

**Uitspraak Geschillencommissie Financiële Dienstverlening nr. 2019-403
(mr. R.J. Paris, voorzitter en mr. J. Hadziosmanovic, secretaris)**

Klacht ontvangen op : 12 juli 2018
Ingediend door : Consument I en Consument II, verder tezamen te noemen Consumenten
Tegen : ING Bank N.V., gevestigd te Amsterdam, verder te noemen de Bank
Datum uitspraak : 13 juni 2019
Aard uitspraak : Bindend advies

Samenvatting

Consumenten hebben de toegangscode tot de Mobiel Bankieren App van de Bank aan een onbekende derde afgegeven. Deze persoon heeft € 2.750,- van de rekening van Consumenten ontvreemd. De omstandigheden waaronder Consumenten de toegangscode hebben afgegeven, zijn omstandigheden die niet voor rekening van de Bank komen. Er zijn geen omstandigheden gebleken die de aansprakelijkheid van Consumenten beperken. De vordering wordt afgewezen.

I. Procesverloop

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

- het door Consumenten ingediende klachtformulier;
- het verweerschrift van de Bank;
- de repliek van Consumenten;
- de aanvullende stukken van Consumenten;
- de dupliek van de Bank.

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

De Commissie stelt vast dat het niet nodig is de zaak mondeling te behandelen. De zaak kan daarom op grond van de stukken worden beslist.

2. Feiten

De Commissie gaat uit van de volgende feiten.

- 2.1 Consumenten houden bij de Bank afzonderlijk van elkaar een betaalrekening aan en hebben de beschikking over een bankpas met pincode.

Zij maken gebruik van internetbankieren. Aan het internetbankieren van Consument II zijn de spaarrekeningen van hun (minderjarige) kinderen gekoppeld.

- 2.2 Consument I heeft via Marktplaats een analoge camera te koop aangeboden. Op 27 november 2017 bleek een derde geïnteresseerd in de aankoop hiervan. Via Whatsapp hebben Consument I en deze derde contact gehad over het kopen van de camera door de derde en het voldoen van het aankoopbedrag. Een afschrift van het Whatsapp-gesprek maakt onderdeel uit van het dossier.
- 2.3 De derde geeft in het Whatsapp-gesprek aan eens te zijn opgelicht en om vertrouwen te krijgen verzoekt zij Consument I om een foto van zijn bankpas en zijn legitimatiebewijs toe te sturen. Consument I heeft het verzoek opgevolgd en een foto gestuurd van zijn bankpas en legitimatiebewijs.
- 2.4 De derde geeft aan dat zij het aankoopbedrag via haar zakelijke rekening zal overboeken en dat hiervoor vereist is dat Consument I handelingen uitvoert via het internetbankieren op zijn computer.
- 2.5 Consument I heeft vervolgens ingelogd in het internetbankieren van Consument II. De derde heeft vastgesteld dat de betaling hierdoor niet kan slagen en heeft Consument I verzocht om een foto van de bankpas van Consument II en haar geboortedatum toe te sturen. Dit heeft Consument I gedaan.
- 2.6 Via het internetbankieren heeft Consument I vervolgens, met begeleiding van de derde, een Iphone [type] geactiveerd. Deze telefoon is in het bezit van de derde. Vervolgens heeft Consument I de derde de door hem ontvangen TAN-code en bevestigingscode, ten behoeve van de koppeling van de Iphone [type], verstrekt. De derde heeft hiermee de Mobiel Bankieren App (hierna: de App) geactiveerd. Via de App kon de derde beschikken over de internetbankieren omgeving van Consument II en over de daaraan gekoppelde betaalrekeningen, inclusief de rekeningen van de kinderen. De derde kon hierdoor transacties verrichten met deze rekeningen.
- 2.7 In de avond hebben Consumenten ontdekt dat zij slachtoffer zijn geworden van internet-fraude. De derde heeft € 2.750,- van de rekening van Consument II en de daaraan gekoppelde spaarrekeningen van de kinderen onttrokken.

