Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

# 29 911 Bestrijding georganiseerde criminaliteit

**Nr. 314** **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 15 juni 2021

In deze brief geef ik mijn reactie op het verzoek van uw Kamer om te rapporteren over de inspanningen om criminelen die met behulp van spoofing en bankfraude slachtoffers maken, op te sporen en het misdaadgeld af te pakken[1]. Ook geef ik mede namens de Minister van Financiën en de Staatssecretaris van Economische Zaken en Klimaat een toelichting op de ingezette verbeteringen, zoals de maatregelen die de telecomsector en banken tot dusverre hebben genomen en die grotendeels zijn ingevoerd sinds het najaar van 2020. De telecomsector en Autoriteit en Consument (ACM) hebben aangeven dat de eerste resultaten reeds zijn geboekt met het reduceren van telefoniespoofing, met name bankhelpdeskfraude. Ook hebben de banken een coulancekader voor slachtoffers van spoofing in de vorm van bankhelpdeskfraude in het leven geroepen. Dit kader is met terugwerkende kracht in 2020 door banken toegepast en heeft geleid tot compensatie aan 96% van de geregistreerde slachtoffers. Door de banken zijn recentelijk de aanvullende toetsingscriteria gepubliceerd, zodat tevens transparant is wanneer banken spoofing in de vorm van bankhelpdeskfraude uit coulance niet vergoeden. Onze interdepartementale inzet is erop gericht om dit beleid te continueren en deze aan te vullen met gerichte publiek-private samenwerking in de vorm van concrete acties. Dit zullen wij na de zomer nader toelichten met een publiek-privaat plan voor een integrale aanpak.

## Spoofing en oplichting

Spoofing houdt in dat door misbruik van het systeem voor nummerdoorgifte een niet-toegekend nummer wordt weergegeven (zoals een telefoonnummer), of het nummer van iemand anders getoond wordt dan het nummer van de beller/afzender in het adresveld van een oproep of bericht.

[1] Kamerstuk 35 570 VI, nr. 52

kst-29911-314
ISSN 0921 - 7371
's-Gravenhage 2021

Oplichters maken misbruik van het vertrouwen van degene met wie zij contact opnemen, omdat zij het doen voorkomen alsof zij bellen vanaf het telefoonnummer van een ander.
Bij bankhelpdeskfraude doet een crimineel zich voor als een medewerker van de bank van het slachtoffer. De crimineel misbruikt hiervoor de naam en/of het telefoonnummer van de bank en haalt het slachtoffer over om een betaling te doen naar een zogenaamd veilige rekening van zijn of haar bank.
In de brief van 20 februari 2020[2] heb ik mede namens de Staatssecretaris van Economische Zaken en Klimaat de stand van zaken geschetst omtrent de ontwikkelingen van niet-bancaire fraude door middel van phishing en de aanpak ervan door publieke en private partijen, waaronder door telecomaanbieders.

Phishing is een overkoepelende term voor vormen van (financiële) fraude waarbij gegevens van een gebruiker onrechtmatig op afstand worden verkregen. Phishing kan plaatsvinden door misleidende informatie over de afzender op te nemen in de inhoud van de communicatie. Hierbij worden verschillende kanalen ingezet, waaronder telefonie, sms (waarbij ook alfanumerieke tekens worden gebruikt als afzenderinformatie), e-mail en internetcommunicatietoepassingen zoals Whatsapp en berichtendiensten die worden gebruikt bij online marktplaatsen. Niet-bancaire fraude omvat diverse vormen van oplichting, waaronder fraude met betaalmiddelen door middel van phishing en spoofing. Soms vragen criminelen aan hun slachtoffers om pincodes en beveiligingscodes of om direct toegang tot hun computer te geven, waardoor oplichters malware kunnen installeren.

Deze vormen van oplichting raken zowel burgers als het bedrijfsleven, veroorzaken grote (vervolg)schade en dit kan ook het vertrouwen in het betalingsverkeer en de veiligheid op het internet ondermijnen. Het is aan de overheid om dit vertrouwen te waarborgen en hierbij in het bijzonder op te komen voor kwetsbare groepen zoals ouderen, jeugdigen, laaggeletterden en het midden- en kleinbedrijf.

