1. Samenvatting van de klacht

Op 1 april 2022 kreeg de klager een mail die leek te komen van zijn bank en die betrekking had op de vervanging van zijn kaartlezer.

Hij klikte rond 22 uur op de link om de nieuwe kaartlezer, zonder kosten, aan te vragen. Hij kwam op een venster terecht waar hij de kaartnummer van zijn debetkaart moest invullen. Een goede 20 minuten later werd hij opgebeld door een onbekend nummer. Het was een vriendelijke en beleefde man die zich uitgaf voor medewerker van de bank in Brussel. De man sprak perfect Nederlands.

In de klacht bij Ombudsfin heeft de klager vermeld dat deze man hem zei dat er fraude was gepleegd met zijn kaart, waarna hij vroeg zijn kaartlezer aan te sluiten op zijn computer.
Er werd hem gevraagd om zijn kaartlezer te gebruiken, met zijn debetkaart en vervolgens ook met zijn kredietkaart. Hij heeft dan mondeling de instructies van de man gevolgd. Hij heeft meerdere keren hetzelfde stappenplan doorlopen.

Na 3 keer werd het gesprek beëindigd. De klager werd bedankt voor de medewerking en het goede verloop. De man zei dat alles in orde zou komen en dat er nog iemand de klager zou opbellen op zaterdag om alles te verduidelijken.

De klager had een raar gevoel en keek zijn rekeningen na. Hij zag meteen een verdachte betaling van 12.455 euro ten gunste van B. Hij heeft meteen zijn kaarten laten blokkeren.

Hij hoopt dat de bank in zijn schade zal tussenkomen.

2. Standpunt van de bank

De cliënt verklaarde een bericht te hebben ontvangen van een afzender met als e-mailadres 'no-reply@...bank.be', waarvan hij vermoedde dat dit afkomstig was van de bank. Nadat hij op de toegevoegde link had geklikt, en hierbij zijn kaartnummer doorgaf, werd hij telefonisch gecontacteerd door een persoon die zich uitgaf voor een medewerker van de bank. De cliënt verklaarde in het proces-verbaal dat hij instructies ontving om handelingen te stellen met kaart en kaartlezer en dat u meerdere keren het stappenplan doorliep.

De cliënt betwist een aankoop via het internet met zijn originele kredietkaart op datum van 1 april 2022 om 22.18 uur voor een bedrag van 12 455 euro.

De betwiste transactie is van het type 3D-Secure. Om ze te valideren, waren de volgende 3 elementen onontbeerlijk: in het fysieke bezit van de kredietkaart zijn en het nummer ervan kennen; beschikken over de geheime code, die enkel de kaarthouder kent; beschikken over de van de kaartlezer afkomstige autorisatiecode (na de kaart en de geheime code in de kaartlezer te hebben ingevoerd).

Er bestaat momenteel geen solidere of meer beveiligde manier van authenticatie.

Voorafgaand aan de validatie van de transactie met de kredietkaart verscheen op de kaartlezer van de bank het bericht '**aankoop op internet?**' waarna het betrokken 'bedrag' 12455 ingevoerd moest worden, gevolgd door **OK**.

De wet op de betaalinstrumenten (Wetboek Economisch Recht) bepaalt de rechten en plichten van de bezitter van een betaalinstrument. Artikel VII 44 zegt ter zake: “de betaler draagt geen enkel verlies indien het verlies, de diefstal of het onrechtmatig gebruik van een betaalinstrument niet door de betaler kon worden vastgesteld voordat een betaling werd uitgevoerd (…)” .

Het feit of fraude vooraf al of niet kan worden vastgesteld, wordt beoordeeld op basis van de feitelijke omstandigheden. In dit dossier zijn er aanwijzingen die uw aandacht hadden kunnen trekken:

- De cliënt ontvangt een e-mail van no-reply@...bank.be < onlinehelp3@magenta.de > met een link. Er wordt nochtans al geruime tijd via diverse kanalen gewaarschuwd voor dit soort frauduleuze berichten
- hij heeft zijn kredietkaart en de kaartlezer van de bank gebruikt zoals die ook gebruikt wordt om een betaling uit te voeren;
- op zijn kaartlezer verscheen de tekst ‘een limiet wijzigen?’ waarna hij de limietverhoging van zijn kredietkaart diende te bevestigen; op zijn Belfius-kaartlezer verscheen de tekst ‘aankoop op internet?’ waarna hij effectief het betrokken bedrag diende in te voeren en te bevestigen;
- hij diende codes door te geven aan een derde en hij ontving codes die hijzelf diende in te voeren. Per definitie zijn aangemaakte codes geheim en mogen die nooit met derden worden gedeeld.
- hij wordt telefonisch gecontacteerd waarbij reeds geruime tijd wordt gewaarschuwd voor phishing, ook via de website van de bank:

Artikel VII 44 van het Wetboek Economisch Recht zegt ook: “de betaler draagt alle verliezen in verband met niet-toegestane betalingstransacties indien de betaler ze heeft geleden doordat hij frauduleus heeft gehandeld of opzettelijk of door grove nalatigheid een of meer van de in artikel VII 38 genoemde verplichtingen niet is nagekomen.”

Artikel VII 38 luidt: “de gebruiker van betaaldiensten neemt, zodra hij een betaalinstrument ontvangt, in het bijzonder alle redelijke maatregelen om de veiligheid van het betaalinstrument en zijn gepersonaliseerde veiligheidsgegevens te vrijwaren.”

