Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

29 911 Bestrijding georganiseerde criminaliteit

Nr. 341 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 30 november 2021

Hierbij informeer ik uw Kamer over een viertal onderwerpen.

1) De ontwikkeling van een integraal plan van aanpak voor de bestrijding van online fraude mede namens de Minister van Economische Zaken en Klimaat en de Minister van Financiën.[1]
2) Mijn toezegging om met banken in gesprek te gaan over een extra beveiligingsmechanisme bij het overboeken van geld door slachtoffers van vriend-in-nood-fraude.[2]
3) De uitvoering van de motie van het lid van Nispen c.s. om met het openbaar ministerie te spreken over de wenselijkheid van een richtlijn of kader voor zelfmelding en zelfonderzoek door bedrijven met de inschakeling van advocaten.[3]
4) Tot slot informeer ik u mede namens de Minister voor Rechtsbescherming over de bijgewerkte planning voor het opstellen van een beleidsreactie op de evaluatie van de Wet controle op rechtspersonen.[4]

1. Integrale aanpak van online fraude

Aanleiding

Online fraude is een groeiend maatschappelijk probleem. Door de technologie en het internet hebben oplichters in korte tijd een zeer groot bereik en kunnen zij snel en eenvoudig hun werkwijze aanpassen. Vroeger ging het om skimming van bankpassen, tegenwoordig gaat het vooral om spoofing, bankhelpdeskfraude, phishing en de zogenoemde hulpvraagfraude. Online fraude heeft grote emotionele en financiële gevolgen voor slachtoffers en veroorzaakt een aanzienlijke schadelast voor het bedrijfsleven. De banken geven aan dat met de schade door phishing en bankhelpdeskfraude in de eerste zes maanden van 2021 ruim 22,5 miljoen is

[1] Kamerstuk 29 911, nr. 314.
[2] Handelingen II 2020/21, nr. 99 item 50.
[3] Kamerstuk 29 279, nr. 664.
[4] Kamerstuk 33 857, nr. 4.

kst-29911-341
ISSN 0921 - 7371
's-Gravenhage 2021

gemoeid. Hun verwachting is dat als deze groei doorzet het totaal het schadebedrag van 2020 (39,5 miljoen) zal overstijgen. De groeiende omvang van fraude vraagt om integrale samenwerking; gerichte aanpak aan de bron, gezamenlijke inzet op preventie, detectie en interventies en strafrechtelijke opsporing. Een integrale aanpak voorkomt versnippering van initiatieven. Bovendien denken we daarmee een grotere impact te bereiken dan met losstaande initiatieven en om in de toekomst nieuwe fraudevormen effectief te bestrijden. In onze eerdere brief hebben we beschreven welke acties al genomen worden door de telecomsector, de bankensector en de overheid om digitale fraude tegen te gaan, hebben we het belang van een integrale aanpak benoemd en hebben we aangegeven uw Kamer opnieuw te informeren.

Beleidsambities

In het voorjaar is het overleg gestart met vertegenwoordigers van de Nederlandse Vereniging van Banken (NVB), de Betaalvereniging Nederland (BVN), de Vereniging COIN (Vereniging voor telecomaanbieders) en met het Ministerie van Economische Zaken en Klimaat en het Ministerie van Financiën. In de afgelopen maanden is een gezamenlijke probleemanalyse uitgevoerd. Hieruit kwam naar voren dat er zowel op publiek als privaat vlak meerdere initiatieven zijn genomen, maar dat een gedeelde strategie en regie ontbreekt. Dit is nodig om in de toekomst als publieke partijen samen met private partners een grotere impact te bereiken en om op langere termijn en met structurele maatregelen (zoals wetgeving) de groei van onlinefraude daadwerkelijk terug te dringen.
Onze gezamenlijke beleidsambities zijn gericht op:

- preventie: het vergroten van de bewustwording omtrent online fraude en veiligheidsmaatregelen die burgers zelf kunnen treffen, daar is de grootste winst qua preventie te behalen;
- interventies: het wegnemen van gelegenheid en het verstoren van fraude en het opwerpen van barrières;
- slachtofferhulp: slachtoffers handelingsperspectief bieden door middel van voorlichting waar zij terecht kunnen voor hulp en hoe financiële schade is te verhalen op daders; en
- het faciliteren van expertise- en informatiedeling.

