsprocedure van de daglimiet, de (papieren) TAN-codes en de in dit verband van de Bank te verwachten maatregelen is aangevoerd. Hier gaat het namelijk niet om. In de kern gaat het er om dat betaaldienstgebruikers, zoals Consumenten, zich houden aan de ter zake overeengekomen veiligheidsvoorschriften. En als zij dit niet doen, de gevolgen daarvan voor hun rekening en risico blijven en niet de Bank kunnen worden aangerekend.

4.15 De Commissie gaat voorbij aan het verwijt van Consumenten dat de Bank zich niet dan wel onvoldoende zou hebben ingespannen om de schade te herstellen. Als hiervoor onder 4.5 is overwogen waren de opgegeven transacties onherroepelijk. Los daarvan is door de Bank de zogenoemde SCT-recall procedure uitgevoerd. Maar omdat de transacties onherroepelijk waren en omdat uit de informatie van de buitenlandse bank bleek dat de gelden niet meer op de rekening stonden, konden de gelden niet meer worden teruggehaald. Gelet hierop en het feit dat de Bank Consumenten naar de politie en/of justitie heeft verwezen, heeft zij aan haar inspanningsverplichting voldaan. Al het overige dat door Consumenten is aangedragen, leidt niet tot een ander oordeel.

4.16 De Commissie passeert het verwijt van Consumenten dat de transacties ten onrechte niet als witwastransacties zijn aangemerkt, waardoor de schade te voorkomen zou zijn geweest. De Commissie volgt de Bank in haar stelling dat zij niet tot ingrijpen in het betalingsverkeer kan worden verplicht zolang het betalingsverkeer van de desbetreffende klant niet leidt tot het vermoeden van witwaspraktijken of terrorisme. Daarbij heeft te gelden dat detectie geen garantie biedt dat alle frauduleuze transacties worden gedetecteerd dan wel dat de fraude wordt voorkomen. De vergelijking met de door Consumenten aangehaalde uitspraak van de Commissie geregistreerd onder nummer 2019-619, gaat niet op. In die aangehaalde kwestie ging het om 119 transacties in korte tijd, terwijl het in deze kwestie om 6 transacties gaat. Al het overige dat door Consumenten in dit verband is aangedragen, laat hetgeen hiervoor is overwogen onverlet.

4.17 Ook hetgeen door Consumenten over het coulance beleid van de Bank is aangedragen en over de door hen ervaren bejegening leidt niet tot een beperking van de aansprakelijkheid van Consumenten. Wat er ook zij van het coulance beleid van de Bank: coulance is juridisch niet afdwingbaar. En wat de ervaren bejegening betreft stelt de Commissie vast dat Consumenten geruime tijd en met regelmaat al dan niet voorzien van bijstand met de Bank over deze kwestie hebben gecorrespondeerd. Dat Consumenten zich niet in het beleid van de Bank kunnen vinden, leidt niet tot een ander oordeel.

4.18 Uit al hetgeen hiervoor is overwogen volgt logischerwijs dat de gevorderde schade aan de computer niet wordt toegewezen.

4.19 Alhoewel de Commissie goed begrijpt hoe zeer Consumenten gedupeerd zijn door behendige oplichters die hen een belangrijk geldbedrag afhandig hebben gemaakt, kan echter deze schade op juridische gronden niet op de Bank verhaald worden. De conclusie dient derhalve te luiden dat de Bank in haar dienstverlening niet toerekenbaar tekort is geschoten of onrechtmatig heeft gehandeld. De klacht wordt in al haar onderdelen ongegrond geacht en de daarop gebaseerde vordering dient te worden afgewezen.

5. Beslissing

De Commissie wijst de vordering af.

De uitspraak heeft de vorm van een niet-bindend advies. 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.

U kunt, binnen twee weken na de verzenddatum van deze uitspraak, bij de Voorzitter van de Geschillencommissie Financiële Dienstverlening schriftelijk een verzoek indienen tot herstel van kennelijke vergissingen in de uitspraak. U moet daarbij met name denken aan correctie van reken- of schrijffouten en verbetering van namen en data. De volledige procedure met de termijnen die daarbij in acht moeten worden genomen staat beschreven in artikel 40 van het Reglement.