3. Vordering, klacht en verweer

Vordering Consumenten

3.1 Consumenten vorderen dat de Bank wordt veroordeeld tot vergoeding van de door Consumenten geleden schade, te weten een bedrag van € 2.750,-, zijnde het bedrag dat op 27 november 2017 van de betaalrekeningen is ontvreemd. Subsidiair vorderen Consumenten dat de Bank wordt veroordeeld tot vergoeding van de gelden die van de rekeningen van de kinderen zijn ontvreemd ad € 2.050,-, met wettelijke rente.

Grondslagen en argumenten daarvoor

3.2 Deze vordering steunt, kort en zakelijk weergegeven, op de volgende grondslag.

Consumenten stellen dat de Bank toerekenbaar is tekortgeschoten in de nakoming van haar zorgplicht en voeren hiertoe de volgende argumenten aan:

- de Bank is tekortgeschoten het betalingssysteem voldoende te beveiligen, nu in de App met één 5-cijferige code geld kan worden overgemaakt tot aan de daglimiet;
- de stappen voor het activeren van de App op een mobiele telefoon vinden allemaal in dezelfde fase plaats, er is geen vangnet meer;
- gekoppelde (spaar-)rekeningen zijn eveneens direct toegankelijk in de App, ondanks dat zij andere rekeningnummers dragen;
- doordat de Bank de gevaren voor de gekoppelde (kinder)rekeningen niet heeft benoemd bij het afsluiten ervan, heeft de Bank haar waarschuwingplicht geschonden;
- bij phishing zou de Bank wel overgaan tot vergoeding van de schade en deze fraude kan worden gezien als een vorm van phishing. Hierom dient de Bank ook in dit geval over te gaan tot vergoeding.

Verweer van de Bank

3.3 De Bank heeft, kort en zakelijk weergegeven, de volgende verweren gevoerd:

- Consument I is door een voor hem onbekend persoon door de internetbankieren omgeving (hierna: Mijn ING) geleid waarbij hij de App voor het gebruik van internetbankieren voor de rekening van Consument II op de mobiele telefoon van die derde heeft geactiveerd. Hij kreeg vervolgens een bevestigingscode die hij aan de voor hem onbekende persoon heeft doorgegeven. Hierdoor kon deze persoon met behulp van de App via zijn eigen telefoon over het tegoed op de betaalrekening en gekoppelde spaarrekeningen beschikken en betalingsopdrachten geven. Uit de stappen die Consument heeft doorlopen, blijkt duidelijk dat het gaat om het aanvragen van de App en het toevoegen van een mobiele telefoon, te weten de Iphone [type] van meergenoemde derde;
- Consument heeft door het doorgeven van de bevestigingscode in strijd met de Algemene Bankvoorwaarden, de Voorwaarden Betaalrekening en de Uniforme Veiligheidsregels gehandeld;

- de App is voldoende beveiligd. De App moet middels een via Mijn ING ontvangen bevestigingscode worden geactiveerd. De schade is nadrukkelijk niet ontstaan doordat de beveiliging van de App met een 5-cijferige beveiligingscode niet zou voldoen. De schade is ontstaan door het niet geheimhouden van de bevestigingscode;
- Consumenten waren ervan op de hoogte welke rekeningen Consument II kon beheren in haar internetbankieren omgeving. De Bank meent dat indien Consumenten dit een te groot risico vonden, Consumenten hadden moeten afzien van het gebruik van de App;
- zowel op de website van de Bank, als in Consumentenprogramma's wordt regelmatig gewaarschuwd voor dergelijke vormen van zogenoemde Marktplaatsfraude. De Bank heeft aan haar waarschuwingsplicht voldaan;
- de Bank stelt dat er in dit geval geen sprake is van phishing. Bij phishing denkt het slachtoffer namelijk werkelijk op de site van de Bank in te loggen, echter speelt men de gegevens door aan een oplichter. De oplichter doet zich in dat geval voor als de Bank. Hierbij is sprake van andere omstandigheden. Overigens bestaat er ook bij phishing-fraude geen (wettelijke) plicht voor de Bank om tot vergoeding over te gaan. Het betreft coulance en ieder geval wordt individueel beoordeeld.

