Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2021–2022

29 911 Bestrijding georganiseerde criminaliteit

Nr. 372

BRIEF VAN DE MINISTERS VAN JUSTITIE EN VEILIGHEID, VAN FINANCIËN, VAN ECONOMISCHE ZAKEN EN KLIMAAT EN VOOR RECHTSBESCHERMING

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 8 juli 2022

Inleiding

Online fraude is een groeiend maatschappelijk probleem. Bij online fraude is sprake van oplichting – bijvoorbeeld door het aannemen van een valse naam, identiteit of hoedanigheid – waarmee de fraudeur het slachtoffer digitaal beweegt tot de afgifte van goederen, diensten of andere financiële voordelen.[1] Uit recent onderzoek blijkt dat het aantal slachtoffers van online fraude stijgt.[2] Naast financiële schade voor slachtoffers – zowel bij burgers als in het bedrijfsleven – kan online fraude ook emotionele of psychische schade veroorzaken. Het is van groot belang om met brede preventie en gerichte repressie een kentering aan te brengen in deze ontwikkeling. Dat kan alleen door met alle bij dit onderwerp betrokken publieke en private partijen samen te werken. In de brief over spoofing en bankhelpdeskfraude van 15 juni 2021, heeft mijn ambtsvoorganger uw Kamer mede namens de Minister van Financiën en de Staatssecretaris van Economische Zaken en Klimaat toegezegd om te komen tot een integrale aanpak van online fraude.[3] Op 30 november 2021 is uw Kamer geïnformeerd over de ontwikkeling hiervan.[4] Met de motie van het lid Michon-Derkzen is het kabinet vervolgens verzocht om de integrale aanpak zo spoedig mogelijk te presenteren.[5] De noodzaak daartoe wordt ook onderschreven door de bevindingen uit het onderzoek «Fraudevicti-

[1] Zie ook Artikel 326 (Oplichting) Wetboek van Strafrecht.
[2] fraudevictimisatie-in-nederland.pdf (utwente.nl).
[3] Kamerstuk 29 911, nr. 314.
[4] Kamerstuk 29 911, nr. 341.
[5] Kamerstuk 28 684, nr. 678.

kst-29911-372
ISSN 0921 - 7371
's-Gravenhage 2022

misatie in Nederland», waar wij op verzoek van de Commissie voor Justitie en Veiligheid van uw Kamer een eerste reactie op geven in deze brief.[6]

In de voorbereidingen voor de integrale aanpak online fraude hebben wij sinds begin dit jaar gesprekken met verschillende stakeholders gevoerd en hebben wij expertsessies georganiseerd met relevante publieke en private partijen. Uit die gesprekken blijkt een behoefte aan intensievere samenwerking in de bestrijding van online fraude vanuit een gezamenlijke visie, waarbij rekenschap wordt gegeven van het veelvoud aan initiatieven die daartoe al ondernomen wordt. Daarom geven we in deze brief een overzicht van bestaande initiatieven en aanvullende stappen die in het afgelopen half jaar zijn gezet door publieke en private partners om online fraude tegen te gaan. Recent hebben we enkele belangrijke acties ondernomen, waaronder:

– de uitbreiding van de pilot directe aansprakelijkheid waarbij slachtoffers van online fraude schade kunnen verhalen op daders via een civielrechtelijke procedure;
– het informeren van jongeren via sociale media over nieuwe vormen van online fraude om te voorkomen dat zij slachtoffer worden;
– de start van een systeemdoorlichting online fraude om beter inzicht te krijgen in ontwikkelingen in modus operandi van fraudeurs, het opwerpen van barrières en effectief ingrijpen in criminogene processen;

De bestaande en nieuwe acties vormen de basis waarop de integrale aanpak verder wordt ontwikkeld. We schetsen in deze brief hoe die aanpak de afgelopen maanden is vormgegeven en blikken vooruit naar de verdere invulling ervan, waarover wij uw Kamer in januari 2023 informeren. Tot slot wordt uw Kamer, vanwege de nauwe samenhang met de integrale aanpak geïnformeerd over de uitvoering van de motie van de leden Michon-Derkzen en Van Nispen betreffende «vriend in nood»-fraude[7] en over de uitvoering van de motie van de leden Van Nispen en Ellian over oninbare civiele vorderingen.[8]

Onderzoek «Fraudevictimisatie in Nederland»

