

Dossier van de maand : Phishing – Frauduleuze verrichtingen tussen (onder andere) een persoonlijke rekening en een rekening waarop de houder van de persoonlijke rekening volmachthouder was - Gebrek aan sterke cliëntauthenticatie

1. DE KLACHT

U dient een klacht in in eigen naam en als bestuurder van een vennootschap. U, de vennootschap en een aantal verenigingen van mede-eigenaars (VME's) waarvoor u gevolmachtigde was, houden allen rekeningen aan bij dezelfde bank.

U werd het slachtoffer van fraude. U hebt hierover een klacht ingediend bij de politie.

In het proces-verbaal van de strafklacht en in de klacht die u bij Ombudsfm hebt ingediend, lezen wij de volgende feiten:

- Vorig jaar kreeg u een melding op uw computer met de boodschap dat u via een vermeld telefoonnummer contact diende op te nemen met de bank.
- Volgens uw verklaring in het proces-verbaal belde u het vermelde telefoonnummer op en kreeg u een man aan de lijn die zich voorstelde als een medewerker van de bank. De man deelde u mee dat er verdachte verrichtingen plaatsvonden op uw rekening. In uw klacht bij Ombudsfm hebt u echter aangegeven dat u werd opgebeld.
- Om te controleren of u wel degelijk een bankmedewerker aan de lijn had gaf u 2 eind nummers van een bankrekening en vroeg u om het saldo op een bepaalde datum te geven. De man aan de lijn kon dit.
- U moest op instructie van de zogezegde bankmedewerker verschillende handelingen stellen om uw rekeningen te blokkeren. U kreeg argwaan toen u ook vragen kreeg over uw rekeningen bij een andere bank.
- Na stopzetting van het frauduleus telefoongesprek, hebt u contact opgenomen met de andere bank met de vraag om uw rekening te blokkeren.
- U bent ook opgebeld door een andere financiële instelling met de vraag of u via hun platform een overschrijving naar een buitenlandse rekening had uitgevoerd. U ontkende dit en vroeg om deze overschrijving tegen te houden.
- Daarna bent u naar uw lokaal bankkantoor gegaan van de bank tegen wie u deze klacht hebt gericht. Daar heeft men uw rekeningen laten blokkeren (via, naar u vermoedt, een oproep naar een interne dienst van de bank). Men heeft u ook aangeraden om een klacht in te dienen bij de politie. U kreeg geen rekeninguittreksel mee van de frauduleuze verrichtingen.
- Enkele dagen later bent u opnieuw naar uw lokaal bankkantoor gegaan en ontving u een afdruk van de rekening van de vennootschap waarvan u bestuurder bent. Hierop stelde u vast dat er vanop de rekening van de

vennootschap een bedrag van 25.015 euro was overgeschreven naar een buitenlandse rekening. Er was geen begunstigde vermeld. Uw bankmedewerker schreef nadien met de hand de naam van de begunstigde op het afschrift. Het betrof een begunstigde met een rekeningnummer buiten de SEPA-zone. U stelde ook vast dat voorafgaand aan de buitenlandse overschrijving verschillende overschrijvingen waren uitgevoerd naar de rekening van de vennootschap: een totaalbedrag van 39.350 euro werd overgeschreven vanop rekeningen van VME's (waarvoor u gevolmachtigde was) en een bedrag van 11.250 euro werd vanop uw persoonlijke rekening overgeschreven naar de rekening van de vennootschap.

- Diezelfde dag bent u opnieuw naar de politie gegaan om een proces-verbaal te laten opmaken. U sprak met de politieagent over de mogelijkheid dat het naar een buitenlandse rekening buiten de SEPA-zone overgeschreven geld nog op een wachtrekening stond en mogelijks zou kunnen worden gerecupereerd (doch zonder garanties).
- In de periode juli -september 2025 diende u zich verschillende keren naar uw lokaal bankkantoor te begeven om facturen te laten betalen en om te informeren naar nieuwe bankkaarten. U ontving pas begin oktober 2025, en dus meer dan 3 maanden na de fraude, nieuwe bankkaarten.

