Uitspraak Geschillencommissie Financiële Dienstverlening nr. 2019-619
(mr. R.J. Paris, voorzitter, mr. W.F.C Baars, mr. dr. M.D.H. Nelemans, leden en mr. M.A. Kleijer, secretaris)

Klacht ontvangen op	: 20 april 2018
Ingediend door	: Consumenten en ieder afzonderlijk te noemen de man of de vrouw
Tegen	: ING Bank N.V., gevestigd te Amsterdam, verder te noemen Bank
Datum uitspraak	: 29 augustus 2019
Aard uitspraak	: Bindend advies

Samenvatting

Consumenten zijn slachtoffer geworden van Microsoftfraude. Alhoewel Consumenten in strijd met de voorwaarden en instructies van de Bank hebben gehandeld en uit dien hoofde aansprakelijk zijn voor de daardoor geleden schade, is de Commissie van oordeel dat gegeven de specifieke feiten en omstandigheden van dit geval die aansprakelijkheid op de voet van artikel 529 lid 3 van boek 7 (oud) BW dient te worden beperkt. De vordering wordt gedeeltelijk toegewezen.

1. Procesverloop

De Commissie beslist met inachtneming van haar Reglement en op basis van de volgende stukken en de daarbij behorende bijlagen:

- het door Consumenten ingediende klachtformulier;
- het verweerschrift van de Bank;
- de repliek van Consumenten;
- de dupliek van de Bank;
- de door de gemachtigde van Consumenten ter zitting overgelegde pleitaantekeningen.

De Commissie stelt vast dat partijen hebben gekozen voor bindend advies.

Partijen zijn opgeroepen voor een hoorzitting op 9 mei 2019 en zijn aldaar verschenen.

2. Feiten

De Commissie gaat uit van de volgende feiten.

2.1 Consumenten houden zowel afzonderlijk als gezamenlijk bij de Bank betaal- en spaarrekeningen aan. Consumenten hebben tevens een internetbankierenovereenkomst (Mijn ING) met de Bank afgesloten.

2.2 Op 26 oktober 2017 zijn Consumenten slachtoffer geworden van zogenoemde Microsoft-fraude. Op die dag is de man namelijk gebeld door een vrouwelijk persoon die zich voordeed als medewerker van Microsoft (verder: medewerker) en die de man vertelde dat diens computer was gehackt hetgeen door haar kon worden opgelost.

2.3 De man heeft vervolgens op verzoek van de medewerker een zogenoemde "teamviewer" gedownload en de medewerker de daarbij behorende inlogcode gegeven. De medewerker heeft hierop de besturing van de computer van de man overgenomen. Vervolgens is op Mijn ING ingelogd. Om ongeveer 15:30 uur heeft de man de via zijn mobiele telefoon ontvangen codes aan de medewerker, op haar verzoek, doorgegeven. Die codes, zo is de man naderhand duidelijk geworden, waren zogenoemde TAN-codes oftewel autorisatiecodes om via het internetbankieren (Mijn ING) transacties uit te voeren. Die TAN-codes heeft de man tot ongeveer 21:45 uur aan de medewerker doorgegeven.

2.4 Gebleken is dat op 26 oktober 2017 twee keer een bedrag van € 20.000,- ten laste van de spaarrekeningen naar de betaalrekeningen is overgeboekt. Verder zijn op diezelfde dag tussen 15:30 en 22:00 uur 119 transacties van € 300,- ten laste van de betaalrekeningen geboekt. Uit de op die transacties betrekking hebbende omschrijving blijkt dat daarmee iTuneskaarten via de website van XXX zijn aangeschaft.

2.5 Daags na de fraude is nog twaalf keer een bedrag van € 300,- van een betaalrekening afgeboekt.

2.6 In totaliteit is voor een bedrag van € 35.700,- van de betaalrekeningen van Consumenten afgeschreven.

2.7 De man heeft op de dag van de fraude zijn rekeningen via de alarmlijn van de Bank laten blokkeren.

2.8 De man heeft bij de politie aangifte van cybercrime gedaan.

2.9 Op de contractuele relatie van partijen zijn van toepassing de Algemene Bankvoorwaarden, de Voorwaarden Betaalrekening, de Voorwaarden Mijn ING en de Uniforme Veiligheids-regels.