De aard van online fraude – in al zijn verschillende vormen – maakt het moeilijk om goed inzicht te krijgen in de gevolgen ervan. Voor een effectieve aanpak van online fraude is onderzoek daarom van groot belang. Het recente rapport van de Universiteit Twente over «Fraudevictimisatie in Nederland» geeft een verdiepend beeld van wie de slachtoffers van online fraude zijn, de schade die zij ondervinden en de hulp die zij zoeken en krijgen.[9] Het onderzoeksrapport biedt een goede inkijk in het groeiende maatschappelijke probleem van online fraude en doet heldere aanbevelingen om slachtofferschap terug te dringen. Terwijl de meeste criminaliteitsvormen in het fysieke domein – zoals overvallen en straatroof – de afgelopen jaren een dalende trend hebben laten zien, is online criminaliteit, waaronder online fraude, sterk toegenomen.[10] Hoewel deze stijging al enkele jaren geleden is ingezet, maakt het onderzoek duidelijk dat de Covid-19-pandemie als katalysator heeft gediend omdat we (nog) meer van onze tijd online door zijn gaan brengen.[11] De stijging in online

---

[6] fraudevictimisatie-in-nederland.pdf (utwente.nl).
Verzoek van de vaste commissie voor Justitie en Veiligheid d.d. 14 april 2022.
[7] Kamerstuk 28 684, nr. 679.
[8] Kamerstuk 28 684, nr. 680.
[9] fraudevictimisatie-in-nederland.pdf (utwente.nl).
[10] Kamerstuk 28 684, nr. 666.
[11] https://www.utwente.nl/nl/bms/fraudvic/fraudevictimisatie-in-nederland.pdf.

criminaliteit, waaronder online fraude, betrof ruim 75% sinds het begin van de coronacrisis ten opzichte van een jaar eerder.[12] Het CBS constateert in haar veiligheidsmonitor dat 10% van de bevolking (ruim 1,7 miljoen Nederlanders) in 2021 slachtoffer is geworden van online fraude.[13]

Het onderzoek van de Universiteit Twente bevestigt dat een aanzienlijk deel van de Nederlandse bevolking te maken krijgt met fraude (41,7% maakt een poging mee, 15,7% wordt daadwerkelijk slachtoffer) en dat iedereen slachtoffer kan worden; socio-demografische variabelen zoals leeftijd en geslacht spelen maar een beperkte rol. Wel stellen de onderzoekers dat jongeren gemiddeld genomen iets vaker slachtoffer zijn van fraude dan ouderen. De totale jaarlijkse schade van online fraude bedraagt naar schatting € 2,75 miljard euro. In tegenstelling tot andere onderzoeken,[14] stelt het rapport dat de impact van slachtofferschap van fraude voor de meeste slachtoffers beperkt is. Er is echter een kleine significante groep (5 á 15 procent) die erg veel schade ondervindt, zowel financieel, mentaal, lichamelijk als sociaal. Het onderzoek constateert verder dat de aangiftebereidheid van slachtoffers bij de politie slechts 11,8% is, vanwege schaamte (slachtoffers geven zichzelf de schuld) of lage schadebedragen (de meeste slachtoffers verliezen € 50 of minder). Bijna een derde van de slachtoffers zoekt geen enkele vorm van hulp, wat leidt tot een aanzienlijk hiaat in het zicht op de daadwerkelijke omvang van slachtofferschap van online fraude. Het onderzoek biedt ook perspectief en concludeert dat het aantal slachtoffers van online fraude kan dalen als mensen beter op de hoogte zijn van de werkwijze van fraudeurs. Ook het tegengaan van snelle beslissingen door potentiële slachtoffers kan daarbij helpen. De grootste winst zou volgens de onderzoekers daarom te behalen zijn in het proactief informeren en waarschuwen van burgers tegen verschillende vormen van online fraude, bijvoorbeeld met een publiekscampagne of campagnes op scholen. Verder zouden technische maatregelen, bijvoorbeeld bij banken of in de telecomsector, helpen om barrières te creëren voor fraudeurs en slachtofferschap te voorkomen. Een aantal van de acties die in deze brief worden genoemd, geven directe invulling aan de aanbevelingen uit het rapport. De conclusies van het onderzoek sluiten kortom goed aan bij het ingezette beleid en worden meegenomen in de verdere uitwerking van de integrale aanpak.

Veel voorkomende vormen van online fraude:
Phishing: *Bij phishing probeert de fraudeur om via e-mail en sms vertrouwelijke informatie, zoals persoonsgegevens, wachtwoorden, bankgegevens en creditcardnummers, te bemachtigen.*
Online handelsfraude:*Online handelsfraude betreft aan- en verkoopfraude via bijvoorbeeld online-handelsplaatsen of valse webwinkels. Bij aankoopfraude maakt de verkopende partij er de gewoonte van om producten of diensten niet te leveren na betaling door het slachtoffer. Bij verkoopfraude worden goederen of diensten wel geleverd door het slachtoffer, maar maakt de ontvanger er de gewoonte van om daar niet voor te betalen.*
Spoofing: *Spoofing houdt in dat door misbruik van het systeem voor nummerdoorgifte een niet-toegekend nummer in het adresveld verschijnt als het nummer van een betrouwbare of bekende beller/afzender. De fraudeur gebruikt bijvoorbeeld het telefoonnummer van een bank of overheidsinstelling om potentiële slachtoffers te bellen.*
Vriend-in-noodfraude: *Bij vriend-in-noodfraude doet de fraudeur zich voor als een bekende die in geldnood is en vraagt om geld over te maken. Dit gebeurt meestal via instant messaging apps, e-mail, SMS en sociale media.*

