Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2020–2021

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1075

Vragen van de leden **Van Nispen** en **Alkaya** (beiden SP) aan de Ministers van Justitie en Veiligheid en van Financiën over *schadevergoedingen door banken bij spoofing* (ingezonden 11 november 2020).

Antwoord van Minister **Hoekstra** (Financiën), mede namens de Minister van Justitie en Veiligheid (ontvangen 11 december 2020). Zie ook Aanhangsel Handelingen, vergaderjaar 2020–2021, nr. 959.

Vraag 1
Heeft u kennisgenomen van de uitzending van Radar, meer specifiek het onderwerp spoofing en de schade die dit soort criminaliteit voor slachtoffers veroorzaakt?[1]

Antwoord 1
Ja.

Vraag 2, 3
Deelt u de mening dat banken bij spoofing slachtoffers moeten compenseren, net zoals bij phishing reeds wettelijk verplicht is? Zo nee, waarom niet? Deelt u de mening dat het enige argument voor banken om wel of niet over te gaan tot compensatie zou moeten zijn of er sprake is van grove nalatigheid bij het slachtoffer? Deelt u de mening dat door de aard van spoofing (zeer geraffineerd en bouwend op het vertrouwen dat mensen in banken hebben) het niet eerlijk is van banken om te stellen dat een slachtoffer per definitie grof nalatig is geweest door zelf geld over te maken? Zo nee, waarom niet?

Antwoord 2, 3
In het Burgerlijk Wetboek is vastgelegd dat banken voor bepaalde soorten fraude wettelijk verplicht zijn om schade te vergoeden.[2] Daarbij gaat het om zogenoemde bancaire fraude: fraude waarbij er sprake is van misbruik van betaalmogelijkheden die de bank aan klanten ter beschikking stelt. Hierbij geldt dat een bank schade niet hoeft te vergoeden als er sprake is van grove nalatigheid door de klant. Om meer duiding te geven aan het begrip «grove nalatigheid», hebben de banken en de Consumentenbond in 2014 een vijftal

[1] Radar, 9 november 2020, «Tientallen miljoenen euro's schade door bankfraude, wanneer krijg je compensatie?», https://radar.avrotros.nl/uitzendingen/gemist/item/tientallen-miljoenen-euros-schade-door-bankfraude-wanneer-krijg-je-compensatie/

[2] Artikel 7:528 en 7:529 BW.

ah-tk-20202021-1075
ISSN 0921 - 7398
's-Gravenhage 2020

uniforme veiligheidsregels opgesteld[3]. Wanneer aan deze vijf veiligheidsregels is voldaan, kan de klant erop rekenen dat zij de schade vergoed krijgt. *Phishing* [4] valt niet onder het begrip bancaire fraude. Banken zijn niet bij wet verplicht om schade te vergoeden als de klant de transactie zelf geïnitieerd heeft (de zogenaamde niet-bancaire fraude), zoals het geval is bij *spoofing* [5] en in sommige gevallen van phishing. Bij phishing hebben de banken besloten schade in de meeste gevallen wel te vergoeden uit coulance, aangezien er bij veel phishinggevallen geen sprake is van grove nalatigheid op basis van de uniforme veiligheidsregels.
Het wordt voor consumenten steeds lastiger om spoofing en hulpvraagfraude via bijvoorbeeld WhatsApp te detecteren. In sommige gevallen is sprake van zeer grote schade. Banken hanteren een verschillend coulancebeleid, wat leidt tot onbegrip en onduidelijkheid over wanneer er wel en niet vergoed wordt. Daarom ben ik, zoals ik ook heb toegezegd in het mondelinge vragenuur van 10 november 2020, in samenspraak met de Minister van Justitie en Veiligheid[6] met de banken in gesprek over de compensatie van slachtoffers bij niet-bancaire fraude. Daarnaast verken ik parallel hieraan of aanpassing van wetgeving op dit gebied wenselijk en mogelijk is. Ik informeer uw Kamer in het eerste kwartaal van 2021 over de voortgang op beide punten.

Vraag 4, 7
Vindt u dat de voorlichting van banken op orde is op het gebied van spoofing? Vindt u dat banken er voldoende aan doen om spoofing te voorkomen? Zo ja, waarom?
Zou een deel van het probleem van spoofing voorkomen kunnen worden als het ophogen van het maximale betalingsbedrag niet meteen geregeld kan worden, maar dat er voor de veiligheid een aantal uren zit tussen de aanvraag en de daadwerkelijke ophoging? Zou het ook helpen wanneer de bank ook bij elke handeling om het betalingsbedrag te verhogen een spoofing-waarschuwing laat zien? Zo ja, bent u bereid banken tot deze maatregelen te verplichten dan wel aan te sporen?

Antwoord 4, 7
Het voorkomen van slachtoffers door goede voorlichting over spoofing en andere vormen van online fraude is van groot belang. Er wordt op dit vlak, onder meer door de banken, al veel ondernomen. Vrijwel alle banken besteden aandacht aan verschillende vormen van fraude via hun websites, social media en nieuwsbrieven. Ook hebben de Nederlandse Vereniging van Banken en de Betaalvereniging Nederland een website, www.veiligbankieren.nl, waar zij voorlichting geven over verschillende vormen van fraude en zijn er campagnes geweest om klanten te waarschuwen voor online fraude. Daarnaast is er sinds een aantal jaar de campagne «hang op, klik weg, en bel uw bank» die regelmatig plaatsvindt om het algemene publiek te informeren via radio, televisie en andere media. De Minister van Justitie en Veiligheid heeft afgelopen september in samenwerking met veel private en publieke partijen, waaronder de banken, de campagne «Senioren en veiligheid» uitgevoerd. In deze campagne is onder andere aandacht besteed aan phishing en hulpvraagfraude. Er wordt momenteel gewerkt aan een vervolg van deze campagne, waarbij aandacht wordt besteed aan spoofing. Tenslotte is er ook op de website van de Fraudehelpdesk veel informatie te vinden.
Tegelijkertijd zie ik ook dat er de laatste maanden steeds meer mensen slachtoffer zijn geworden van deze vorm (en andere vormen) van fraude. Dit komt doordat de door criminelen gebruikte methoden steeds geraffineerder worden. Zowel het inbouwen van een vertraging bij het ophogen van het maximale betalingsbedrag als het laten zien van een spoofing-waarschuwing kan helpen bij het voorkomen van spoofing. Er is ook al een aantal banken dat deze maatregelen implementeert. Echter, alleen deze maatregelen zullen het probleem niet oplossen. Het is belangrijk om een integrale aanpak te

---

[3] Te raadplegen via: https://www.consumentenbond.nl/betaalrekening/bankvoorwaarden.
[4] Phishing is een vorm van internetfraude waarbij internetcriminelen proberen persoonlijke gegevens of wachtwoorden te onttrekken, bijvoorbeeld door slachtoffers naar een valse website te sturen.
[5] Er is sprake van spoofing wanneer de crimineel een andere identiteit aanneemt, bijvoorbeeld die van de bank, en op die manier het slachtoffer oplicht.
[6] Mede naar aanleiding van de motie van het lid Van Nispen. Kamerstuk 35 570-VI, nr. 52.

hanteren. Samen met de Minister van Justitie en Veiligheid onderzoek ik hoe we de samenwerking met banken op het gebied van fraudebestrijding, waaronder voorlichting en dit soort barrière-verhogende maatregelen, verder kunnen vormgeven en hoe we die fraudebestrijding nog meer kunnen versterken. Ook is de Staatssecretaris van Economische Zaken en Klimaat in gesprek met de telecomsector over de aanpak van phishing en spoofing. Naar verwachting stuurt zij voor eind december een brief hierover aan uw Kamer.

Vraag 5
Hoe verklaart u dat het nu voor de politie zo lastig is om de criminelen die dit soort fraude plegen op te sporen en dus het geld van de slachtoffers te achterhalen? Is dit technologisch onmogelijk of heeft het te maken met een gebrek aan opsporingscapaciteit? Wat gaat u er aan doen om nog meer geld dat via spoofing is verdwenen op te sporen en af te pakken?

Antwoord 5
Criminaliteit digitaliseert in toenemende mate. Gedigitaliseerde criminaliteit is zeer dynamisch en kent vaak een internationale dimensie. Het is snel schaalbaar en er kunnen dus veel slachtoffers worden gemaakt, zoals bijvoorbeeld het geval is bij fraude door middel van spoofing. Daarnaast heeft de crimineel verschillende mogelijkheden om zijn of haar identiteit af te schermen, wat de opsporing bemoeilijkt. Voor de effectieve bestrijding van deze vorm van criminaliteit is inzicht in het fenomeen en overzicht ten aanzien van de omvang en impact noodzakelijk. Daarnaast vereisen deze gedigitaliseerde vormen van criminaliteit een combinatie van onder andere digitale expertise en financiële expertise.
De politie is actief bezig om met onder meer het Openbaar Ministerie, banken en de telecomsector om meer effectieve interventiestrategieën te ontwikkelen om deze vormen van criminaliteit tegen te gaan, te verstoren en aan te pakken.
Preventie blijft zeer belangrijk. Politie en het OM delen daarom signalen van modus operandi van fraude met partijen die in staat zijn preventieve maatregelen te nemen, zoals banken, telecommunicatiebedrijven en departementen en informeren ook zelf de samenleving over de gevaren van bepaalde fraudevormen.

Vraag 6
Welke concrete juridische en/of praktische belemmeringen zijn er nu om frauduleuze geldstromen te volgen en, in het verlengde daarvan, crimineel verkregen vermogen op te sporen en af te pakken? Hoe denkt u die belemmeringen weg te nemen?

Antwoord 6
Zoals hiervoor vermeld is gedigitaliseerde criminaliteit dynamisch en vaak internationaal. Het vermogen dat door criminelen wordt buit gemaakt, wordt veelal via zogenaamde «geldezels» weggesluisd. Door de snelheid van het betalingsverkeer kunnen bedragen die van de slachtofferrekening worden overgemaakt naar een «geldezel» of naar een buitenlandse rekening worden doorgesluisd en/of nagenoeg direct contant worden opgenomen. Het volgen van de geldstroom wordt hierdoor bemoeilijkt. Het is daarom niet alleen belangrijk om in te zetten op de geldstromen, maar ook op het eerder interveniëren in het proces. Banken kunnen hierbij een belangrijke rol spelen aangezien zij bijvoorbeeld via fraudedetectiesystemen zicht hebben op die geldstromen.
Zoals de Minister van Justitie en Veiligheid op 17 november jl. aan uw Kamer heeft gemeld[7], hebben politie en banken een aantal projecten ingericht om hun samenwerking te versterken. Eén van die projecten richt zich op een betere detectie van «geldezels» en het bewustmaken van doelgroepen om te voorkomen dat iemand «geldezel» wordt. Daarnaast wordt gekeken naar de versterking van de gegevensdeling tussen politie en banken. De Minister van Justitie en Veiligheid heeft tijdens de begrotingsbehandeling aangegeven met banken en politie te gaan onderzoeken wat er op het terrein van de gezamen-

[7] Kamerstuk 28 684, nr. 638

lijke gegevensverwerking voor de aanpak van internetoplichting noodzakelijk is om effectief te kunnen opereren en wat onder de bestaande wetgeving de knelpunten zijn die een effectieve aanpak in de weg staan[8].

Vraag 8
Bent u bereid, nu u heeft toegezegd de juridische mogelijkheden te onderzoeken om banken te dwingen de schade van slachtoffers van spoofing te compenseren, op zo kort mogelijke termijn de verschillende juridische mogelijkheden om dit doel te bereiken in kaart te brengen? Wanneer kan de Kamer hier over geïnformeerd worden?

Antwoord 8
Zoals ik eerder in het mondelinge vragenuur heb gezegd, heeft het mijn voorkeur om afspraken te maken met de banken over de compensatie van slachtoffers bij niet-bancaire fraude. Een van de redenen hiervoor is dat het wijzigen van de wet gepaard gaat met een lange doorlooptijd. Bovendien kan er op die manier makkelijker ingespeeld worden op de actualiteit. Desalniettemin heb ik bij het vragenuur toegezegd om, parallel aan het maken van afspraken met de banken, een juridische verkenning te doen. Ik informeer uw Kamer hierover in het eerste kwartaal van 2021.

[8] Kamerstuk 33 570 VI