U bent van mening dat de bank uw fraudemelding niet correct heeft opgevolgd en heeft nagelaten de schade-verwekkende overschrijving van de rekening van de vennootschap naar een buitenlandse rekening buiten de SEPA-zone tegen te houden. U verwijst daarbij naar communicaties van de bank waarin wordt aangegeven dat het voor niet-SEPA overschrijvingen tot 5 dagen kan duren vooraleer de gelden beschikbaar zijn voor de begunstigde.

U vraagt dat de bank het financieel nadeel van 25.015 euro vergoedt. Dit is het bedrag dat vanop de rekening van de vennootschap is overgeschreven naar een buitenlands rekeningnummer buiten de SEPA-zone (plus kost). Deze overschrijving werd voorafgegaan door een overschrijving vanop uw persoonlijke rekening (voor een bedrag van 11.250 euro) en overschrijvingen vanop de rekeningen van de VME's (voor een totaalbedrag van 39.350 euro) telkens naar de rekening van de vennootschap.

2. OORSPRONKELIJK STANDPUNT VAN DE FINANCIËLE INSTELLING

De bank heeft ons volgend initiële standpunt bezorgd:

“ (...) De klant betwist negen overschrijvingen die allen op dezelfde datum zijn uitgevoerd van verschillende rekeningen waarvan zij mandataris of titularis is. Zelf kan de klant geen verklaring geven hoe de overboekingen konden worden uitgevoerd.

Analyse van de verrichtingen toont aan dat de verrichtingen werden uitgevoerd via internetbankieren en namelijk:

Interne transfers: (...)

Uitgaande overschrijving: (...)

De aanmelding voor gebruik van internetbankieren werd uitgevoerd via de persoonlijke bankkaart van de klant. De kaart werd ook nooit als verloren of gestolen gemeld. Er werd ook gebruik gemaakt van een bijkomende manipulatie met de kaart en kaartlezer.

Aangezien deze aanmelding via een strenge authenticatie verliep zijn de betwiste verrichtingen volgens Artikel VII.32 §1 en 2 van het WER toegestaan. In dat geval is de bank er niet toe gehouden om de schade ervan te vergoeden.

Ook indien de klant van mening is geen toestemming te hebben gegeven voor deze transacties, is het zo dat ze ofwel werden uitgevoerd door een derde die tijdelijk toegang had tot de bankkaart en kennis had van de hieraan verbonden geheime code ofwel dat de klant een derde heeft toegelaten in het bezit te komen van haar handtekeningprocedure en dit door bankgegevens door te geven, wat een nalatigheid vanwege de klant uitmaakt.

Het niet naleven van de voorzorgsmaatregelen zoals opgenomen in de algemene bankvoorwaarden wordt als element van grove nalatigheid beschouwd.

Het begrip 'grote nalatigheid' is een juridische term en houdt geen waardeoordeel van de bank in.

Na de fraudemelding werd op (datum) een recuperatieaanvraag overgemaakt. De corresponderende bank verwees evenwel naar de wetgeving van het land van de begunstigde die voorziet dat de begunstigde zijn of haar akkoord dient te bevestigen voor een eventuele terugboeking. Aangezien er geen contact kon gelegd worden door de correspondent was er geen terugboeking mogelijk.

Conclusie

Gebaseerd op alle bovenstaande dossierelementen dienen we te bevestigen niet te kunnen ingaan op de gevraagde vergoeding van de geleden schade.

De verrichtingen verliepen via een strenge authenticatie en de bank heeft eveneens een recuperatieaanvraag overgemaakt; maar daar wilde de correspondentbank niet op ingaan."

3. ONS ADVIES

A. Fraudeverloop: vishing

U bent jammer genoeg het slachtoffer geworden van fraude gekend als vishing (voice + phishing), waarbij een fraudeur erin geslaagd is om u via de telefoon te overtuigen

handelingen te stellen met uw bankkaart, pincode en kaartlezer om zogezegde fraude tegen te gaan.

In het proces-verbaal van uw strafklacht hebben wij gelezen dat u, nadat u een bericht ontving op uw computer dat afkomstig leek van de bank, het in het bericht vermelde nummer hebt opgebeld en dat u dacht een medewerker van de bank aan de lijn te hebben. U hebt ons tijdens onze bemiddeling het betrokken bericht niet kunnen overmaken. Ook het telefoonnummer dat u diende te bellen hebt u niet kunnen terugvinden. U hebt ons eveneens aangegeven dat u in uw herinnering opgebeld werd door een onbekend nummer (eerder dan dat u zelf gebeld hebt). U hebt navraag gedaan bij uw telecomprovider om de tijdstippen van deze oproep(en) na te gaan, maar u hebt deze niet ontvangen.