---

[12] Dit betreft een gemiddelde van de stijging ten opzichte van een jaar eerder zoals wekelijks gemeld in de Corona Crime Change Monitors sinds week 14 van 2020.
[13] 5. Online criminaliteit (cbs.nl).
[14] Veiligheidsmonitor 2021 vermeldt dat 18% van de slachtoffers na het delict last hebben gehad van emotionele, financiële en/of psychische problemen.

Bestaande en nieuwe acties om online fraude tegen te gaan

In de brieven aan uw Kamer van 15 juni 2021 en 30 november 2021 hebben onze voorgangers bestaande initiatieven benoemd van verschillende publieke en private partners om online fraude tegen te gaan. Sinds het versturen van deze brieven hebben experts van de betrokken organisaties elkaar gesproken in verschillende werksessies, die zijn begeleid door het Centrum voor Criminaliteitspreventie en Veiligheid. Daarin is onder andere door het bedrijfsleven het belang van cross-sectorale gegevensdeling, naar Engels model, onderstreept.[15] Ook is de aanpak van online fraude onderwerp van gesprek geweest tussen publieke en private bestuurders tijdens een ondernemersdiner op 16 mei 2022. Met kennisinstellingen als TNO, CBS en Universiteit Twente is gesproken om inzicht in het fenomeen online fraude te vergroten. Tot slot is er een begin gemaakt met het leren van ervaringen in andere landen met betrekking tot hun aanpak. Zo is een werkbezoek gebracht aan de Belgische collegas die een succesvol phishing-meldpunt hebben ingericht. Naast de waardevolle uitwisseling van informatie en ervaringen heeft dit er ook toe geleid dat we bestaande acties nog beter in beeld hebben gekregen en het afgelopen half jaar nieuwe acties hebben kunnen verwelkomen. We hechten eraan om deze waardevolle acties hier te benoemen. Ze vormen de basis waarop de integrale aanpak rust en bieden tegenwicht aan de groei van online fraude. Hieronder treft u een overzicht hiervan aan, gecategoriseerd in de pijlers van de integrale aanpak online fraude:

1. Preventie;
2. Technische barrières;
3. Slachtofferhulp;
4. Opsporing en vervolging; en
5. Expertise en informatiedeling.

1. Preventie – Het vergroten van de bewustwording omtrent online fraude en veiligheidsmaatregelen die burgers zelf kunnen treffen

Bestaande acties

- Cyberrijbewijs. Om daderschap en slachtofferschap in het digitale domein te voorkomen, is de pilot cyberrijbewijs gestart. Binnen deze pilot wordt in het basisonderwijs onderwezen over verschillende vormen van online criminaliteit, waaronder online fraude. Na de pilotfase wordt het cyberrijbewijs beschikbaar voor alle scholen in het basisonderwijs, waarbij het programma wordt aangeboden via verschillende onderwijsplatforms.
- Eerst checken, dan klikken. Via dit convenantoverleg wordt periodiek met partners uit de ICT-sector, telecomsector, dienstverleners op het internet en bankwereld, de rijksoverheid, gemeenten en brancheorganisaties gesproken over het terugdringen van gedigitaliseerde criminaliteit waaronder online fraude. Initiatieven die voortkomen uit dit overleg richten zich onder andere op voorlichting, het voorkomen van slachtoffers en situationele preventie.
- Samen Digitaal Veilig. In 2021 hebben de Ministeries van Justitie en Veiligheid en van Economische Zaken en Klimaat in samenwerking met VNO-NCW, MKB-NL en de BOVAG de intentieovereenkomst «Samen Digitaal Veilig» afgesloten. Op basis van dit initiatief is een platform opgericht waarbij leden van de BOVAG via hun branchevereniging in een vertrouwde omgeving worden voorgelicht over veilig

[15] Zie ook beleidsreactie «Cross-sectorale gegevensdeling tussen private partijen voor fraudebestrijding», Kamerstukken 17 050 en 32 761, nr. 576.

