BV-OECO thesisprijs 2024 Consumentenbescherming

Aansprakelijkheid bij phishing-fraude

Analyse van Belgische rechtspraak, met focus op

het verhogen van de rechtszekerheid

Masterproef voorgelegd voor het behalen van de graad master in de rechten aan UGent

Karl Dobbelaere

Promotor: Prof. dr. Reinhard Steennot

Commissaris: Sabe De Graef

SAMENVATTING

"En toen ik daarna op mijn rekening keek, bleek dat er grote bedragen waren overgeschreven."

Dagelijks doen Belgische slachtoffers deze tragische vaststelling nadat ze - al dan niet door een zogenaamde bankmedewerker - gecontacteerd werden per mail of telefoon.

Situering

Febelfin schat de financiële schade door phishingfraude in België op 40 M€/jaar, terwijl de financiële sector jaarlijks 120M€ aan phishingtransacties weet te blokkeren of te recupereren.

De Payment Services Directive (PSD2), voorziet in een Europese consumentbeschermingsregeling, waaronder een aansprakelijkheidsregeling. Voor niet-toegestane betalingen ligt de schadelast hierdoor in de regel grotendeels bij de betalingsdienstaanbieder (de bank), tenzij de betaler (phishing-slachtoffer) frauduleus handelde of grof nalatig was met betrekking tot zijn verplichtingen.
Met de invoering van de Payment Services Regulation (verwacht in de loop van 2026) zal de bestaande regeling verder uitgebreid worden naar bepaalde gevallen van toegestane betalingen, onder meer waar sprake is van spoofing-fraude (waarbij de fraudeur zich voordoet als een bankmedewerker). Ook zal de betalingsdienstaanbieder verplicht worden om een IBAN/naam-controle aan te bieden en om (nog meer) inspanningen te doen om verdachte transacties op te sporen en te blokkeren.

Masterproef beoogt rechtsonzekerheid bij phishingfraude te verminderen

In de masterproef onderzoeken we de obstakels waar een slachtoffer-consument in België mee te maken krijgt als hij door zijn bank vergoed wil worden voor geleden phishingschade bij niet-toegestane betalingen. Drie aspecten uit de aansprakelijkheidsregeling zorgen hierbij voor onduidelijkheid: de onmiddellijke restitutieplicht, het al dan niet toegestane karakter van de betaling en de beoordeling van grove nalatigheid in hoofde van de betaler.

In betwiste phishingdossiers blijkt de **onmiddellijke restitutieplicht** ex art. VII.43 WER heel vaak **dode letter**. Hoewel dit verklaard kan worden, en een strikte toepassing van deze regel ook ongewenste effecten zal hebben voor de consument die de finale aansprakelijkheid draagt, zorgt deze situatie er de facto wel voor dat een consument-slachtoffer vaak gedwongen wordt om een (juridische) procedure op te starten, wil hij vergoed worden.

Doorheen de afgelopen jaren heeft de Belgische rechtspraak de **criteria voor niet-toegestane betalingen verfijnd**. Het onderzoek gaf aanleiding tot een schema dat deze criteria samenvat op een manier die zowel voor een rechtspracticus als voor een slachtoffer-consument begrijpelijk en toepasbaar is. (zie Bijlage 1 bij deze samenvatting: *Criteria niet-toegestane betalingen*)

Hoewel een dergelijke dissectie ook voor het topic van de grove nalatigheid nuttig zou zijn, is het niet mogelijk om voor grove nalatigheid dergelijke criteria op te stellen. Het is namelijk de rechter die de grove nalatigheid dient te beoordelen, rekening houdend met alle feitelijke gegevens.
Om die reden werd een empirisch schema opgesteld dat de rode lijnen doorheen de Belgische rechterlijke uitspraken over grove nalatigheid weergeeft. Het schema laat toe om een aantal **bakens** aan te brengen **in het grensgebied tussen de gewone en de grove nalatigheid**. Ook dit schema helpt een slachtoffer-consument om zijn kansen op recht op vergoeding beter in te schatten. (zie Bijlage 2 - *Empirisch diagram Grove nalatigheid*)
Het telefonisch doorgeven van geheime codes leidt bijvoorbeeld systematisch tot een beoordeling als grove nalatigheid. Hoewel toenemende geraffineerdheid er zou kunnen voor zorgen dat een rechter hierover in de toekomst anders besluit, geeft het empirisch schema toch een eerste indicatie van de kansen die je als slachtoffer hebt op schadevergoeding.