Tijdens onze bemiddeling hebt u aangegeven dat u uw bankkaartnummer diende over te maken opdat de zogezegde bankmedewerker een overzicht zou krijgen van alle rekeningen waarop u volmacht had.

De zogezegde bankmedewerker won uw vertrouwen doordat hij u de correcte saldi van de rekeningen kon geven. Hoe dit kan, kunnen wij jammer genoeg niet verklaren. Oplichters maken vaak gebruik van technieken van psychologische manipulatie om u de indruk te geven dat zij over uw informatie beschikken. Ook maken fraudeurs gebruik van eerder via klassieke phishing onderschepte (bank)gegevens om hun slachtoffer op een geloofwaardige manier te overtuigen van de legitimiteit van een oproep. Wanneer oplichters via een voorafgaande phishing al toegang hebben verkregen tot de online bankomgeving van hun slachtoffer (waarbij zij zicht hebben op de rekeningen van het slachtoffer en al verrichtingen tussen eigen rekeningen van het slachtoffer kunnen uitvoeren), slagen zij er veelal in een zeer geloofwaardig verhaal te brengen. Of dit ook in het voorliggend dossier is gebeurd, kunnen wij evenwel niet achterhalen.

Verder hebt u ons toegelicht dat u, nadat de zogezegde bankmedewerker uw vertrouwen had gewonnen, u een aantal cijfers per rekening diende in te geven zogezegd om uw rekeningen te blokkeren. U gaf ons eveneens mee dat u met uw bankkaart, pincode en kaartlezer codes diende aan te maken en door te geven (via uw computer die onder controle stond van de fraudeur). Dit was nodig om zogezegde frauduleuze verrichtingen op de rekeningen tegen te houden en de rekeningen te blokkeren. U herinnert zich verder geen details over welke handelingen u exact diende te stellen.

Uit de technische gegevens van de bank blijkt dat minstens twee responscodes moeten zijn aangemaakt en door de fraudeur onderschept. Een fraudeur slaagde er zo in om met één onderschepte responscode in te loggen op uw internetbankieren en overschrijvingen tussen de rekeningen waarop u volmacht had goed te keuren. Met een tweede onderschepte responscode werd de schade-verwekkende overschrijving van 25.000 euro (plus 15 euro kosten) goedgekeurd. De bankkaart en pincode die werden gebruikt voor de aanmaak van deze responscodes was de bankkaart gekoppeld aan uw persoonlijke rekening.

Tijdens de bemiddeling hebt u aangegeven dat u geen aanwijzingen hebt dat uw computer werd overgenomen vanop afstand (bijvoorbeeld via applicaties zoals Anydesk of Teamviewer). Het feit dat u, volgens uw verklaring in het proces-verbaal van uw strafklacht, een bericht zag op uw computerscherm doet evenwel anders vermoeden. Ook heeft de bank ons tijdens de bemiddeling meegedeeld dat de acties op uw internetbankieren gebeurden vanop een door de bank voor u gekend IP-adres dat eerder ook voor uw internetbankieren was gebruikt. Dat vanop een bij de bank voor uw gekende locatie gebruik werd gemaakt van uw internetbankieren, terwijl u betwist dat u zelf de verschillende verrichtingen hebt uitgevoerd, doet vermoeden dat een fraudeur er wel degelijk in geslaagd is uw computer over te nemen.

U sprak verder tijdens onze bemiddeling over het gebruik van een e-id kaartlezer. Wij hebben evenwel geen zicht op het eventueel misbruik dat een fraudeur van uw e-id gegevens zou hebben gemaakt.