Een significant effect bij fraudebestrijding is te verwachten van bewustwording, preventie, interventies en barrières en het bieden van een duidelijk handelingsperspectief aan (potentiële) slachtoffers. Ook het bieden van duidelijkheid aan slachtoffers over de mogelijkheden hoe zij geleden schade kunnen verhalen is belangrijk. Voor de fraudebestrijding is het evenwel noodzakelijk om ook te investeren aan de voorkant, dat wil zeggen in het voorkomen van slachtofferschap. Het stimuleren en voorlichten over veilig internetgedrag, het vergroten van de bewustwording van mogelijke risico's alsook het opwerpen van barrières om de impact van fraude te beperken, zijn daarom onderdeel van het uitgevoerde beleid. Dit beleid wordt versterkt met publiek-private samenwerking in een integrale aanpak. Voor het treffen van effectieve maatregelen is het wenselijk om de handen ineen te slaan met onder meer de telecom- en internetproviders, social media platforms, banken en betaalinstellingen, omdat de maatregelen die getroffen of uitgevoerd zouden kunnen worden, ook buiten het beleidsterrein van Justitie en Veiligheid vallen.

## De inzet van het strafrecht

Het belang van preventie en samenwerking wordt versterkt door de stijging van het aantal aangiften van onlinecriminaliteit. Uit het Jaarbe-

[2] Kamerstuk 29 911, nr. 273

richt 2020[3] van het Openbaar Ministerie (OM) is dit ook zichtbaar in de cijfers. Het aantal verdachten van fraude met betaalproducten nam toe met 48%, van 450 naar 680 verdachten en het aantal verdachten van fraude met online handel met 16%: van 285 naar 330. Ten slotte nam het aantal verdachten van identiteitsfraude toe met 20%; van 120 naar 140.

Aangiften met betrekking tot gebruik van spoofing worden niet als zodanig afzonderlijk geregistreerd, omdat het niet altijd mogelijk is om de methode van fraude vast te stellen. Zulk soort zaken worden onder één van de hiervoor genoemde fraudevormen (classificaties) opgenomen. Daarnaast zijn de methoden die criminelen gebruiken veelvoudig en veranderen ze snel. Voor afpakresultaten geldt ook dat deze niet specifiek voor spoofing worden bijgehouden. Het is daarom niet preciezer aan te geven wat het kwantitatieve of financiële resultaat is.
Als slachtoffers ook de stap zetten om daadwerkelijk aangifte te doen, zijn de verwachtingen van de opsporing hoog. Niet elke aangifte biedt echter genoeg aanknopingspunten voor een opsporingsonderzoek. Zoals bij elk opsporingsonderzoek bepaalt het OM op basis van een aantal factoren een prioritering. Het strafrecht wordt binnen de integrale publiek-private aanpak van fraude ingezet voor die zaken waarbij het strafrecht effectief is. Het gaat dan bijvoorbeeld om zaken met grote maatschappelijke schade, een ondermijnend karakter, stelselmatige daders of kwetsbare slachtoffers.
Bij de opsporing van daders spelen praktische belemmeringen. Kenmerk van gedigitaliseerde fraude is dat het vluchtig én snel opschaalbaar is. Daders opereren in veel gevallen anoniem en vanuit het buitenland en slaan in korte tijd hun slag. Het geld verdwijnt vervolgens naar het buitenland. Dit vraagt om intensieve inspanningen terwijl de slagingskans klein is. Daarom wordt ook in Europees verband aandacht gevraagd voor Europese samenwerking in de fraudebestrijding. Een goede kennispositie en zicht op de veranderingen van (modus operandi van) criminelen zijn nodig voor de aanpak. Uitwisseling van informatie tussen lidstaten en dreigingsbeelden van Europol zijn daarvoor nuttig.
Ook investeren we in snellere informatie uitwisseling tussen banken en opsporingsdiensten door middel van bijvoorbeeld het verwijzingsportaal bankgegevens. Via dit portaal kunnen sinds vorig jaar identificerende bankgegevens geautomatiseerd worden opgevraagd. Er wordt nu gewerkt aan een doorontwikkeling van het portaal waarbij ook saldo- en transactiegegevens geautomatiseerd kunnen worden opgevraagd.

## De inzet van de telecomsector

De integriteit van telecommunicatievoorzieningen, waaronder het gebruik van nummers, speelt een belangrijke rol bij het voorkomen van phishing en spoofing. De telecomsector heeft in samenspraak met de financiële sector, Belastingdienst, ACM en politie medio 2020 middels een gecoördineerd plan van aanpak maatregelen in kaart gebracht. De maatregelen die de telecomsector tot dusverre heeft genomen zijn grotendeels ingevoerd sinds het najaar van 2020 en zijn door de Staatssecretaris van EZK eerder toegelicht[4]. De telecomsector en ACM geven aan dat de eerste resultaten reeds zijn geboekt met het reduceren van telefoniespoofing, met name spoofing van telefoonnummers van banken. Dit verkeer komt binnen via internationale routes. De telecomaanbieders en banken nemen maatregelen bij het signaleren van een telefoonnummer van een bank die mogelijk wordt gespoofd. Daarnaast blokkeren telecomaanbieders frequent simkaarten die gebruikt worden voor phishing via sms, ofwel smishing.