Actielijnen

We hebben met de NVB, BVN en COIN verkend waar een integrale aanpak betrekking op zou moeten hebben. Het is belangrijk om tot een stevige aanpak te komen, omdat het aantal oplichtingszaken stijgt en de schade toeneemt. Het gaat tegelijkertijd om een complexe maatschappelijke opgave. Het ontwikkelen van een door alle partners gedragen strategie heeft bovendien tijd nodig. Ook op de langere termijn zal sectoroverstijgende inzet en samenwerking nodig zijn. Daar is tijd en een breed draagvlak voor nodig. Naast de genoemde partners zijn ook andere partijen belangrijk voor samenwerking, zoals de Fraudehelpdesk, internet serviceproviders, online platforms voor sociale media, online handelsplatformen en bijvoorbeeld ouderen- en jongerenorganisaties. Dit zijn ook belangrijke partners de integrale aanpak van cybercriminaliteit. Bovendien kan niet alles tegelijk en voor de verwezenlijking van ambities zijn middelen en capaciteit en nodig. De keuzes en prioriteitstelling daarvoor zijn ook aan een volgend kabinet.
Op basis van het gevoerde overleg schetsen we de gewenste richting en de grote lijnen voor een integrale aanpak. Dit wordt de komende tijd verder uitgewerkt.

• Preventie en slachtofferhulp

Op dit moment worden zowel vanuit de overheid als de private sector verscheidene voorlichtingscampagnes georganiseerd voor kwetsbare doelgroepen, zoals senioren en jongeren. De ambitie is om consumenten en bedrijven te informeren over online risico's en de digitale hygiëneregels voor veilig internetverkeer actief onder de aandacht te brengen. Door middel van samenwerking en regie kan het effect van een gezamenlijke publiekscampagne en -voorlichting gericht op digitale weerbaarheid versterkt worden. Een concreet voorbeeld is de voorlichtingscampagne gericht op «ouderen en veiligheid». Het is voorts van belang slachtoffers handelingsperspectief te bieden door verwijzing naar instanties waar zij terecht kunnen met vragen. Voor betekenisvolle opvolging voor slachtoffers is het van belang dat zij eenvoudig aangifte kunnen doen en dat er laagdrempelige voorzieningen zijn voor slachtoffers om hun schade te verhalen op daders, zoals een directe aansprakelijkstelling of met inschakeling van deurwaarders.

• Interventies

De ambitie is om de keten van signaleren, melden en aangifte te verbeteren. Onder deze actielijn wordt in aanvulling op bestaande preventieve en repressieve maatregelen in kaart gebracht wat nog meer mogelijk is binnen de bestaande wettelijke kaders, zoals de uitvoering van het spoofingverbod en de toepassing van een notice and take downprocedure. De Autoriteit Consument en Markt zal haar visie geven over wat telecomaanbieders binnen het huidige wettelijke kader kunnen en moeten doen. Het door de Minister van Economische Zaken en Klimaat aangekondigde wetsvoorstel tot aanpassing van de Telecommunicatiewet met aanscherping van het spoofingverbod en flankerende maatregelen zal naar verwachting in het eerste kwartaal van 2022 gereed zijn voor internetconsultatie.

Naast de gewenste inzet op preventie en interventies is de inzet van het strafrecht van belang. Het strafrecht wordt toegepast als optimum remedium en in betekenisvolle zaken. Dit heeft geleid tot meerdere aanhoudingen en tot succesvolle strafrechtelijke vervolging, waarbij de rechter gevangenisstraf heeft opgelegd.[5]

Tegen de achtergrond van de toename van gedigitaliseerde criminaliteit inclusief online fraude is de vraag te stellen hoe de inzet van het strafrecht betekenisvol kan blijven en wat dit vraagt van de benodigde expertise en organisatie van de opsporing. Deze verkenning wordt momenteel door de politie uitgevoerd. Op Europees niveau wordt operationeel samengewerkt door opsporingsdiensten. Dit is nodig omdat het een probleem is dat daders, geldezels en de buit van online fraude in veel gevallen naar het buitenland verdwijnen.

[5] 4,5 jaar gevangenisstraf wegens grootschalige digitale oplichting | Nieuwsbericht | Openbaar Ministerie (om.nl); Politie Oost-Brabant houdt 47 verdachten aan voor WhatsApp-fraude – Telecompaper; Rechtbank legt celstraffen op voor WhatsApp fraude | Nieuwsbericht | Openbaar Ministerie (om.nl); Gevangenisstraf geëist tegen «gehaaide» phishingverdachten | Nieuwsbericht | Openbaar Ministerie (om.nl); Belangrijke facilitator betaallink-fraude opgepakt | Nieuwsbericht | Openbaar Ministerie (om.nl); Grootschalige phishing: OM eist tot twee jaar gevangenisstraf | Nieuwsbericht | Openbaar Ministerie.