B. Wettelijke aansprakelijkheidsregeling bij niet-toegestane betalingstransacties voor consumenten versus niet-consumenten

Ombudsfin is van mening dat u duidelijk aannemelijk maakt dat u niet bewust heeft ingestemd met de betwiste verrichtingen. U werd telefonisch gecontacteerd door een fraudeur die zich voordeed als een bankmedewerker. U werd volledig misleid en heeft de instructies van de fraudeur gevolgd. U dacht dat u door uw handelingen fraude zou voorkomen. U wist niet dat u door uw handelingen responscodes zou berekenen waarmee de fraudeur toegang zou verwerven tot uw internetbankieren, overschrijvingen tussen rekeningen waarop u een volmacht had zou uitvoeren en uiteindelijk de schade-verwekkende overschrijving naar een buitenlandse rekening buiten de SEPA-zone zou goedkeuren.

Aangezien u niet hebt ingestemd met de uitvoering van de betwiste verrichtingen, is in dit dossier sprake van niet-toegestane betalingstransacties in de zin van artikel VII.32 van het Wetboek Economisch Recht (hierna 'WER').

Bijgevolg zijn de bepalingen uit het WER inzake de aansprakelijkheidsverdeling bij niet-toegestane betalingstransacties (artikelen VII.43 en VII.44 WER) van toepassing. Deze aansprakelijkheidsregeling speelt in principe zowel ten aanzien van consumenten als niet-consumenten. Wel is het zo dat het WER toelaat dat banken met klanten die geen consumenten zijn overeenkomen dat de objectieve aansprakelijkheidsregeling bij niet-toegestane betalingstransacties geheel of gedeeltelijk niet van toepassing is.

Artikel VII.29 WER luidt als volgt:

“Wanneer de betalingsdienstgebruiker geen consument is, kunnen partijen overeenkomen dat de artikelen VII.30, § 1, VII.32, § 3, VII.33, VII.42, VII.44, VII.46 en VII.47, VII.50, VII.55/3 tot VII.55/7, in het geheel of ten dele niet van

toepassing zijn. *Partijen kunnen ook een andere termijn overeenkomen dan die welke is bepaald in artikel VII.41.” (eigen markering)*

De bank heeft van deze mogelijkheid gebruik gemaakt via haar algemene bankvoorwaarden: (...)

In het voorliggend dossier bent u als privépersoon houder van uw persoonlijke rekening en kwalificeert u wat deze rekening betreft als consument. De vennootschap kwalificeert niet als consument. Wij geven u verder mee dat VME's wat betreft de toepassing van artikel VII.43 en VII.44 WER volgens ons ook niet als consument kwalificeren. Hoewel het WER in bepaalde domeinen voorziet dat sommige VME's dezelfde bescherming als consumenten genieten (zie bijvoorbeeld artikel VI.81/1 WER wat betreft onrechtmatige bedingen in overeenkomsten met consumenten), voorziet het WER niet in zo'n bescherming wat betreft de toepassing van de artikelen VII.43 en VII.44 WER.

Nu er in het kader van de fraude waarvan u het slachtoffer werd sprake is van een verrichting vanop uw persoonlijke privérekening naar de professionele rekening van de vennootschap, gevolgd door een verrichting vanop die laatste rekening naar een derde, stelt zich de vraag in welke mate de bank zich kan beroepen op de in haar algemene voorwaarden voorziene beperking van de wettelijke aansprakelijkheidsregeling bij niet-toegestane betalingstransacties voor niet-consumenten.

Tijdens de behandeling van het dossier heeft Ombudsfm hierover haar college van deskundigen specifiek geraadpleegd.

Het college van deskundigen heeft op 7 april 2026 het volgende advies verschaft:

“Wanneer in het kader van één enkele fraude door een fraudeur eerst gelden worden overgemaakt van een privérekening naar een professionele rekening waartoe de houder van de privérekening via zijn webbanking toegang heeft, en vervolgens gelden worden getransfereerd van deze professionele rekening naar de rekening van een fraudeur, dan kan van artikel VII.44 WER enkel worden afgeweken voor de tweede niet-toegestane betalingstransactie. Voor de eerste niet-toegestane transactie is een afwijking van het regime uit artikel VII.44 WER niet mogelijk, aangezien het slachtoffer deze rekening voert als een consument. Deze interpretatie verzekert dat een consument die het slachtoffer wordt van betaalfraude op dezelfde manier wordt behandeld ongeacht het verdere verloop van de fraude.