4. Beoordeling

- 4.1 Aan de Commissie ligt de vraag voor of de Bank de door Consument betwiste transactie dient te vergoeden. De Commissie oordeelt als volgt.
- 4.2 De wet (artikel 7:529 lid 1 (oud) Burgerlijk Wetboek (BW)) bepaalt dat de houder van een betaalrekening tot een bedrag van ten hoogste € 150,- de schade draagt die een gevolg is van onrechtmatig gebruik van zijn bankpas. Dit is alleen anders – zie artikel 7:529 lid 2 (oud) BW – als de pashouder frauduleus heeft gehandeld of opzettelijk dan wel met grove nalatigheid één of meer verplichtingen voor het veilig gebruik van het betreffende betaalinstrument niet is nagekomen. Als dit laatste het geval is, komt de gehele schade voor zijn rekening. Onder de hiervoor bedoelde verplichtingen wordt verstaan: handelen in de zin van de Algemene Voorwaarden waarin het gebruik van en de omgang met de bankpas en de beveiligingscodes nader zijn bepaald (artikel 7:524 (oud) BW).

Artikel 7:529 lid 3 (oud) BW biedt ten slotte ruimte om, als wordt geoordeeld dat de betaler wel grof nalatig, maar niet opzettelijk of frauduleus heeft gehandeld, de aansprakelijkheid van de betaler te beperken als de specifieke omstandigheden van het geval daartoe aanleiding geven.

- 4.3 Consumenten bestrijden niet dat Consument I onder meer in strijd met toepasselijke voorwaarden heeft gehandeld door de bevestigingscode aan de onbekende persoon te verstrekken.

Consumenten stellen zich evenwel op het standpunt dat de App onvoldoende is beveiligd. Op grond hiervan dient de schade niet voor hun eigen rekening te blijven, althans hun aansprakelijkheid onder de gegevens omstandigheden dient te worden beperkt in de zin van artikel 7:529 lid 3 (oud) BW.

- 4.4 De stelling dat aan de App tekortkomingen zouden kleven dan wel onvoldoende beschermende maatregelen zijn getroffen, is door de Bank uitdrukkelijk gemotiveerd betwist. De fraude is mogelijk gemaakt doordat Consument I persoonlijke gegevens en de bevestigingscode aan de derde heeft doorgegeven, die op deze wijze de App op haar telefoon heeft kunnen activeren en zich toegang heeft verschaft tot de rekeningen.
- 4.5 Ook het verwijt dat de Bank niet zou hebben gewaarschuwd wordt gepasseerd. Inmiddels mag als algemeen bekend worden beschouwd dat internetfraude voortvloeit uit het verlenen van toegang tot de persoonlijke beveiligde bancaire internet-omgeving aan derde(n) en ook door het verstrekken van beveiligingscodes aan derde(n). Bovendien mag als algemeen bekend worden verondersteld dat een derde ten laste van zijn betaalrekening een overboeking kan uitvoeren zonder assistentie van de ontvangende partij.
- 4.6 Tot slot hebben Consumenten zich op het standpunt gesteld dat deze vorm van fraude (Marktplaatsfraude) gezien kan worden als een vorm van phishing, welke schade doorgaans wel door de Bank wordt vergoed. De Commissie oordeelt dat in het onderhavige geval echter geen sprake is van phishing. Er is geen sprake van met phishing-fraude vergelijkbare feiten en omstandigheden waarbij de oplichter het slachtoffer leidt naar een valse website om het slachtoffer op deze manier diens inloggegevens te ontfutselen. De oplichter doet zich in het geval van phishing voor als (een medewerker van) de bank. In het onderhavige geval heeft Consument I persoonlijke gegevens en codes bewust doorgespeeld op verzoek van een derde. Van een vergelijking is dan ook geen sprake.

Bovendien heeft de Bank onweersproken gesteld dat er geen (wettelijke) plicht bestaat om ook in gevallen van phishing-fraude tot vergoeding over te gaan.

Conclusie

- 4.7 Het voorgaande brengt met zich mee dat, hoewel Consumenten slachtoffer zijn geworden van een gewiekste handelwijze van criminelen, de schade als gevolg daarvan voor hun rekening dient te blijven. De vordering van Consumenten dient te worden afgewezen. Voor de volledigheid merkt de Commissie op dat 'grof nalatig' een wettelijke term is. Tot die juridische toets heeft de Commissie zich beperkt.

5. Beslissing

De Commissie wijst de vordering af.

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.