Hetzelfde geldt bijvoorbeeld voor het doorgeven van een betaalapp-activatiecode die de bank per SMS doorstuurde onder expliciete vermelding om die code aan niemand door te spelen.

Consument nog te vaak in de kou

Zoals recente rapporten van Ombudsfin duidelijk aangeven, blijft de consument in een belangrijk deel van de betwiste phishingdossiers in de kou staan. In de gegronde dossiers werd de bemiddeling slechts in 32,7% van de gevallen succesvol afgesloten met een tussenkomst van de bank. De bank lijkt te wachten tot de consument de zaak voor de rechter brengt, of hoopt dat hij dat helemaal niet doet. In plaats van een "onmiddellijk herstel" van de rekening, duurt het hierdoor gemiddeld anderhalf jaar (4,5 jaar bij beroep) vooraleer het slachtoffer weet waar hij aan toe is.

Verbeterpistes aansprakelijkheidsregeling

Aangezien de geplande Payment Services Regulation de basisprincipes van de huidige regeling bevestigt, gaan we ervan uit dat er weinig ruimte is voor radicaal andere benaderingen om de consumentenbescherming te verhogen, alvast niet voor de nabije toekomst.

Vaststelling blijft dat phisher-fraudeurs de gemeenschappelijke vijand zijn van zowel banken als slachtoffers. In dat opzicht pleiten we voor een nauwe samenwerking van de verschillende *goede* actoren (o.m. financiële sector (Febelfin), consumenten(verenigingen) zoals Test-Aankoop, OmbudsFin, politiediensten en federale overheid). Het is hierbij aangewezen om maximaal te blijven inzetten op bewustzijn, preventie, detectie en bestrijding van phishing. Ook verder onderzoek naar o.m. het phishing- en money mule fenomeen blijft nuttig om de bewustmakingscampagnes optimaal aan te sturen.

Daarnaast pleiten we ook voor een *faire toepassing* van de regelgeving. Hierbij kunnen we denken aan het opstellen/aanvaarden/hanteren van gemeenschappelijke criteria voor niet-toegestane betalingstransacties. Verder zou ook een koppeling van de restitutieverplichting ex art. VII.43 WER aan een positief advies door Ombudsfin, of een restitutie door middel van een tijdelijk geblokkeerde rekening, kunnen bijdragen aan de consumentenbescherming. Dit kan tevens een compromis of tussenstap zijn tussen de huidige situatie en een radicale "pay first and argue later"-benadering[1]

Verbeterpistes bestrijding phishing

Tenslotte blijft er de algemene indruk dat de phishers al te vaak vrijuit gaan, en dat de vervolging ervan (te) weinig aandacht of prioriteit krijgt. Bij nagenoeg elke phishingpoging worden nochtans sporen nagelaten die kunnen helpen om figuren achter dit fenomeen te traceren en te stoppen.

Vandaag is het inzamelen van technisch-operationele details over de phishingfraude of poging daartoe zeer versnipperd, en niet gestandaardiseerd. Een nauwere samenwerking met en ondersteuning van de politiediensten vanuit de financiële sector, zou ongetwijfeld kunnen bijdragen aan de gezamenlijke strijd tegen een gemeenschappelijke vijand. Van een dergelijke investering kan op termijn iedereen de vruchten plukken.

[1] In de zaak C-409/22 voor het Hof van Justitie bevestigde Advocaat-Generaal CAMPOS SÁNCHEZ-BORDONA in dit verband recent de "pay first and argue later" filosofie.