In casu werd van de privérekening van het slachtoffer een bedrag van 11.250 euro overgemaakt naar een professionele rekening van een vennootschap waartoe het slachtoffer toegang had via zijn internetbankieren omgeving. Vervolgens werd via deze rekening 25.000 euro overgemaakt naar een rekening onder controle van de fraudeur in het buitenland. Bovenstaande redenering impliceert dat voor de niet-toegestane betalingstransactie ten belope van 11.250 euro het regime uit artikel

VII.44 WER toepassing vindt. Voor de tweede niet-toegestane betalingstransactie kan van het regime uit artikel VII.44 WER worden afgeweken in de bankvoorwaarden.”

Hierna bespreken wij eerst de toepassing van de wettelijke aansprakelijkheidsregeling op de niet-toegestane betalingstransactie vanop uw privérekening ten belope van 11.250 euro.

Daarna gaan wij verder in op de niet-toegestane betalingstransactie vanop de rekening van de vennootschap ten belope van 25.015 euro.

C. Toepassing van de wettelijke aansprakelijkheidsregeling op de niet-toegestane betalingstransactie vanop uw privérekening

Vooreerst is artikel VII.43, §1 WER van toepassing. Op basis van dit artikel moet de bank haar klant onmiddellijk (maar op voorlopige basis) het bedrag van niet-toegestane betalingstransacties terugbetalen, tenzij de bank redelijke gronden heeft om fraude in hoofde van haar klant te vermoeden en de bank deze gronden schriftelijk heeft meegedeeld aan de FOD Economie.

In de context van internetfraude stelt Ombudsfinaal vast dat banken maar zeer zelden tot (voorlopige) terugbetaling overgaan, omdat zij doorgaans eerst de toepassing van de in artikel VII.44 WER voorziene regels rond aansprakelijkheidsverdeling tussen de klant en de bank wil analyseren. De toepassing van de regels van artikel VII.44 WER bepaalt op definitieve wijze in welke mate de bank moet tussenkomen in de schade.

Bijzonder relevant in het voorliggend dossier is artikel VII.44§2 WER dat luidt als volgt:

“§2. Wanneer de betalingsdienstaanbieder van de betaler geen sterke cliëntauthenticatie verlangt, draagt de betaler geen eventuele financiële verliezen, tenzij de betaler frauduleus heeft gehandeld.

Ingeval sterke cliëntauthenticatie door de begunstigde of de betalingsdienstaanbieder van de begunstigde niet wordt aanvaard, wordt de door de betalingsdienst-aanbieder van de betaler geleden financiële schade door hem vergoed.” (eigen markerings)

In het voorliggend dossier is een fraudeur erin geslaagd om op basis van één onderschepte responscode (aangemaakt met bankkaart, pincode en kaartlezer) in te loggen op internetbankieren. De toegang tot internetbankieren was dan ook onderworpen aan een sterke cliëntauthenticatie.

Als algemene regel geldt verder dat banken in sterke cliëntauthenticatie moeten voorzien indien een betaler:

- zich online toegang tot zijn betaalrekening verschaft;

- een elektronische betalingstransactie initieert;
- via een communicatiemiddel op afstand een verrichting uitvoert die een risico op betalingsfraude of andere vormen van misbruik of bedrog met zich mee kan brengen.

(zie artikel 47 en 145 van de [wet van 11 maart 2018 betreffende het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld](#))

Afwijkingen zijn evenwel toegestaan, voor zover deze in lijn zijn met de [Europese Gedelegeerde Verordening Sterke Cliëntauthenticatie](#).

De bank lichte ons tijdens de behandeling van het dossier toe dat wat betreft de overschrijving van uw privérekening naar de rekening van de vennootschap zelf geen sterke cliëntauthenticatie vereist was als volgt:

"Als een klant interne overboekingen wil uitvoeren tussen de eigen rekeningen en/of rekeningen waarvoor de klant gekend is als gevolmachtigde, dienen deze overboekingen niet bijkomend te worden ondertekend. Aangezien dit interne overdrachten betreft is er ook geen verlies voor de klant".

Vanuit Ombudsfin meenden wij dat bij deze praktijk vragen konden worden gesteld. Tijdens de behandeling van het dossier heeft Ombudsfin hierover dan ook haar college van deskundigen specifiek geraadpleegd.

