1. DE FEITEN

Op 1 mei hebt u 2 jassen van uw moeder via Vinted te koop aangeboden. Hiervoor had u een nieuw Vinted-profiel gecreëerd. Het was uw eerste verkoop. U vroeg 30 euro per jas. U kreeg meteen reactie van een persoon die zich voorstelde als hleblond11. De persoon deed een bod op een jas en zei dat het bedrag meteen overgemaakt was.

Ondertussen kreeg u mails van Vinted. Toen u doorklikte leek het dat de app van Vinted openging. U moest dan uw rekening koppelen aan Vinted zodat het bedrag van 30 euro op uw rekening kwam. U hebt dit uitgevoerd zoals gevraagd.

Het was niet mogelijk om de debetkaart te koppelen, daarom hebt u uw kredietkaart genomen. U moest uw kaartlezer gebruiken en M2 gebruiken. U vond dit vreemd. Er verscheen op het scherm dat u dit nogmaals 2 keer moest doen. Omdat u dit verdacht vond, bent u meteen uw uitgaven van uw kredietkaart nagegaan. U zag dat er 1.500 euro was afgegaan als betaling naar Western Union. U hebt de kredietkaart laten blokkeren en de fraude gemeld aan de bank.

De bank heeft u initieel doen denken dat u het geld mogelijk zou terugkrijgen, er is u valse hoop gegeven.

Via deze procedure hoopt u alsnog op een tussenkomst van de bank in uw schade.

2. STANDPUNT VAN DE BANK

De Bank heeft nazicht van de betwiste transactie gedaan. Hieruit blijkt dat de transactie tot stand is gekomen met de Visakaart xxxx, die op uw naam staat en dat deze werd bevestigd met een code die door een kaartlezer werd gegenereerd. Dat maakt het tot een 3DSecure-verrichting die tot stand kwam door middel van zijn persoonlijke identificatiegegevens, zoals ook EquensWorldline (EWL) in hun antwoord vermeldde. In de hoger beschreven omstandigheden waarin de verrichtingen zich hebben voorgedaan, is EWL er niet toe gehouden om het bedrag te vergoeden. Ook de bank is daartoe niet gehouden.

Daarvoor verwijzen we naar de Algemene Voorwaarden van de Bank, en meer bepaald naar het Artikel x “Grove nalatigheid“. Dit artikel vermeldt : “Afhankelijk van de feitelijke omstandigheden en onverminderd de beoordelingsbevoegdheid van de rechter kan als grove nalatigheid in hoofde van de Houder of de Gebruiker worden beschouwd: • het onthullen van een Persoonlijk veiligheidsgegeven, inclusief een authenticatiecode, op een website of een mobiele applicatie die niet van de Bank is noch van een dienstverlener zoals bedoeld in artikel 8 van deze bijlage, terwijl de gebruiker geacht wordt de gebruikelijke informaticabeveiligingsregels toe te passen, beschreven in de voorzorgsmaatregelen zoals bedoeld in artikel 5.2.”

Op basis van het geheel van bovenvermelde elementen begrijpt de bank het standpunt dat EWL in deze zaak heeft meegedeeld en dat zij ook aan de bank hebben bevestigd. Om hogervermelde redenen is het ook voor de bank niet mogelijk om een schadevergoeding uit te keren in dit dossier.

3. ONS ADVIES

U bent jammer genoeg het slachtoffer geworden van phishing. In het kader van de verkoop van kledingstukken via Vinted (uw eerste ervaring met Vinted) kreeg u een bericht van de koper via de Vinted-chat.

U kreeg nadien een mail, schijnbaar van “offers VintedTeam”:

U moest op een knop klikken om de aankoop te autoriseren. De mail leek van Vinted te komen maar werd feitelijk verzonden vanuit het mailadres ‘notify192688@icloud.com’.

Na het klikken op de knop, kwam u terecht op een pagina waarin u uw kaartgegevens moest linken aan uw profiel aan de hand van kaart en kaartlezer.

U voerde enkele keren een handeling uit, eerst met uw debetkaart -maar dit lukte niet- en nadien met uw kredietkaart en kaartlezer. Toen u de melding kreeg dat u dit nogmaals 2 keer moest herhalen, kreeg u argwaan en stopte u uw handelingen.

U wist niet dat u door het aanklikken van de link op een valse website, onder controle van een fraudeur, terechtgekomen was. Door hier met kredietkaart en kaartlezer gegenereerde codes in te voeren, is de fraudeur erin geslaagd deze te onderscheppen. Hiermee heeft de fraudeur vervolgens 1 betaling kunnen bevestigen.

Aansprakelijkheidsverdeling bij niet-toegestane betalingstransacties

Aangezien u in geen geval ingestemd hebt met de uitvoering van de betwiste verrichting, is in dit dossier sprake van een niet-toegestane betalingstransactie in de zin van artikel VII.32, §2, lid 4 WER (Wetboek Economisch Recht). Bijgevolg zijn de bepalingen uit het WER inzake de aansprakelijkheidsverdeling bij niet-toegestane betalingstransacties van toepassing.

We kunnen vooreerst verwijzen naar artikel VII.43, § 1, WER. Dit artikel legt het beginsel vast dat de betalingsdienstaanbieder van de betaler in geval van een niet-toegestane betalingstransactie de betaler onmiddellijk het bedrag van die betalingstransactie moet terugbetalen. In de context van internetfraude stelt Ombudsfin vast dat de banken maar zelden deze bepaling toepassen, omdat zij doorgaans artikel VII.44 van het WER, dat afwijkt van voornoemd artikel VII.43 WER door de regels voor de aansprakelijkheidsverdeling vast te leggen, willen analyseren alvorens tot terugbetaling over te gaan.