gebruik van het internet. Hierdoor zijn ondernemers naar verwachting minder snel slachtoffer van verschillende vormen van online criminaliteit, waaronder online fraude.[16]
- Preventie activiteiten op social media: In opdracht van het Ministerie van Justitie en Veiligheid maken Scholieren.com en het Centrum voor Criminaliteitspreventie en Veiligheid online content om jongeren te informeren. Dit betreft o.a. filmpjes over geldezels, en aan-/ verkoopfraude die via social media wordt verspreid.
- Voorlichting op scholen door Halt.alt heetHalt heeft tezamen met het Ministerie van Justitie en Veiligheid en het Centrum voor Criminaliteitspreventie en Veiligheid de voorlichting »online fraude en cybercrime» gemaakt die wordt gegeven door medewerkers van Halt op middelbare scholen.
- Maand van senioren en veiligheid. Het Ministerie van Justitie en Veiligheid heeft in april jl. voor de derde keer de campagne «Senioren en Veiligheid» gedraaid. Hiervoor zijn informatiefilmpjes gemaakt en uitgezonden. In deze filmpjes worden de onderwerpen babbeltrucs, phishing, hulpvraagfraude en spoofing toegelicht en worden er tips gegeven om slachtofferschap van (online) fraude onder senioren te voorkomen. In het tv-programma «Tijd voor Max» is aandacht besteed aan de start van de campagne. Vervolgens hebben veel partners, waaronder de ouderenbonden, bibliotheken, de fraudehelpdesk, banken, telecomproviders en ruim 250 gemeenten, de filmpjes via hun eigen (sociale) mediakanalen verspreid.

Nieuwe acties

- Communicatiestrategie online fraude. Zoals ook gesteld in het onderzoek van Universiteit Twente, is proactieve communicatie over online fraude van groot belang om slachtofferschap te voorkomen. Het Ministerie van Justitie en Veiligheid bespreekt met het Ministerie van Algemene Zaken een communicatiestrategie voor online fraude. Partners en kennisinstellingen worden hierbij betrokken, omdat zij ook veel aan communicatie doen, zoals bijvoorbeeld de campagne «Veilig Bankieren» van banken. De communicatiestrategie heeft tot doel burgers zo veel mogelijk alert te laten zijn op online fraude.
- Preventie doelgroep jongeren. In opdracht van het Ministerie van Justitie en Veiligheid organiseert het Centrum voor Criminaliteitspreventie en Veiligheid in het najaar van 2022 een denktank met onder andere Halt, het Centraal Meldpunt voor Identiteitsfraude en de politie om verdere invulling te geven aan samenwerking op de doelgroep jongeren.
- Communicatie richting jongeren. In opdracht van het Ministerie van Justitie en Veiligheid zetten het Centrum voor Criminaliteitspreventie en Veiligheid en Scholieren.com hun samenwerking voort door jongeren te informeren over nieuwe vormen van online fraude. Dit doen zij met filmpjes, artikelen en andere online content die wordt verspreid via verschillende sociale media.

2. Technische barrières – Het wegnemen van gelegenheid en verstoren van fraude door technische aanpassingen in systemen

Bestaande acties

- Technische barrières bankwezen. Banken werken met de IBAN-Naamcheck, waarmee controle van tenaamstelling en rekeningnummer plaatsvindt voordat geld wordt overgeboekt. Verder hanteert een aantal banken een fraudedetectiesysteem: Bij afwijkende of mogelijk

[16] Zie ook Kamerbrief Preventie cybercrime voor het midden- en kleinbedrijf, d.d. 6 juli 2022.

risicovolle overboekingen, wordt uit voorzorg contact opgenomen met de cliënt. De banken blijven deze systemen door ontwikkelen, waar mogelijk in samenwerking met elkaar en andere partners.
– Technische barrières telecomsector. Telecomaanbieders hebben maatregelen getroffen om smishing (SMS-phishing) met alphanumerieke en numerieke nummers tegen te gaan, en hebben in samenwerking met banken maatregelen getroffen om spoofing van telefoonnummers van banken tegen te gaan. Voorts worden in samenwerking met politie en op verzoek van de Autoriteit Consument en Markt vaste telefoonnummers die worden gebruikt voor helpdeskfraude (techsupport-scams) geblokkeerd.
– Marktplaats barrières. Marktplaats heeft een aantal maatregelen getroffen om aan-/verkoopfraude aan te pakken, waaronder de uitbreiding van Kopersbescherming. Dit is een extra mogelijkheid die gebruikers op het platform kunnen kiezen, waarbij het aankoopbedrag op een tussenrekening van Online Betaalplatform blijft staan tot de koper het product in goede staat heeft ontvangen. Als er iets misgaat, bemiddelt de betaalpartner tussen verkoper en koper. Marktplaatsgebruikers worden ook aan de voorkant beter in staat gesteld iets te doen bij onwenselijk gedrag van andere gebruikers. Een gebruiker kan nu een ander account melden en Marktplaats kan op dit signaal handelen door bijvoorbeeld dat account te blokkeren. Als preventiemaatregel is ook overgegaan naar het slechts optioneel zichtbaar maken van telefoonnummers op het platform. Iedere gebruiker die wel zijn of haar telefoonnummer zichtbaar wil laten zijn wordt actief geïnformeerd over de risico's van die keuze.
– Notice-and-takedown: Stichting registratie internetdomein kan op verzoek van particulieren en politie een domeinnaam uit de lucht halen. De politie maakt hier veelvuldig gebruik van om nepwebwinkels uit de lucht te halen. Ook andere overheidsinstanties zoals de Belastingdienst, CJIB en Logius (DIGID) zijn hier volop mee bezig om nepwebsites na phishingmails uit de lucht te halen.