Het college van deskundigen heeft hieromtrent het volgende advies verschaft:

"Wat de transactie van 11.250 euro betreft, wordt vastgesteld dat zij heeft plaatsgevonden zonder sterke cliëntenauthenticatie. De overboeking van dit bedrag kon immers plaatsvinden zonder dat daarbij een geheime code moest worden ingevoerd. Het loutere feit dat voorafgaandelijk aan de uitvoering van de transactie gebruik werd gemaakt van sterke cliëntenauthenticatie om toegang te verkrijgen tot de omgeving van internetbankieren volstaat niet opdat de betalingstransactie op zich het voorwerp uitmaakt van sterke cliëntenauthenticatie. Een eerder geauthenticeerde sessie kan wel één element van de SCA leveren, maar dan moet bij de betaling zelf nog het andere element aanwezig zijn én, bij remote betalingen, een dynamic linking met het concrete bedrag en de begunstigde (https://www.eba.europa.eu/single-rule-book-qa/qna/view/publicId/2018_4141). Als de transactie dus enkel kon doorgaan omdat men al in de omgeving van internetbankieren zat, zonder een bijkomende transactie specifieke authenticatie (zoals het expertenpanel afleidt uit de beschikbare gegevens in het dossier), dan is de betaling uitgevoerd zonder sterke cliëntenauthenticatie.

In dat geval draagt de betaler op grond van artikel VII.44 §2 WER geen enkele aansprakelijkheid voor deze niet-toegestane transactie die heeft plaatsgevonden

zonder sterke cliëntenauthenticatie. Deze bijzondere regel vindt niet alleen toepassing wanneer op grond van de Gedelegeerde Verordening sterke cliëntenauthenticatie verplicht is, doch tevens wanneer de Gedelegeerde Verordening inzake sterke cliëntenauthenticatie toelaat om geen gebruik te maken van sterke cliëntenauthenticatie. We merken in dit kader ook nog op dat de uitzondering waarin artikel 15 voorziet voor transacties tussen door dezelfde natuurlijke persoon of rechtspersoon aangehouden rekeningen niet speelt indien de rekeninghouder van de gedebiteerde rekening slechts een volmacht heeft met betrekking tot de begunstigde rekening en niet de titularis van de rekening is.

In geval waarin de vrijstelling van aansprakelijkheid speelt ingevolge afwezigheid van sterke cliëntenauthenticatie, speelt een eventuele grove nalatigheid in hoofde van de betaler geen rol. De betalingsdienstaanbieder dient in casu dan ook de privé-rekening met 11.250 euro te crediteren. Gelet op de afwijking van artikel VII.44 WER in de bankvoorwaarden met betrekking tot de professionele rekening (rekening op naam van de vennootschap), rust er geen aansprakelijkheid op de betalingsdienstaanbieder voor de transactie van 25.015 euro (die overigens wel het voorwerp uitmaakte van een sterke cliëntenauthenticatie). Het bedrag van 25.015 euro moet dan ook niet opnieuw gecrediteerd worden op de professionele rekening.”

Op basis van dit advies hebben wij de bank gevraagd om haar initieel standpunt te herzien en u het bedrag van 11.250 euro te vergoeden.

De bank heeft ons meegedeeld dat zij akkoord gaat met de gevraagde tussenkomst van 11.250 euro als oplossing voor dit dossier.

Om de terugbetaling te kunnen uitvoeren zal de bank u een kwijtschrift voorleggen. De bank zal hierover rechtstreeks met u in contact treden.

D. Wat betreft de niet-toegestane betalingstransactie vanop de rekening van de vennootschap

Zoals hierboven toegelicht voorzien de algemene bankvoorwaarden van de bank dat rekeninghouders die geen consument zijn zich niet kunnen beroepen op bepaalde regels van objectieve aansprakelijkheidsregeling bij niet-toegestane betalingstransacties zoals voorzien in artikel VII.44 van het WER (in het bijzonder §1 en §2).