• *Kennis- en informatiedeling*

In aanvulling op de genoemde actielijnen worden de mogelijke voordelen van een expertisecentrum en een centraal meldpunt bezien voor het kunnen uitwisselen van kennis en signalen van online fraude. We betrekken in het onderzoek internationale voorbeelden alsook de Fraudehelpdesk. Het is wenselijk dat online bedreigingen en signalen effectief kunnen worden gedeeld zodat dit ook omgezet kan worden in een snelle respons. Bijvoorbeeld in de vorm van gerichte waarschuwingen aan de betreffende doelgroepen of het informeren van actoren die malafide werkwijzen kunnen verstoren. We zien het belang van informatie-uitwisseling van private en publieke partijen. Als rode draad onderzoeken we de ervaren belemmeringen onder het huidige wettelijke kader bij informatiedeling ten behoeve van fraudepreventie en de waarborgen die gelden zoals de bescherming van privacy.

2. Gesprek met banken over het vasthouden of terugdraaien van overboekingen van slachtoffers van vriend-in-nood-fraude

Ik heb uw Kamer toegezegd om met banken te spreken over het treffen van een extra veiligheidsmechanisme bij het overboeken van geld aan vermoedelijke fraudeurs. Al eerder heb ik uw Kamer geïnformeerd over wat banken al doen tegen bancaire en niet-bancaire fraude.[6]

Banken hebben desgevraagd aangegeven dat zij investeren in technische maatregelen om verschillende vormen van fraude terug te dringen en consumenten voor te lichten en te waarschuwen. Banken waarschuwen hun klanten actief in direct contact (bijvoorbeeld via de app) en via de media. Desondanks neemt digitale fraude en oplichting toe, met veel leed en ongemak bij de slachtoffers tot gevolg. In het betalingsverkeer zijn diverse merkbare en niet merkbare maatregelen ingevoerd. Voorbeelden hiervan zijn de invoering van een IBAN-Naam Check (naam-nummer-controle), de mogelijkheid om betaallimieten in te stellen, de tweefactor authenticatie en de zogenoemde «gelijk oversteken»-service, die klanten van een online marktplaats kunnen inzetten om hun transacties veilig te laten verlopen.

Ook werken banken met verschillende fraudedetectiesystemen om fraudeleuze transacties op te sporen en te onderzoeken. Wanneer er sprake is van een verdachte transactie, wordt deze transactie automatisch geparkeerd of tegengehouden door de bank. Er is dus al sprake van een veiligheidsmechanisme bij het overboeken van geld aan vermoedelijke fraudeurs. Hierbij geldt wel dat niet iedere frauduleuze transactie wordt gedetecteerd.

Bij hulpvraagfraude, zoals via WhatsApp, worden consumenten buiten het zicht van de bank, op geraffineerde wijze misleid om zelf een betaling over te maken aan een zogenaamde bekende. Hierdoor heeft een dergelijke betaling alle kenmerken van een legitieme transactie en zal deze transactie in de meeste gevallen niet als verdachte transactie naar voren komen in het fraudedetectiesysteem. Dat is ook niet altijd wenselijk vanwege het belang van een goed functionerend en betrouwbaar betalingsverkeer. Op het moment dat slachtoffers zich bij de bank melden, is het veelal te laat. Criminelen hebben het geld vaak al weggesluisd naar andere (buitenlandse) bankrekeningen of het geld is via geldezels al contant opgenomen. Terugboeken is in deze situatie dan niet aan de orde.

---

[6] Kamerstuk 29 911, nr. 237 resp. Kamerstuk 29 911, nrs. 302 en 314.

Sinds begin dit jaar kan een gedupeerde rekeninghouder (onder voorwaarden) de naam, adres en woonplaatsgegevens van de (vermeende) fraudeur bij de banken opvragen om via een civiele procedure schade te verhalen op de daders. De banken nemen contact op met de vermeende dader met het verzoek het bedrag, dat onder valse voorwendselen werd overgemaakt, terug te boeken aan het slachtoffer.
Wanneer dit niet tot volledige terugbetaling leidt, kunnen slachtoffers vervolgens via een civielrechtelijke procedure het schadebedrag verhalen bij de ontvanger van het geld. Zo is het voor slachtoffers van onder meer hulpvraagfraude via WhatsApp mogelijk om met professionele hulp gemakkelijker het door fraudeurs buitgemaakte bedrag terug te krijgen. Ook worden sinds het najaar 2020 spoofing-slachtoffers financieel gecompenseerd als zij voldoen aan het coulancekader spoofing. Dit hebben banken mogelijk gemaakt na aandringen van uw Kamer en na overleg met de Minister van Financiën. Het kabinet spreekt zijn waardering uit dat banken die verantwoordelijkheid hebben genomen. Banken vragen om mitigerende maatregelen om de groei van online fraude en de schadelast ervan in te dammen. Binnen de integrale aanpak van online fraude zal onderzocht worden wat er nog meer mogelijk is. Een brede samenwerking is van belang, ook met sociale media platforms om er voor te zorgen dat er in een vroeg stadium maatregelen worden genomen om mensen beter te kunnen beschermen tegen specifieke vorm van fraude.