[3] Kamerstuk 28 844, nr. 229
[4] Kamerstuk 29 911, nr. 302

Zoals in het Commissiedebat Telecommunicatie van 20 mei jl. aan de orde kwam (Kamerstuk 24 905, nr. 542), is het voor bepaalde maatregelen nog onduidelijk wat de sector kan en mag doen binnen het wettelijk kader voor de bescherming van privacy en de zorgplicht die in dit verband rust op telecomaanbieders om de privacy van hun gebruikers te beschermen door maatregelen ter beveiliging van hun netwerken en diensten. Dit geldt met name voor het inzetten van technieken om phishing te detecteren. Naar verwachting komt de ACM na de zomer van 2021 met een visie over wat telecomaanbieders binnen deze kaders kunnen en/of moeten doen.

Het totaalbeeld is dat het effect van de betreffende maatregelen op korte termijn voor spoofing en smishing positief is. Echter, voor het vergroten van de effectiviteit is van belang dat de genoemde samenwerking verder wordt geïntensiveerd ten behoeve van het toezicht op de naleving van de telecomregelgeving. Daarbij is ook de opvolging van door telecomaanbieders en banken gemeld phishing verkeer belangrijk. Er worden regelmatig frauduleuze websites met hulp van banken geblokkeerd.

Het voorstel tot aanpassing van de Telecommunicatiewet, met aanvullende maatregelen tegen phishing, onder meer door een effectievere werking van het spoofing verbod, wordt thans door de Staatssecretaris van EZK voorbereid. De regels voor nummerdoorgifte (de afzenderinformatie van een oproep of bericht) zullen daarbij worden aangepast en ook zal het gebruik van alfanumerieke informatie worden betrokken door hieraan passende voorwaarden te verbinden. Het wetsvoorstel omvat voorts een beperking van het extraterritoriale gebruik van nummers uit het nummerplan. Bij de regels voor nummerdoorgifte zullen concrete verplichtingen bij telecomaanbieders worden gelegd, en zal nadrukkelijk ook de rol van de aanbieder van de telecomdienst van waaruit de oproep plaatsvindt of het bericht wordt gestuurd, worden geadresseerd. Met deze aanpassing zal worden aangesloten bij Europees beleid. Met lagere regelgeving zullen een aantal onderdelen van de wet nader moeten worden ingevuld. De Staatssecretaris van EZK zal naar verwachting een voorontwerp van wetswijziging in het derde kwartaal van 2021 voor consultatie aanbieden.

## Schadecompensatie door banken

In december heeft de Minister van Financiën uw Kamer geïnformeerd over het uniforme coulancekader dat de banken gezamenlijk hebben opgesteld om te bepalen wanneer een slachtoffer van spoofing in de vorm van bankhelpdeskfraude in aanmerking komt voor compensatie[5]. Slachtoffers komen in aanmerking voor schadevergoeding als er sprake is van misbruik van de naam en/of het telefoonnummer van de eigen bank, als het een niet-zakelijke klant betreft en als er door het slachtoffer aangifte bij de politie is gedaan. In aanvulling hierop hebben de banken recent een toetsingskader gepubliceerd dat duidelijk maakt wanneer slachtoffers niet in aanmerking komen voor compensatie.[6] Hierbij is het uitgangspunt dat slachtoffers 100% van de schade uit coulance vergoed krijgen tenzij het slachtoffer medeplichtig is aan fraude, al eerder een vergoeding heeft gehad bij dezelfde bank of als het slachtoffer onvoldoende meewerkt aan het fraudeonderzoek van de bank. Ook verwachten de banken een redelijk en billijk niveau van oplettendheid van de klant. Het staat individuele banken vrij om hier ruimhartiger mee om te gaan. In zijn gesprekken met de banken heeft de Minister van Financiën begrip gevraagd voor de moeilijke situatie waarin de slachtoffers door fraudeurs worden gebracht. De banken onderkennen dit ook. Het coulancekader

[5] Kamerstuk 32 545, nr. 128

[6] https://www.nvb.nl/nieuws/toetsingscriteria-voor-coulance-bij-bankhelpdesk-fraude-spoofing/

wordt door de banken met terugwerkende kracht vanaf 1 januari 2020 toegepast. De banken hebben aangegeven dat alle gevallen van spoofing in de vorm van helpdeskfraude uit 2020 inmiddels behandeld zijn en dat in 96% van de gevallen overgegaan is tot schadevergoeding uit coulance.