Een uitsluiting van de aansprakelijkheidsregeling is in principe toegestaan (zie artikel VII.29 WER), met dien verstande dat bepalingen die een kennelijk onevenwicht tussen de rechten en plichten van partijen schept als onrechtmatig zou kunnen worden beschouwd overeenkomstig artikel 5.52 van het Nieuw Burgerlijk Wetboek dat luidt als volgt:

“Elk beding waarover niet kan worden onderhandeld en dat een kennelijk onevenwicht schept tussen de rechten en plichten van partijen is onrechtmatig en wordt voor niet geschreven gehouden.

Bij de beoordeling van het kennelijk onevenwicht wordt rekening gehouden met alle omstandigheden rond het sluiten van het contract.

Het eerste lid is noch van toepassing op de bepaling van de hoofdprestaties van het contract, noch op de gelijkwaardigheid van deze hoofdprestaties.”

Dit maakt dat Ombudsfm wat betreft het financieel nadeel uit betwiste verrichtingen vanop een professionele rekening in principe geen toepassing kan maken van de objectieve aansprakelijkheidsregeling voorzien in het WER en moet terugvallen op de algemene aansprakelijkheidsregeling die speelt tussen partijen. Kort gezegd betekent dit dat een fout of nalatigheid in hoofde van de bank moet worden aangetoond om financieel nadeel dat voortvloeit uit deze fout of nalatigheid vergoed te zien. Wij merken hierbij ook op de bank haar aansprakelijkheid contractueel beperkt tot bedrog of een zware fout begaan door de bank of haar personeel in het kader van haar beroepsactiviteiten.

In deze context hebben wij verder gekeken naar de verplichtingen van de bank inzake (i) toepassing van sterke cliëntauthenticatie, (ii) fraudedetectie (had de bank de fraude zelf sneller moeten detecteren?) en (iii) recuperatie (heeft de bank nadat u de fraude ter kennis hebt gebracht het nodige heeft gedaan om te proberen de gelden te recupereren?).

(i) Wat betreft sterke cliëntauthenticatie

De overschrijving vanop de rekening van de vennootschap naar de buitenlandse rekening buiten de SEPA-zone ten belope van 25.015 euro werd goedgekeurd aan de hand van een met bankkaart, pincode en kaartlezer aangemaakte responscode en was dus onderworpen aan een sterke cliëntauthenticatie.

Wij merken in het voorliggend dossier wel op dat voor de overschrijvingen die gebeurden vanop de rekeningen vanop de VME's naar de rekening van de vennootschap (net zoals voor de overschrijving vanop uw privérekening) geen sterke cliëntauthenticatie werd gevraagd.

Nochtans is de bank verplicht sterke cliëntauthenticatie toe te passen bij de initiatie van betalingstransacties of bij de uitvoering via een communicatiemiddel op afstand van een verrichting die een risico op betalingsfraude of andere vormen van misbruik of bedrog met zich mee kan brengen (zie het hierboven geciteerd wettelijk kader inzake sterke cliëntauthenticatie).

Gelet op de wettelijke verplichting tot toepassing van sterke cliëntauthenticatie, menen wij dat vragen kunnen worden gesteld bij de rechtmatigheid van de uitsluiting van artikel VII.44 §2 WER in de algemene bankvoorwaarden van de bank.

Wij hebben dan ook gevraagd aan de bank of zij bereid was om ook voor het resterende financieel nadeel dat voortvloeit uit de verrichtingen die gebeurden vanop de rekeningen van de VME's een voorstel tot tegemoetkoming te doen. De bank wenste hier evenwel niet op in te gaan.

(ii) Wat betreft de verplichting tot fraudedetectie

Banken moeten beschikken over performante fraudepreventie- en fraudedetectiesystemen om fraudes te voorkomen en te stoppen. Verdachte transacties moeten zoveel als mogelijk worden gedetecteerd en tegengehouden. Deze verplichting vloeit voort uit de Europese Gedelegeerde Verordening 2018/389 over sterke cliëntauthenticatie en kadert in de algemene zorgvuldigheidsnorm die op eenieder rust, en meer specifiek de algemene zorgplicht van de bank ten aanzien van haar klanten.