Artikel VII.44, §1, lid 2, 1° WER voorziet het volgende:

> *“In afwijking van het eerste lid, draagt de betaler geen enkel verlies indien het verlies, de diefstal of het onrechtmatig gebruik van een betaalinstrument niet kon worden vastgesteld door de betaler voordat een betaling plaatsvond, tenzij de betaler zelf frauduleus heeft gehandeld.”*

Dit wetsartikel is van toepassing wanneer het slachtoffer van een fraudegeval het onrechtmatig gebruik van zijn betaalinstrument vooraf niet kon detecteren. De voorbereidende werken bij de wet stellen dat dit artikel bijvoorbeeld kan worden toegepast in bepaalde gevallen van phishing. De vraag of de fraude al dan niet op voorhand gedetecteerd kon worden, hangt af van alle feitelijke elementen. De niet-detecteerbaarheid moet worden aangetoond door de betaler.

Volgens Ombudsfin is deze bepaling in dit dossier niet van toepassing. U had zich immers vragen kunnen stellen bij het door de fraudeur gebruikte emailadres ('notify192688@icloud.com').
Ook gebeurt alle communicatie tussen koper en verkoper in principe binnen de Vinted app, niet daarbuiten via aparte mails. We merken in dit kader terzijde op dat de website van Vinted duidelijk wijst op het feit dat alles binnen de app moet blijven verlopen:
De website *https://www.vinted.be/help/4/26-stap-voor-stap-verkopen*, vermeldt expliciet onder de noemer 'Belangrijk': **"***Het is belangrijk dat je tijdens het gehele verkoopproces op Vinted blijft (*dus in de app!) – *vanaf het chatten tot het ontvangen van je betaling…".*

Ombudsfin is van mening dat u de fraude op voorhand had kunnen detecteren (zelfs als het echter ook vaststaat dat u de fraude als dusdanig niet gedetecteerd hebt).

Aangezien artikel VII.44, §1, lid 2, 1° WER niet van toepassing is, moet worden teruggevallen op de basisregel 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.

Ombudsfin is van mening dat er enkele zaken kunnen doen besluiten tot een zekere onvoorzichtigheid maar dat er onvoldoende elementen in dit dossier bewijs vormen van een *grove* nalatigheid.

U wist immers niet dat de link naar een valse website, onder controle van de fraudeur, leidde. Belangrijk is dat uw gegevens op slinkse wijze zijn *onderschept*. U hebt uw gegevens op geen enkel moment zomaar doorgegeven aan de fraudeur. U hebt ze ingevoerd in een specifiek scherm waarin u enkel de gegevens van uw kaart en de verkregen code kon invoeren.

U hebt aangetoond dat de frauduleuze mail er echt uitzag en dat die op het eerst gezicht ook van Vinted zelf leek te komen (gelijkaardige "look and feel").

Verder menen we ook dat de website van Vinted niet geheel duidelijk is op alle vlak. Voor een eerste gebruiker kon deze procedure als niet *flagrant* afwijkend overkomen.

U dacht, als eerste gebruiker, effectief dat dit de geijkte procedure was en dat u de handelingen moest doen om uw kaart te koppelen aan uw profiel. Het gebruik van de kaart en kaartlezer, alhoewel onlogisch als een bedrag moet ontvangen worden, hoeven volgens Ombudsfin niet per se te leiden tot grove nalatigheid. De kaartlezer wordt al een tijdje niet meer enkel gebruikt om betalingen te doen. De kaartlezer wordt ook gebruikt om itsme te installeren (en de identiteit te bevestigen), om kaarten te koppelen aan betaalapps zoals Payconiq (en de kaartgegevens dus te bevestigen en zich akkoord te verklaren met de koppeling). Bovendien vermeldt de bank ook geen contextboodschappen op de kaartlezer waardoor u niet niet flagrant kon weten dat u een online betaling voor een bepaald bedrag aan het bevestigen was.

Op basis van voorgaande elementen hebben wij ten aanzien van de bank verdedigd dat de bank in dit dossier gehouden is tot een tussenkomst in uw schade. Jammer genoeg heeft de bank ons laten weten dat zij niet zal ingaan op onze vraag tot tussenkomst, noch geheel noch gedeeltelijk.

Recuperatie

De betwiste verrichting betrof een betaling. Eenmaal betalingen geïnitieerd en goedgekeurd zijn, kunnen deze niet meer worden tegengehouden door de bank. De handelaar kreeg immers van de bank de bevestiging dat de transactie goedgekeurd was, waarna deze kon overgaan tot de levering van de door de fraudeur bestelde goederen/diensten.

Aangezien bij betalingen vaak meteen goederen of diensten in ruil geleverd worden, kunnen per betaling ontvreemde gelden veelal niet meer gerecupereerd worden. Een recuperatie van een frauduleuze betaling zal slechts mogelijk zijn wanneer de begunstigde handelaar actief medewerkt. Slechts in sommige gevallen zal de handelaar een terugbetaling toestaan. Het is echter niet de verantwoordelijkheid van de bank om een terugbetaling te vorderen ten aanzien van de handelaar.

Wij sluiten ons dossier hierbij af.