Nieuwe acties

– Technische barrières bankwezen. Het Ministerie van Financiën gaat in gesprek met partijen om meer sector overstijgende technische maatregelen te nemen die fraude voorkomen (bijvoorbeeld het inbouwen van een vertraging voor het verhogen van het overboekings- en opnamelimiet).
– Technische barrières telecomsector. Telecomaanbieders werken aan aanvullende maatregelen om misbruik van telefoonnummers bij online fraude tegen te gaan.
– Aanscherping spoofingverbod: Het door de Minister van Economische Zaken en Klimaat aangekondigde wetsvoorstel tot aanpassing van de Telecommunicatiewet – met aanscherping van het spoofingverbod, een beperking van het gebruik van Nederlandse nummers vanuit het buitenland en flankerende maatregelen – gaat voor de zomer in consultatie. Met lagere regelgeving zullen een aantal onderdelen van de wet nader moeten worden ingevuld.
– Best practices notice-and-takedown. Het Ministerie van Justitie en Veiligheid doet samen met betrokken partijen onderzoek naar best practices in notice-and-takedown procedures, waarbij frauduleuze content snel offline gehaald kan worden.

3. Slachtofferhulp – Slachtoffers handelingsperspectief bieden door middel van voorlichting waar zij terecht kunnen voor hulp en hoe financiële schade is te verhalen op daders

Bestaande acties

- Coulancekader. De banken hebben een coulancekader voor slachtoffers van bankhelpdeskfraude opgezet waarbinnen banken de financiële schade van het slachtoffer compenseren.
- Verschillende meldpunten online fraude. De fraudehelpdesk adviseert gedupeerden van (online) fraude en verwijst hen naar instanties die verder kunnen helpen. Het centrale meldpunt voor identiteitsfraude biedt persoonlijke begeleiding aan slachtoffers en schakelt zo nodig ketenpartners zoals de Belastingdienst, politie of RDW in. Ook kunnen slachtoffers digitaal aangifte doen bij de politie, waarna de aangifte door het Landelijk Meldpunt Internet Oplichting van de politie in behandeling wordt genomen.
- Pilot directe aansprakelijkheid. Vanuit het Landelijk Meldpunt Internetoplichting (LMIO) van de Politie, de Service Organisatie Directe Aansprakelijkstelling (SODA) en de Landelijke Associatie van Gerechtsdeurwaarders (LAVG) heeft een pilot gedraaid om de verhaalkans voor slachtoffers van online fraude en de toegang tot het recht te vergroten door verdachte rekeninghouders civielrechtelijk aansprakelijk te stellen. Het ging om slachtoffers van aan-/verkoopfraude. Deze aanpak heeft er toe geleid dat inmiddels ruim 200 slachtoffers van aan-/verkoopfraude hun geld hebben kunnen terugeisen van verdachte rekeninghouders. Tientallen slachtoffers hebben hun geld al teruggekregen of zij krijgen het terug via aflossingsregelingen.[17] Binnen de pilot zijn onder voorwaarden NAW-gegevens van fraudeurs verstrekt aan SODA/LAVG om de financiële schade te kunnen verhalen.
- Handelingsperspectief. Verschillende partijen bieden handelingsperspectief aan slachtoffers van online fraude, zoals Slachtofferhulp Nederland en de Consumentenbond. Die partijen adviseren slachtoffers over hoe te handelen en kunnen doorverwijzen naar de juiste instanties.

Nieuwe acties

- Toepassing coulancekader. Het Ministerie van Financiën monitort de toepassing van het coulancekader van banken voor slachtoffers van bankhelpdeskfraude en zet in op een ruimhartige toepassing van dit kader.
- Vervolg pilot directe aansprakelijkheid. De politie is bezig met een vervolg op de hierboven genoemde pilot directe aansprakelijkheid. Het vervolg houdt in eerste instantie in dat de pilot op korte termijn wordt uitgebreid naar meer politie-eenheden. Parallel aan uitbreiding van de pilot, zal samen met het Ministerie van Justitie en Veiligheid, het OM de Service Organisatie Directe Aansprakelijkstelling, gerechtsdeurwaarders en banken (voor verstrekking van NAW-gegevens) verkend worden wat de mogelijkheden zijn voor landelijke implementatie. Bij verdere uitrol van de pilot is een punt van aandacht de «oninbaarheid» van civiele vorderingen, in lijn met motie Van Nispen.[18] Uit praktijkervaring van deurwaarders blijkt dat ogenschijnlijk oninbare vorderingen toch verhaald kunnen worden, bijvoorbeeld met aflossingsregelingen. Ook zal er aandacht zijn voor verschillende dadergroepen, zoals geldezels.

[17] Politie en deurwaarders strijden tegen online oplichting | politie.nl.
[18] Kamerstuk 28 684, nr. 680.

De mogelijkheid om de pilot te verbreden naar slachtoffers van vriend-in-noodfraude wordt in de verdere uitrol ook onderzocht. Dit om slachtoffers van vriend-in-noodfraude te kunnen ondersteunen bij het verhalen van hun schade, in lijn met motie Michon-Derkzen.[19]

4. Opsporing en vervolging – De aanpak van daders

Bestaande acties

- Opsporing en vervolging. Politie en het Openbaar Ministerie hebben meerdere criminele netwerken en grote aantallen geldezels opgespoord en vervolgd in verband met phishing, bankhelpdeskfraude en vriend-in-noodfraude.
- Samenwerking politie en OM met banken, marktplaats en Payment Service Providers. Politie en OM hebben een Convenant met banken en Marktplaats. Bij drie meldingen vanuit Marktplaats van aan- en verkoop fraude, gaat een signaal naar de politie die dit doorgeeft aan de banken om het rekeningnummer van de fraudeur te blokkeren. Verder loopt er bij de politie een pilot met een in het buitenland gevestigde payment service provider: Deze buitenlandse payment service provider ontvangt vanuit het Landelijk Meldpunt Internet Oplichting alerts over mogelijk malafide verkopers. Hierdoor kan grootschalige fraude worden voorkomen doordat in een vroeg stadium betalingen worden geblokkeerd. Bij drie meldingen bij de politie over een malafide webwinkel wordt dit doorgegeven aan banken, de payment service provider en SIDN, zodat deze maatregelen kunnen nemen – zoals het blokkeren van de rekening of website.

Nieuwe acties

- Afspraken over opsporing en vervolging. In de Veiligheidsagenda 2023–2026 worden prestatieafspraken met de politie en het OM gemaakt, onder meer over het aantal en de aard van strafrechtelijke onderzoeken naar gedigitaliseerde criminaliteit, waaronder online fraude. Dit draagt bij aan de kwaliteit en kwantiteit van de opsporingsonderzoeken naar onder andere online fraude. Uw Kamer zal eind 2022 over de veiligheidsagenda worden geïnformeerd.
- Gezamenlijke visie opsporing en vervolging. De politie en het OM ontwikkelen een gezamenlijke visie op de inzet van opsporing ter bestrijding van gedigitaliseerde criminaliteit, waaronder online fraude.
- Pilot heterdaad aanhouding cybercashers. In de eenheid Noord-Nederland is de politie in samenwerking met Rabobank en een elektronicawinkel recent gestart met een pilot om cybercashers op heterdaad aan te houden. Het geld dat wordt verdiend met online criminaliteit kan worden omgezet in cryptovaluta, doorgesluisd en gepind worden of gebruikt worden voor het kopen van online producten of diensten. Online bestellingen worden met regelmaat opgevolgd door een verzoek van een bank om een bestelling te annuleren vanwege fraude. De winkel annuleert de bestelling, maar doet geen melding bij de politie. In deze pilot wordt wel direct melding gedaan bij de politie en pakt de politie de melding direct op. Deze pilot heeft tot doel om vanuit meerdere partijen interventies toe te passen. Zo kan de politie de «casher» op heterdaad aanhouden voor betrokkenheid bij witwassen, de bank kan besluiten de betrokkene(n) tijdelijk in het incidentenwaarschuwingssysteem te zetten en de winkel kan de verdachte een winkelverbod opleggen. Het belang hierbij is zicht te krijgen op de cashers en het afschrikken van de daders, het verstoren

[19] Kamerstuk 28 684, nr. 679.

van criminele werkprocessen en het opwerpen van barrières voor toekomstige daders om dit soort activiteiten te ontplooien.

5. Expertise en Informatiedeling

Bestaande acties

- Centrale verzameling van meldingen van fraude bij de politie. Meldingen bij de politie van aan-/verkoopfraude worden door de politie en het Openbaar Ministerie centraal verzameld via het Landelijk Meldpunt Internet Oplichting.
- Verkenning cross-sectorale gegevensdeling. Het WODC is op verzoek van het Ministerie van Justitie en Veiligheid dit jaar een onderzoek gestart om de meerwaarde, risico's en de benodigde juridische waarborgen van sectorale gegevensdeling goed in beeld te brengen. Het onderzoeksrapport wordt eind 2022 verwacht.
- Actieprogramma Veilig Ondernemen. In het Nationaal Platform Criminaliteitsbeheersing (NPC), een samenwerkingsverband tussen overheid en bedrijfsleven, wordt gewerkt aan een nieuwe Actieprogramma Veilig Ondernemen. In de uitwerking van het nieuwe Actieprogramma wordt aandacht besteed aan knelpunten op het gebied van informatie- en gegevensdeling in de aanpak van georganiseerde ondermijnende criminaliteit, die ook voor online fraude gelden.

Nieuwe acties

- Systeemdoorlichting door TNO. Het Ministerie van Justitie en Veiligheid heeft TNO de opdracht gegeven om een systeemdoorlichting te doen van online fraude, gericht op zowel het fenomeen als de aanpak van online fraude en wat daarvoor nodig is. De systeemdoorlichting zal o.a. inzicht geven in ontwikkelingen in modus operandi en kansen voor barrières en effectief ingrijpen in criminogene processen.
- Digitale Veiligheidsmonitor CBS. Het CBS start een monitor digitale veiligheid waarin online fraude aan bod komt.
- Gezamenlijke taxonomie. Het Ministerie van Justitie en Veiligheid ontwikkelt samen met de betrokken PPS partners een gezamenlijke taxonomie voor online fraude. Voor de samenwerking is het namelijk van belang dat alle partners dezelfde »taal spreken» over online fraude en hetzelfde verstaan onder (verschillende vormen van) online fraude.
- Optimalisatie van informatie-uitwisseling telecomsector. Telecomaanbieders onderzoeken hoe zij binnen de bestaande regelgeving informatie beter kunnen uitwisselen om online fraude tegen te gaan.
- Kennisoverdracht Politie en telecomsector. Tijdens het ondernemersdiner van 16 mei jl. hebben verschillende partners uit de telecomsector de intentie uitgesproken om kennis en expertise uit te wisselen met de politie o.a. door het opleiden van politiemensen. Politie verkent op welke wijze dit bestaande samenwerking en kennis- en expertiseopbouw kan aanvullen.
- Verkennen van het landschap aan meldpunten. Er zijn verschillende meldpunten voor online fraude. We verkennen samen met de meldpunten hoe we belangrijke informatie, bijvoorbeeld over modus operandi, kunnen delen. Bijvoorbeeld of dit kan leiden tot vroegtijdige interventies en/of betere slachtofferhulp.

Tussenstand ontwikkeling integrale aanpak online fraude

In de brief van 30 november 2021 heeft mijn ambtsvoorganger de gewenste richting en de grote lijnen voor een integrale aanpak geschetst.[20] Op basis hiervan is in de afgelopen maanden gesproken met politie, Openbaar Ministerie, de bankensector, de telecomsector, VNO-NCW, vertegenwoordigers van consumenten en marktpartijen, fraudemeldpunten, stichtingen die slachtoffers helpen, Halt, het Verbond van Verzekeraars, relevante internetplatforms en kennisinstellingen (zie bijlage 1 voor het complete overzicht van betrokken partners). Uit die gesprekken is een grote gedeelde urgentie gebleken om intensiever en gerichter samen te werken op dit belangrijke dossier. Wij zijn alle partners zeer erkentelijk voor hun bijdrage.

De inspanningen binnen onze departementen ten behoeve van de parlementaire enquête Fraudebeleid hebben er helaas voor gezorgd dat de beschikbare capaciteit voor de ontwikkeling van de integrale aanpak lange tijd minder is geweest dan gehoopt. Inmiddels is extra capaciteit aangetrokken. Eén van de vraagstukken die de komende tijd met prioriteit aandacht krijgt, is gegevens- en informatie-uitwisseling. Ervaren knelpunten hierin zijn een rode draad gebleken in de gesprekken die we hebben gevoerd met onze partners. Dit is een complex onderwerp waar we goed moeten onderzoeken welke gegevensuitwisseling in de samenwerking binnen de huidige juridische kaders kan worden vormgegeven. Om goed in beeld te krijgen wat de partners nodig hebben en waar zij tegenaan lopen, gebruiken we de zomerperiode om een aantal gesprekken met partners te voeren. Verder organiseren we direct na de zomer een aantal overleggen, te beginnen met een bijeenkomst over cross-sectorale en sectorale gegevensuitwisseling specifiek in het kader van online fraude. Met deze bijeenkomst start een traject van expertsessies over dit onderwerp. Deze bijeenkomsten vinden plaats in afstemming met de PPS werkgroep cross-sectorale en sectorale gegevensdeling die reeds is gestart – onder andere in het kader van online fraude – en waarin praktijkervaring wordt uitgewisseld. Datzelfde geldt voor de verkenning met PPS-partners naar de vormgeving van een vragenloket, waar PPS partners voor juridische vragen over gegevensuitwisseling terecht kunnen. De integrale aanpak zal zorgen voor de verbinding en afstemming tussen deze initiatieven op dit onderwerp.