Deze verplichting tot fraudedetectie in hoofde van de bank is een inspanningsverbintenis. Dit betekent dat de bank niet kan worden verplicht tot een resultaat waarbij elke fraude in elk individueel dossier wordt gedetecteerd. Bij het instellen van detectiesystemen bepalen banken algemene parameters om zoveel mogelijk fraude te detecteren, waarbij banken ook een afweging maken tussen veiligheid en gebruiksgemak. Een fraudetool kan daarbij nooit volledig een frauderisico ondervangen wanneer de klant zelf bepaalde bevestigingen uitvoert.

In het voorliggend dossier zagen wij onvoldoende elementen om bij de bank te bemiddelen voor een tussenkomst op basis van een eventuele gebrekkige fraudedetectie.

(iii) Wat betreft de recuperatiepogingen na kennisgeving van fraude

Na de kennisgeving van fraude met betwisting van betalingstransacties moet de bank redelijke inspanningen leveren om de gelden van de betwiste betalingstransacties te recupereren. Dit betekent dat de bank na de kennisgeving zo snel mogelijk het nodige moet doen om (i) in de mate van het mogelijke, betwiste verrichtingen tegen te houden, (ii) eventuele begunstigde rekeningen bij de bank zelf te blokkeren en (iii) een bericht te sturen naar iedere begunstigde financiële instelling met de vraag om de begunstigde rekeningen te blokkeren en eventueel beschikbare fondsen terug te storten. Deze verplichtingen voor de bank kaderen in de algemene zorgvuldigheidsnorm die op eenieder rust, en meer specifiek de algemene zorgplicht van de bank ten aanzien van haar klanten.

De bank gaf ons tijdens onze bemiddeling aan dat de gelden voor de internationale overschrijving snel na de bevestiging door de bank werden doorgestuurd en het niet zo is dat de overschrijving nog kon worden tegengehouden.

Wel stellen wij vast dat de bank pas de volgende dag een recall heeft uitgestuurd naar de bank van de begunstigde, terwijl de fraude al gekend was op de dag van de fraude toen de klant zich aanbood in uw lokaal bankkantoor om fraude te melden.

Vanuit de adviespraktijk van Ombudsfm vinden wij een tijdspanne van meer dan 20 uur na de kennisgeving van de fraude zonder meer te lang voor de opstart van een recuperatiepoging bij de bank van de begunstigde. Wij hebben dit tijdens onze bemiddeling voorgelegd aan de bank en gevraagd dat de bank alsnog zou tussenkomen in het geleden financieel nadeel, en dit minstens in de mate dat er bij de begunstigde financiële instellingen nog gelden beschikbaar waren onmiddellijk na uw fraudemelding.

De bank wenste hier evenwel niet op in te gaan en deelde ons het volgende mee:

"We gaan niet akkoord dat de bank haar recall laattijdig zou hebben overgemaakt. Bovendien zou een eventuele snellere aanvraag ook geen verschil hebben uitgemaakt aangezien de begunstigde bank zich verschuilt achter hun nationale wetgeving die voorziet dat de begunstigde zijn schriftelijk akkoord dient te bevestigen voor een eventuele terugboeking. Een eventuele nog snellere aanvraag had de terugboeking ook niet mogelijk gemaakt."

Hoewel wij van mening blijven dat de actie van de bank bij de begunstigde bank laattijdig was, kunnen wij, rekening houdend met het gebrek aan verplichte medewerking van de buitenlandse bank, het laattijdige opstarten van de recuperatiepoging door de bank niet zonder meer aanduiden als oorzaak van uw financieel nadeel.

Besluit

U bent het slachtoffer geworden van fraude door een geroutineerd fraudeur waarbij u ongetwijfeld onder druk en mogelijks vanuit een paniecreactie hebt gehandeld op de telefonische instructies van een fraudeur.

Wij zijn tevreden dat de bank bereid is gevonden om u het bedrag van 11.250 euro (met name de schade op uw privérekening) te vergoeden.

Verder zagen wij ruimte voor bemiddeling wat betreft het resterende financieel nadeel uit de niet-toegestane betalingstransactie vanop de rekeningen van de VME's naar de rekening van de vennootschap. Zo meenden wij dat de niet-toepassing van sterke cliëntauthenticatie bij de overschrijvingen vanop de rekeningen van de VME's naar de rekening van de vennootschap aan de bank kon worden verweten. De bank wenste onze argumentatie hierover evenwel niet te volgen.