3. Overleg over de wenselijkheid van een richtlijn voor zelfonderzoek door bedrijven met inschakeling van advocaten

Ter uitvoering van de motie van het lid Van Nispen (SP) heb ik met het Openbaar Ministerie (OM) besproken of het wenselijk is een richtlijn of kader te ontwikkelen, waarin beschreven wordt waar zelfonderzoek door bedrijven aan moet voldoen en met bijzondere aandacht hoe omgegaan moet worden met de geheimhoudingsplicht van de betrokken advocaat.

Bedrijven die worden verdacht van financieel-economische criminaliteit kunnen eigen advocaten inschakelen om de gang van zaken te onderzoeken. In opdracht van het WODC wordt momenteel onderzoek uitgevoerd naar de voor- en nadelen van zelfonderzoek en zelfmelding door bedrijven. Het onderzoek zal ingaan op de betrouwbaarheid en bruikbaarheid van de resultaten van dergelijk zelfonderzoek voor opsporingsinstanties. Ook zal het onderzoek ingaan op de vraag hoe kan worden omgegaan met zelfmeldingen van bedrijven inzake financieel-economische criminaliteit. Er bestaat nu geen kader of richtlijn. Het OM heeft aangegeven dat het wenselijk is om voor een standpuntbepaling over de wenselijkheid van een mogelijk kader de bevindingen van het WODC-onderzoek af te wachten. Na de afronding van het onderzoek, naar verwachting in maart 2022, zal ik uw Kamer zo spoedig mogelijk informeren.

4. Beleidsreactie evaluatie Wet controle op rechtspersonen

Onlangs is uw Kamer geïnformeerd over de WODC-evaluatie en is aangegeven dat een beleidsreactie later dit jaar volgt.[7] Uit de evaluatie blijkt dat de maatregelen van de wet in de praktijk worden gebracht zoals was bedoeld door de wetgever. Door de onderzoekers is echter ook aangegeven dat niet is vast te stellen in welke mate deze uitvoering effectief is omdat gekwalificeerde doelen voor deze wet ontbreken. Het onderzoeken van de toegevoegde waarde is van belang en daarom zal ter voorbereiding van de beleidsreactie met Justis en met stakeholders

[7] Kamerstuk 33 857, nr. 4.

besproken worden wat de meerwaarde van risicomeldingen is voor de uitvoering van hun wettelijke taken voor controle, opsporing en handhaving. Hierbij zal -naast de bevindingen van de onderzoekers in deze evaluatie- breder verkend worden wat er in de toekomst nodig is voor het toezicht op rechtspersonen, gegeven de maatschappelijke ontwikkelingen en in het licht van andere producten of opgaves. Bezien zal onder meer worden of de kring van afnemers kan worden uitgebreid en wordt de mogelijkheid onderzocht om een eigen bijdrage van de behoeftestellers te vragen. Deze tussenstappen leiden ertoe dat uw Kamer naar verwachting in de zomer 2022 de beleidsreactie zal ontvangen.

Tot slot

Met deze brief heb ik u de ambitie voor de integrale aanpak van online fraude toegelicht. Dit is een grote en complexe opgave die in de komende periode de nodige inspanning zal vragen. Daarom is tijd nodig om in overleg met partners uitwerking te geven aan de strategische visie en concrete actielijnen. Tegelijkertijd is er tempo gewenst vanwege de toename en om schade voor potentiële slachtoffers te voorkomen.

Het is vervolgens aan het (volgende) kabinet om daarvoor de randvoorwaarden te faciliteren, meetbare doelstellingen te formuleren en zo nodig daarin specifieke beleidsaccenten te leggen. Uw Kamer zal naar verwachting voor de zomer geïnformeerd worden over de uitvoering. Ook ben ik ingegaan op mijn toezegging om met banken in overleg te gaan en over het terughalen van overboekingen aan fraudeurs en over het overleg met het OM over een richtlijn voor zelfonderzoek door bedrijven door inschakeling van advocaten. Zowel de toezegging als de motie beschouw ik als uitgevoerd.

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