## Verkenning wettelijke schadevergoeding spoofing

Zoals toegezegd in het debat van 10 november 2020[7] heeft de Minister van Financiën uitgezocht wat nodig zou zijn om met wetgeving slachtoffers van spoofing tegemoet te komen. Uit de verkenning blijkt dat twee aspecten een eventueel wettelijk verankerde vergoedingsplicht voor spoofingfraude ingewikkeld maken. Bij spoofingfraude is van belang dat slachtoffers snel vergoed worden vanwege de impact die dit heeft op hun leven. In de eerste plaats zou een wetswijziging introduceren tijd in beslag nemen waardoor het langer zou duren voordat slachtoffers zekerheid hebben wanneer zij recht hebben op een vergoeding in vergelijking met het coulancekader dat momenteel is opgezet door de banken. In de tweede plaats speelt mee dat in de toekomst op een andere manier fraude kan worden gepleegd dan momenteel het geval is, waardoor een wettelijk vergoedingskader wellicht al verouderd is op het moment dat een wettelijke bepaling van kracht is.
Nu de banken voortvarend een coulancekader hebben vastgesteld en hiermee positieve resultaten lijken te behalen, acht de Minister van Financiën het van belang om te bezien of dit kader ook over een langere periode een effectieve manier is om slachtoffers van spoofing in de vorm van bankhelpdeskfraude te compenseren.

## Integrale aanpak

De complexiteit en de opschaalbaarheid van digitale fraude leveren grote maatschappelijke en financiële schade op. Voor een effectieve aanpak is een brede en integrale aanpak nodig. De overheid en het bedrijfsleven participeren daarom al in diverse samenwerkingsverbanden met het oog op de preventie, interventie en bestrijding van online criminaliteit, bijvoorbeeld het Convenant «Eerst checken dan klikken». Voor de overheid zijn private partijen belangrijke en aantrekkelijke partners. Zij beschikken over specifieke expertise en technologische kennis van hun infrastructuur en dit geeft de samenwerking potentieel grote slagkracht. Omgekeerd is de overheid c.q. de wetgever voor private partijen een belangrijke gesprekspartner als het gaat om het wegnemen van ervaren belemmeringen die bijvoorbeeld informatiedeling ten behoeve van fraudebestrijding bemoeilijken. Zij verlangen van de overheid dat het de kaders aangeeft en verduidelijkt, zodat duidelijk is wat met het oog op preventie en voor de fraudebestrijding mogelijk is en van hen wordt verlangd.

Door de Ministeries is met de Nederlandse Vereniging van Banken (NVB), de Betaalvereniging Nederland (BVN) en de Vereniging van telecomaanbieders (COIN) het initiatief genomen om ter aanvulling van het ingezette beleid samen te werken in gerichte acties en de integrale aanpak effectief vorm te geven. Momenteel bezien we welke aanvullende acties nodig zijn en met welke partijen, ook voor wat betreft internettoepassingen. We willen bijvoorbeeld ook bezien of en hoe we met de verschillende voorlichtingsactiviteiten vanuit de overheidspartijen en bijvoorbeeld banken, telecomaanbieders en social media bedrijven de communicatieboodschap specifiek gericht op preventie van online fraudevormen en internet- en betaalveiligheid kunnen versterken. Hierover zullen wij uw Kamer informeren.

---

[7] Handelingen II 2020/21, nr. 22, item 2

## Slot

In deze brief heb ik u mede namens de Minister van Financiën en Staatssecretaris van Economische Zaken en Klimaat toegelicht welke inspanningen zijn geleverd om bankhelpdeskfraude/spoofing aan te pakken en dat we dit beleid zullen voortzetten. Ook heb ik toegelicht dat we in overleg met private partijen invulling willen geven aan de integrale aanpak. Zoals opgemerkt, zullen wij uw Kamer opnieuw informeren.
Als beleidsverantwoordelijke bewindspersonen zien we- in aanvulling op bestaande trajecten en operationele samenwerking- de meerwaarde van publiek-private samenwerking op het strategisch niveau waardoor beleid en acties in het publieke domein en in het private speelveld op elkaar zijn af te stemmen. Deze aanpak vergt inspanning en samenwerking over de verschillende beleidsdomeinen heen. Wij zijn verheugd met de constructieve inbreng en bereidheid tot samenwerking van banken, telecomaanbieders en andere betrokken partijen om in de integrale aanpak te participeren.
Ik zie het als mijn rol om de benodigde partijen samen te brengen en op bestuurlijk niveau te bevorderen dat ieders inspanning op het gebied van preventie en bestrijding in samenhang effectief zullen zijn.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus