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

438

Vragen van de leden **Van der Linde** en **Yeşilgöz-Zegerius** (beiden VVD) aan de Ministers van Financiën en van Justitie en Veiligheid over *het bericht «WhatsApp-fraude explodeert: «Ik snap niet hoe ik erin ben getrapt»»* (ingezonden 3 september 2020).

Antwoord van Minister **Grapperhaus** (Justitie en Veiligheid), mede namens de Minister van Financiën (ontvangen 13 oktober 2020).

Vraag 1
Bent u bekend met het artikel «WhatsApp-fraude explodeert: «Ik snap niet hoe ik erin ben getrapt»»?[1]

Antwoord 1
Ja.

Vraag 2
Kunt u aangeven wat de omvang van dit probleem is? Zo ja, in hoeveel gevallen wordt er aangifte gedaan of melding gemaakt door slachtoffers en in hoeveel gevallen niet? Zo nee, zijn er redenen bekend waarom niet?

Antwoord 2
De exacte omvang van hulpvraagfraude (ook wel vriend-in-nood-fraude genoemd), is niet bekend, omdat niet alle slachtoffers aangifte doen bij de politie of een melding maken bij hun bank of de Fraudehelpdesk (FHD). Hoewel de exacte omvang niet bekend is kan wel geconcludeerd worden dat er sprake is van een stijging sinds 2019 van het aantal meldingen en aangiftes van deze vorm van fraude.
Bij de FHD zijn tot 1 augustus 2020 7.907 meldingen binnengekomen van hulpvraagfraude. In heel 2019 waren dat er 2.663. Ook de Nederlandse Vereniging van Banken (NVB) meldt dat Nederlandse banken in de maanden maart, april en mei van dit jaar drie keer zoveel meldingen van oplichting via social media hebben ontvangen ten opzichte van de laatste drie maanden van 2019. Het aantal aangiftes bij de politie lag voor de coronacrisis op circa 120 tot 150 aangiftes per week. Sinds april van dit jaar is het mogelijk om digitaal aangifte te doen bij de politie en kwamen tot augustus circa 700 aangiftes per

[1] De Telegraaf, 2 september 2020, https://www.telegraaf.nl/nieuws/1231123395/whats-app-fraude-explodeert-ik-snap-niet-hoe-ik-erin-ben-getrapt.

ah-tk-20202021-438
ISSN 0921 - 7398
's-Gravenhage 2020

week binnen. De politie wijdt de toename van de aangiftes van hulpvraagfraude deels aan het feit dat het makkelijker is om melding te doen, maar ook aan de feitelijke toename van deze vorm van fraude. De feitelijke toename kan volgens de politie mogelijk verklaard worden doordat mensen tijdens de Corona-crisis meer online zijn gegaan om contact te hebben met hun familie en bekenden. Sinds augustus is het aantal aangiftes iets afgenomen.

Vraag 3
In hoeveel gevallen van aangifte of melding wordt er ook daadwerkelijk vervolgd? In hoeveel gevallen wordt er na vervolging een straf opgelegd? Kan een overzicht worden gegeven van het aantal opgelegde straffen naar soort? Zo nee, waarom niet?

Antwoord 3
Hoeveel aangiftes of meldingen hebben geleid tot een vervolging is niet inzichtelijk. Het OM registreert hulpvraagfraude via bijvoorbeeld WhatsApp niet apart. Er worden voor het begaan van hulpvraagfraude soms forse straffen opgelegd. Zo hebben twee mannen uit Deventer die mensen via WhatsApp hebben opgelicht een celstraf van 2,5 jaar en 3 jaar opgelegd gekregen.[2]

Vraag 4
Heeft u zicht op het daderprofiel? Zo ja, wat is kenmerkend voor dit profiel? Hoe zit dit aan de slachtofferkant? Zo nee, wat wordt er concreet gedaan om deze profielen in beeld te krijgen?

Antwoord 4
Bij hulpvraagfraude gaat het in de meeste gevallen om een georganiseerde samenwerking van verschillende daders en medeplichtigen: katvangers/geldezels[3], katvanger-ronselaars, pinners, oplichters, hackers en verkopers van de benodigde kennis[4]. De politie heeft het beste zicht op de katvangers/geldezels, die ook de grootste groep daders vormen. Dit zijn vaak jongeren en/of personen met een sociaaleconomisch zwakkere positie. De politie onderzoekt op verschillende manieren de verschillende dadertypes en de mogelijke (persoonsgerichte)barrières om deze vorm van fraude tegen te gaan.
De politie, FHD, Slachtofferhulp Nederland (SHN) en NVB hebben het beeld dat de meeste slachtoffers ouder zijn dan vijftig jaar. Het is op basis van de informatie van de politie, FHD en SHN niet met zekerheid te stellen dat vijftigplussers ook een hoger risico lopen op slachtofferschap.

Vraag 5
Onder welke voorwaarden staan banken garant bij dit soort vormen van financiële criminaliteit? In hoeveel gevallen hebben slachtoffers tot nu toe hun geld teruggekregen? In hoeveel gevallen gebeurt dit niet?

Antwoord 5
In principe staan banken niet garant voor dit soort vormen van financiële criminaliteit. Wel zijn banken voor bepaalde soorten bancaire fraude wettelijk verplicht[5] om schade te vergoeden. Bij bancaire fraude is er sprake van misbruik van betaalmogelijkheden die de bank aan klanten ter beschikking stelt. Hierbij geldt dat over het algemeen overgegaan wordt tot schadevergoeding wanneer de klant niet grof nalatig is geweest. Of er sprake is van grove nalatigheid is afhankelijk van het individuele geval en wordt uiteindelijk bepaald door de rechter. Wel hebben de banken gezamenlijk met de Consumentenbond een vijftal uniforme veiligheidsregels opgesteld die meer duidelijkheid geven over de vergoeding van schade als gevolg van fraude[6]; houd je beveiligingscodes geheim, zorg ervoor dat je bankpas nooit door een

[2] https://nos.nl/artikel/2347654-gevangenisstraf-voor-whatsapp-fraudeurs.html
[3] Katvangers/geldezelseze stellen bewust dan wel onbewust hun bankrekening ter beschikking voor frauduleuze transacties met als tegenpresentatie een gedeelte van de frauduleuze opbrengst.
[4] Ook wel genaamd; cybercrime – as- a-service
[5] Volgens artikel 7:528 en 7:529 van het Burgerlijke Wetboek
[6] Te raadplegen via: https://www.consumentenbond.nl/betaalrekening/bankvoorwaarden

ander gebruikt wordt, zorg voor een goede beveiliging van de apparatuur die je gebruikt voor je bankzaken, controleer je bankrekening, en meld incidenten direct aan de bank en volg aanwijzingen van de bank op. Wanneer aan deze vijf veiligheidsregels is voldaan, kan de klant erop rekenen dat de schade vergoed wordt.
Banken zijn niet verplicht om schade te vergoeden als er sprake is van niet-bancaire fraude. Bij niet-bancaire fraude is sprake van een slachtoffer die onbewust of onder valse voorwendsels zelf opdracht geeft voor de uitvoering van de betaling aan de fraudeur.
Wanneer een klant zelf een betaalopdracht initieert, zoals het geval is bij hulpvraagfraude via WhatsApp, dan is de bank verplicht deze uit te voeren. Dit is alleen anders als de bank vermoedt dat er sprake is van fraude, bijvoorbeeld omdat de fraudedetectiesystemen aanleiding geven tot twijfel (in antwoord 6 en 8 wordt toegelicht wat banken verder doen ter voorkoming van fraude). Het is echter voor banken lastig om te zien of er sprake is van fraude als de klant zelf de betaalopdracht geeft.
Het kan dat in bepaalde gevallen van niet-bancaire fraude banken uit coulance overgaan tot een vergoeding. Dit is een eigen overweging van de bank op basis van de omstandigheden van het geval. Omdat dit gaat over een eigen overweging van de bank heb ik hierover geen cijfers tot mijn beschikking.

Vraag 6, 8
Op welke manieren proberen banken deze vorm van criminaliteit te voorkomen? Wat doen banken concreet om slachtoffers te waarschuwen en naderhand te adviseren?
Wat kunnen banken doen om deze vorm van criminaliteit te voorkomen? Is het mogelijk dat er een telefoontje vanuit de bank ter controle van de overboeking naar ouderen wordt gepleegd met de vraag of zij zeker zijn van deze overboeking?

Antwoord 6, 8
De NVB en Betaalvereniging Nederland hebben aangegeven dat zij verschillende initiatieven ondernemen ter preventie van fraude, zoals het voorlichten van klanten om hen bewust te maken van potentiële frauderisico's. Dit gebeurt onder andere via veiligbankieren.nl en via de eigen kanalen van de banken. Ook werken banken bij voorlichting samen met andere organisaties, waaronder de ouderenbonden. In september hebben de banken bijvoorbeeld bijgedragen aan de campagne «Senioren en Veiligheid» waarin onder andere aandacht werd besteed aan hulpvraagfraude via WhatsApp[7].
Verder hebben de banken ter voorkoming van fraude de IBAN-naam check ingevoerd. Bij deze check krijgen klanten een melding als de naam en het rekeningnummer die de klant invoert niet in overeenstemming zijn met de gegevens die bekend zijn bij de bank.
Daarnaast werken de banken met verschillende fraudedetectiesystemen om frauduleuze transacties op te sporen en te onderzoeken. De monitoring vindt plaats op basis van vele indicatoren. In samenwerking met de politie wordt op basis van bepaalde modus operandi gekeken welke indicatoren gehanteerd kunnen worden om de fraudedetectiesystemen verder te verbeteren. Omwille van veiligheid kunnen banken hier verder geen toelichting op geven. Wanneer een mogelijk frauduleuze transactie gedetecteerd wordt door het fraudedetectiesysteem, wordt de transactie apart gezet en onderzocht door een medewerker van de bank, waarbij vrijwel altijd contact gezocht wordt met de klant. Met deze fraudedetectiesystemen kunnen banken dus tijdig fraude signaleren en klanten hiervoor waarschuwen. Gezien de grote aantallen overboekingen die dagelijks worden uitgevoerd is het ondoenlijk om ter controle een telefoontje te plegen naar elke klant. Daarnaast dient rekening te worden gehouden met de privacy van de klant.

[7] https://www.alertonline.nl/agenda/senioren-en-veiligheid.

Vraag 7, 10, 11
Gegeven het stijgende aantal slachtoffers en de enorme economische impact, deelt u de mening dat er meer moet worden gedaan om dit soort fraude tegen te gaan? Zo ja, welke maatregelen bent u bereid te treffen en hierbij de fraudehelpdesk, politie en banken te betrekken?
Welke mogelijkheden zijn er om slachtoffers preventief te waarschuwen? Hoe vaak is er daadwerkelijk gehandeld naar deze mogelijkheden?
Wat gaat u doen om deze nieuwe, schadelijke vorm van financiële criminaliteit te voorkomen?

Antwoord 7, 10, 11
Vanwege het stijgende aantal slachtoffers sinds de corona crisis is mijn ministerie snel overgegaan tot voorlichting van het publiek. De meest effectieve aanpak van fraude is namelijk het voorkomen dat mensen slachtoffer worden. Mijn ministerie betrekt hierbij o.a. de politie, de banken, fraudehelpdesk en andere private organisaties. Zo publiceerde het jongerenplatform scholieren.com in samenwerking met het Centrum voor Criminaliteitspreventie en Veiligheid (CCV) en mijn ministerie in augustus jl. een video gericht op jongeren met uitleg over hulpvraagfraude zodat zij ook hun (groot)ouders waarschuwen. In september startte mijn ministerie de campagne «Senioren en Veiligheid» met als doel senioren bewust te maken en handelsperspectief te bieden om slachtofferschap van o.a. hulpvraagfraude) te voorkomen. Ook onze partners zetten zich in om slachtofferschap te voorkomen.
In repressieve zin wordt deze fraudevorm serieus opgepakt door politie en het OM, bijvoorbeeld met de invoering van de internetaangifte. De aanpak van hulpvraagfraude wordt centraal opgezet en gecoördineerd. De aangiftes worden landelijk gebundeld zodat snel zicht is op de zaken die kansrijk zijn. Dit heeft inmiddels geleid tot een aantal succesvolle opsporingsonderzoeken en strafzaken[8].
Daarnaast wordt door het kabinet ook ingezet op het verder versterken van het financieel rechercheren door onder meer het proces van vorderen van gegevens bij banken en andere betaaldienstverleners te automatiseren. Per 10 september jl. is de Wet en het Besluit verwijzingsportaal bankgegevens in werking getreden. Het Verwijzingsportaal bankgegevens maakt het mogelijk dat geautomatiseerd binnen 30 seconden identificerende gegevens van banken en andere betaaldienstverleners kunnen worden verkregen ten behoeve van opsporingsonderzoeken. Zo kan de politie sneller en beter financieel onderzoek doen naar mogelijke fraudeurs. Het vorderen van saldo- en transactiegegevens is een volgende stap bij financieel onderzoeken omdat het wenselijk is ook dit proces te versnellen wordt samen met de aangesloten diensten en de banken gewerkt aan het automatiseren van dit proces. Verder werken de banken nauw samen met de politie in de Electronic Crimes Taskforce (ECTF) en zetten zij zich in op de aanpak van geldezels van verschillende soorten fraude, waaronder ook deze vorm.

Vraag 9
Welke informatie heeft de Financial Intelligence Unit – Nederland (FIU) over deze transacties? Welke informatie hebben zij over daders? Heeft de FIU daarnaast in de gaten om hoeveel dadergroepen gaat dit?

Antwoord 9
De Financial Intelligence Unit-Nederland (FIU-Nederland) is op basis van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft) het enige en centrale meldpunt, waar diverse meldingsplichtige instellingen ongebruikelijke transacties dienen te melden die kunnen wijzen op witwassen en terrorisme financiering. Deze meldingen van ongebruikelijke transacties kunnen ook betrekking hebben op fraude, maar dit betreft bijvangst. Over de jaren 2016 tot en met begin september 2020 heeft de FIU in totaal bijna 4.900

[8] https://www.nu.nl/tech/6076576/twee-mannen-uit-deventer-krijgen-tot-drie-jaar-cel-voor-whatsapp-fraude.html. Andere zaken zijn bijvoorbeeld: https://www.om.nl/actueel/nieuws/2020/08/11/celstraffen-geeist-voor-vriend-in-noodfraude, https://www.politie.nl/mijn-buurt/nieuws/2020/mei/1/02-fraude-via-whatsapp-24-verdachten-aangehouden.html?geoquery=Deventer%2C+Nederland&distance=5.0 en https://www.politie.nl/nieuws/2019/augustus/23/02-apeldoorn-zeventien-arrestaties-na-whatsappfraude.html

meldingen van ongebruikelijke transacties van meldingsplichtige instellingen ontvangen, die mogelijk verband kunnen houden met fraude, waaronder hulpvraagfraude. Vanaf 2018 ziet de FIU een sterk toenemende trend. In 2018 ging het nog om circa 200 meldingen van ongebruikelijke transacties, in 2019 was dat aantal 1.060 en in 2020 waren er tot en met begin september bijna 3.400 meldingen. Ongebruikelijke transacties die na analyse door het hoofd van de FIU-Nederland verdacht zijn verklaard zijn, ook op voornoemd thema, ter beschikking gesteld aan de diverse (bijzondere) opsporingsdiensten en inlichtingen- en veiligheidsdiensten. Door de opsporing wordt op uiteenlopende wijzen gebruik gemaakt van de verdachte transacties, onder meer als sturingsinformatie, als startinformatie voor een strafzaak of als onderdeel van het bewijs in een strafzaak. Deze informatie kan dan ook behulpzaam zijn voor het in kaart brengen van daders en dadergroepen.