De verdere uitwerking van de integrale aanpak gebeurt op basis van de volgende uitgangspunten:
- de doelstelling is om met brede preventie en gerichte repressie een kentering aan te brengen in de stijging van online fraude;
- de echte aanpak gebeurt in alle initiatieven van verschillende partijen, waarvan een selectie in deze brief is opgenomen. De focus die de afzonderlijke initiatieven kenmerkt, is tenslotte bepalend voor het succes. Het is van belang dat de integrale aanpak deze – waar nodig en gewenst – versterkt zonder ze te compliceren;
- de integrale aanpak zorgt voor de ontmoeting op alle niveaus tussen de partners betrokken bij het tegengaan van online fraude en vormt daarmee een «platformfunctie»;
- de integrale aanpak doet recht aan de complexiteit van online fraude en biedt de flexibiliteit om snel te kunnen reageren op nieuwe ontwikkelingen;
- de structuur van de integrale aanpak is gericht op wat partners nodig hebben (met respect voor ieders rol en verantwoordelijkheid) en vermijdt overbodige overleggen;

[20] Kamerstuk 29 911, nr. 341.

– de integrale aanpak zorgt voor versterking in de breedte voor alle initiatieven, bijvoorbeeld door analyse en onderzoek naar effectiviteit en succesfactoren.

De integrale aanpak zal op grond van deze uitgangspunten zorgen voor:
– een flexibele structuur om overkoepelende vragen en nieuwe ontwikkelingen in werkgroepen te bespreken met geïnteresseerde partners (bijvoorbeeld verwerking persoonsgegevens en AVG);
– halfjaarlijkse bijeenkomsten voor bestuurders om ontwikkelingen, voortgang en knelpunten bij het tegengaan van online fraude op een inspirerende wijze te bespreken;
– een interdepartementale overlegstructuur om te zorgen voor een gecoördineerde inbreng vanuit de rijksoverheid;
– een projectteam dat vanuit het Ministerie van Justitie en Veiligheid zorgdraagt voor ondersteuning bij en uitvoering van de integrale aanpak;
– heldere aanspreekpunten bij projectteam en partners om vragen en voorstellen vanuit de verschillende initiatieven over en weer snel en adequaat te adresseren;
– ad hoc conferenties om nieuwe ontwikkelingen en onderzoeksresultaten te presenteren;
– heldere en gedeelde doelstellingen als fundament voor de integrale aanpak, waarin alle initiatieven een plaats krijgen en op basis waarvan uw Kamer periodiek geïnformeerd wordt;
– een onderzoeksprogramma voor online fraude.

Helaas heeft een geplande bijeenkomst van bestuurders van publieke en private partners op 28 juni 2022 niet kunnen plaatsvinden. Er wordt nu een nieuwe datum gezocht om deze aan het eind van de zomer te laten doorgaan. In deze bijeenkomst zal worden gesproken over de inrichting van de integrale aanpak, waaronder concretisering van afspraken op het gebied van samenwerking, governance en doelstellingen. De uitwerking en de duurzaamheid van de integrale aanpak staat met wat we samen kunnen bereiken en dus met het commitment van alle partijen. De komende maanden gaan we deze integrale aanpak vorm en inhoud geven met als basis de acties die al plaatsvinden.

Tot slot

Bovenstaande bestaande en nieuwe acties en de verdere invulling van de integrale aanpak bieden enerzijds een solide basis om online fraude effectief aan te pakken. Anderzijds zullen ze mogelijk leiden tot aanvullende initiatieven. Niet alleen nieuwe vormen van online fraude, maar ook de ervaring van succesvolle acties zullen ervoor zorgen dat de integrale aanpak zich verder zal ontwikkelen. Concreet valt bijvoorbeeld te denken aan betere voorlichting aan specifieke groepen burgers of een bredere publiekscampagne, verbreding van het inzicht in het fenomeen van online fraude door onderzoeken en ondersteuning van slachtoffers door de meldpuntstructuur verder te optimaliseren. Voor deze en andere aanvullende initiatieven, bovenop de uitgewerkte acties die in deze brief staan, is op dit moment geen financiële dekking voorhanden. Daarom zal bij de keuze voor en besluitvorming over aanvullende initiatieven telkens de budgettaire dekking en daarbij te maken keuzes meegewogen moeten worden. Wij sturen uw Kamer uiterlijk in januari 2023 de integrale aanpak online fraude toe, waarna de eerste jaarlijkse voortgangsrapportage in het najaar van 2023 volgt.

Wij kijken er met veel vertrouwen naar uit om de komende jaren samen te werken met alle partners om slachtofferschap van online fraude terug te dringen.

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius

De Minister van Financiën,
S.A.M. Kaag

De Minister van Economische Zaken en Klimaat,
M.A.M. Adriaansens

De Minister voor Rechtsbescherming,
F.M. Weerwind