Tot slot wil de bank bevestigen dat een aankoop op het internet wel degelijk meteen uitgevoerd wordt en niet meer herroepen of tegengehouden kan worden. Het betreft immers een transactie tussen de betaler en de handelaar. Met de kredietkaart staat de bank contractueel toe dat de rekening van de betaler pas gedebiteerd wordt bij de maandelijkse uitgavenstaat. Dat de debitering uitgesteld wordt, doet geen afbreuk aan de onmiddellijke uitvoerbaarheid van de transactie t.a.v. de handelaar. De aankoop werd uitgevoerd op 1 april 2022 om 22.18 uur zodat deze nadien niet meer herroepen kon worden. Worldline bevestigt dat de kredietkaart van de cliënt werd geblokkeerd op 2 april om 9.47 uur.

De bank kan niet verantwoordelijk worden gesteld voor de betwiste transactie en ziet bijgevolg ook geen mogelijkheid om financieel tussen te komen in dit dossier.

3. Het advies van Ombudsfin

De klager is in 2 fases slachtoffer geworden van fraude (phishing en vishing). In een eerste fase, op 1 april 2022, heeft hij een mail ontvangen die zogezegd van de bank afkomstig was. De mail betrof de vervanging van zijn kaartlezer.

Hij klikte op de link in de mail en vulde enkele persoonlijke gegevens in. Wat hij niet wist, was dat hij op een valse website terechtgekomen was. Door hier zijn persoonlijke gegevens in te voeren, heeft de fraudeur die gebruikt voor de volgende fase van de fraude.

In een tweede fase, een klein halfuur na het volgen van de link in de mail en het afsluiten van dat venster, werd hij opgebeld door een voor hem onbekende persoon. Het was een man, een zogezegde medewerker van de bank, die zei dat er fraude was met uw kaart. Hij vroeg de cliënt handelingen te doen met zijn kaarten en kaartlezer.

Door het doorgeven van de kaartgegevens en de verschillende responscodes verkregen via zijn kaarten, pincode en kaartlezer (voor aanmelden in Bank Direct Net, voor de limietverhoging en de kredietkaartverrichting), is de fraudeur erin geslaagd de aankoop te doen met de kredietkaart.

In de verdere analyse ligt de focus op de 2de fase van de fraude, aangezien de frauduleuze verrichting in die fase is uitgevoerd.

De betwiste verrichting betreft een online betaling.

De online betaling werd uitgevoerd via de kredietkaart, vóór de blokkering ervan. Eenmaal betalingen geïnitieerd en goedgekeurd zijn, kunnen deze niet meer worden tegengehouden door de bank. Aangezien bij een betaling meteen goederen en/of diensten in ruil geleverd worden, konden de ontvreemde gelden ook niet meer gerecupereerd worden door de bank.
Dat de aanrekening ervan pas later gebeurde (zoals steeds bij betalingen via kredietkaart) betekent niet dat de uitvoering ervan kon worden tegengehouden.

Niet-toegestane betalingstransacties

De klager heeft uitsluitend de instructies van de fraudeur gevolgd en de responscodes doorgegeven omdat hij ervan uit ging dat dit nodig was om alles terug in orde te brengen na de fraude met zijn kaarten. Hij heeft bijgevolg nooit bewust ingestemd met de betwiste verrichting. Voor hem persoonlijk was het zeker niet duidelijk dat hij door zijn handelingen een limietverhoging (van de kredietkaart) in orde bracht en een aankoop deed.

Ombudsfin meent daarom dat het hier gaat om een niet-toegestane betalingstransactie in de zin van artikel VII.32, §2, lid 4 van het Wetboek van economisch recht (WER). Bijgevolg zijn de bepalingen uit het WER inzake de aansprakelijkheidsverdeling bij niet-toegestane betalingstransacties van toepassing.

Aansprakelijkheidsverdeling bij niet-toegestane betalingstransacties

De wetgever voorziet, bij wijze van uitzondering op de basisregel, de ruimste bescherming voor de betaler (de betaler draagt geen enkel verlies) wanneer het onrechtmatige gebruik van het betaalinstrument niet kon worden vastgesteld door de betaler voordat een betaling plaatsvond.

Men moet dan afwegen of de fraude detecteerbaar was of niet. Wij menen dat de klager de fraude in principe had *kúnnen* detecteren, omwille van de verschillende contextboodschappen die verschenen op uw kaartlezer bv. ‘aanpassing limiet OK?’, ‘aankoop op internet’ gevolgd door het bedrag en OK.

In dit dossier moet dus, omwille van voorgaande, de basisregel worden toegepast uit artikel VII.44 WER: de bank dient het verlies te dragen, na aftrek van een franchise van 50 euro, tenzij de bank bewijs kan leveren

dat de betaler met grove nalatigheid bepaalde verplichtingen niet zou zijn nagekomen. Voor de beoordeling van de grove nalatigheid moet rekening worden gehouden met alle feitelijke elementen.

De klager heeft tijdens het telefoongesprek verschillende responscodes, gegenereerd door gebruik van zijn kaarten en kaartlezer, doorgegeven. Het communiceren van deze codes kan in principe als een grove nalatigheid worden gekwalificeerd. Zelfs een bankmedewerker zal nooit vragen om deze codes mondeling door te geven. Met behulp van deze codes kon de fraudeur de betwiste betaling uitvoeren.

Ook al begrijpen wij dat de cliënt heeft gehandeld vanuit een soort paniekreactie (de man sprak van fraude met zijn kaart), en is in deze absoluut het slachtoffer, zien wij, rekening houdend met de concrete feitelijke omstandigheden, jammer genoeg geen wettelijke basis om van de bank een tussenkomst in de schade te *eisen*.

De bank is niet bereid een vergoedingsvoorstel te doen, ook niet in het kader van deze bemiddelingsprocedure.