2.10 In de Algemene Bankvoorwaarden 2017 (ABV) is in artikel 2 (Zorgplicht) 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 belangrijke regel geldt altijd. Andere regels in de ABV of in de voor producten en diensten geldende overeenkomsten en de daarbij behorende bijzondere 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 van ING, via e-mail, sms, whatsapp, of persoonlijk, geef die dan 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 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 toestemming te geven om uw computer op afstand door hem over te laten nemen. 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 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 12 (*Uw opdracht weigeren*) bepaald:
12.1 ING mag een betaalopdracht weigeren als deze onvolledig, onjuist of onduidelijk is.

12.2 ING mag een betaalopdracht weigeren als wij fraude, misbruik of onregelmatigheden vermoeden. Als blijkt dat ons vermoeden niet juist is, zullen we de betaalopdracht alsnog uitvoeren.
(…)

3. Vordering, klacht en verweer

Vordering Consumenten

3.1 Consumenten vorderen betaling door de Bank van € 35.700,- te vermeerderen met de wettelijke rente daarover sinds 26 oktober 2017.

Grondslagen en argumenten daarvoor

3.2 Deze vordering steunt, kort en zakelijk weergegeven, op de volgende grondslag. De Bank is uit hoofde van haar dienstverlening toerekenbaar tekortgeschoten met schadeplichtigheid als gevolg. Consumenten zijn slachtoffer geworden van cybercrime en hebben daardoor schade geleden. De afwijzing door de Bank van vergoeding van deze schade is onterecht omdat zij haar zorgplicht jegens Consumenten heeft geschonden.

3.3 De totale schade is het gevolg van een zeer groot aantal uitgevoerde transacties in relatief korte tijd namelijk tussen ongeveer 15:30 en 22:00 uur op 26 oktober 2017. De aard (aanschaf iTunes kaarten), omvang (elk € 300,- groot) en frequentie (119 keer) van deze transacties hadden op zichzelf al tot ingrijpen door de Bank moeten leiden.

3.4 Uit de uitspraken van Kifid volgt dat geen algemene signaleringsplicht van banken wordt aangenomen, zie hiervoor GC 31-10-2016, nr. 2017-796, GC17-11-2016, nr. 2016-563, GC 20-01-2017, nr. 2017-476, GC 31-01-2017, nr. 2017-522 en GC 5-7-2017, nr. 2017-440. Tegelijkertijd is uit deze uitspraken op te maken dat op grond van de specifieke feiten en omstandigheden van het geval aanleiding tot direct ingrijpen door de financieel dienstverlener kan ontstaan. Consumenten zijn van mening dat hiervan sprake is. Om te beginnen wijzen zij op de hiervoor onder 3.3 genoemde feiten. Daarnaast dienen de hieraan voorafgegane overboekingen van de spaarrekeningen naar de betaalrekeningen te worden betrokken. Voorts is van belang dat de transacties voor Consumenten ongebruikelijk zijn. Bovendien is na de blokkering van de rekening de volgende dag op 27 oktober 2017 nog twaalf keer een bedrag van €300,- van een rekening afgeschreven. Consumenten achten de verklaring van de Bank hiervoor, namelijk dat die bedragen reeds waren gereserveerd en niet meer konden worden teruggeboekt, niet valide. Consumenten zijn van mening dat de wijze waarop de Bank de betalingstransacties heeft gecontroleerd onder de maat is en hebben ter ondersteuning daarvan overgelegd het door het Openbaar Ministerie opgestelde rapport “Houston”.

Uit dit rapport volgt dat het Openbaar Ministerie van oordeel was dat de Bank zich in de onderzoeksperiode schuldig heeft gemaakt aan overtreding van een aantal bepalingen uit de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) en het Wetboek van Strafrecht. Consumenten zijn tot slot van mening dat hun geen grove nalatigheid kan worden verweten omdat zij nooit het oogmerk hebben gehad een derde toegang tot hun digitale bankomgeving te bieden en zij ook niet bewust hebben gekozen de daaruit voortvloeiende risico's te aanvaarden.

Verweer Bank

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

4. Beoordeling

4.1 Gelet op de vordering van Consumenten tot vergoeding van de vanwege de cybercrime geleden schade, dient de Commissie te beoordelen of die schade voor rekening van de Bank dient te komen.

4.2 In het Burgerlijk Wetboek (verder: BW) is een regeling over betaaldiensten opgenomen, zie hiervoor artikel 522 en volgende in boek 7. De nummering van deze bepalingen is in februari 2019 gewijzigd. Hierna zal worden verwezen naar de ten tijde van de overboekingen geldende wettekst.

4.3 In artikel 529 lid 2 van boek 7 (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 524 van boek 7 (oud) BW niet zijn nagekomen. Zo is in artikel 524 van boek 7 (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.

4.4 De stelling van de Bank dat Consumenten de medewerker kennelijk toegang tot hun digitale bankomgeving hebben verschaft, is niet dan wel onvoldoende betwist en staat derhalve vast. Hiernaast staat vast dat Consumenten voor het uitvoeren van de overboekingen de medewerker van de daarvoor benodigde TAN-codes hebben voorzien. Gelet op het vorenstaande staat dan ook vast dat Consumenten niet aan de veiligheidsvoorschriften van de Bank hebben voldaan en daarmee aansprakelijk zijn voor de door hen geleden schade omdat hun handelwijze, zoals in de wet is bepaald, als '*grof nalatig*' is te kwalificeren.

4.5 De Commissie ziet zich echter gesteld voor de vraag of de aansprakelijkheid van Consumenten op grond van artikel 529 lid 3 van boek 7 (oud) BW, dient te worden beperkt. Consumenten hebben hiertoe aangevoerd dat er voor de Bank, gegeven de bijzondere omstandigheden van dit geval zoals hiervoor onder 3.3 en 3.4 is vermeld, aanleiding bestond om in te grijpen. De Bank heeft zich hiertegen verweerd met de stelling dat contractueel is overeengekomen dat de gegeven betaalopdrachten vanwege de accordering door de TAN-codes definitief waren. Verder is door de Bank aangevoerd dat op haar geen wettelijke verplichting tot controle en/of detectie van de transacties rust. Voorts is door de Bank aangevoerd dat deze vorm van fraude inmiddels als algemeen bekend mag worden verondersteld omdat hiervoor reeds vele jaren via de media en ook door haar via de website wordt gewaarschuwd. De Commissie overweegt als volgt.

4.6 Gelet op de specifieke feiten en omstandigheden in de onderhavige klachtkwestie zoals het grote aantal transacties, alle van gelijke grootte, alle bestemd voor de aankoop van hetzelfde product, het tijdsbestek waarbinnen de transacties zijn opgegeven, het feit dat de Bank met deze vorm van fraude (zie hiervoor onder 2.14) bekend was in relatie tot haar contractuele bevoegdheid om opdrachten te weigeren (zie hiervoor onder 2.15) oordeelt de Commissie dat op de voet van artikel 529 lid 3 van boek 7 (oud) BW, de aansprakelijkheid van Consumenten dient te worden beperkt en stelt dit ex aequo et bono op 40% vast met als gevolg dat € 21.420,- (35.700 x 60%) voor vergoeding door de Bank in aanmerking komt.

4.7 De Commissie volgt, tot slot, Consumenten niet in hun stelling dat daags na de blokkering van de rekeningen ten onrechte door de Bank nog een aantal transacties is uitgevoerd. De Bank heeft toegelicht dat in Mijn ING weliswaar de term reservering stond vermeld, maar dit verband hield met een administratief nog niet afgeronde boeking. Met de Bank is de Commissie van oordeel dat de gegeven betaalopdrachten reeds definitief en daarmee onherroepelijk waren.

5. Beslissing

De Commissie beslist dat de Bank binnen zes weken na de dag waarop een afschrift van deze beslissing aan partijen is verstuurd, aan Consumenten vergoedt een bedrag van € 21.420 met rente gelijk aan de wettelijke rente vanaf 26 oktober 2017 tot aan de dag van algehele voldoening.

In artikel 2 van het Reglement van de Commissie van Beroep Financiële Dienstverlening is bepaald in welke gevallen beroep openstaat van bindende 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 www.kifid.nl/in-beroep-gaan-bij-kifid.

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.