Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2025–2026

29 911 Bestrijding georganiseerde criminaliteit

Nr. 511

BRIEF VAN DE MINISTERS VAN JUSTITIE EN VEILIGHEID EN VAN FINANCIËN EN VAN DE STAATSSECRETARIS VAN ECONOMISCHE ZAKEN EN KLIMAAT

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 3 juli 2026

Online fraude is een omvangrijk maatschappelijk probleem en is onder meer de snelst groeiende vorm van georganiseerde misdaad, in Nederland en in de EU.[1] Online fraude en cybercrime kunnen met behulp van technologieën steeds sneller en met grote aantallen slachtoffers tot gevolg gepleegd worden. Maar liefst 17 procent van de Nederlandse bevolking van 15 jaar en ouder is in 2025 slachtoffer geworden van een of meer online delicten of incidenten.[2] Dit betekent dat bijna 1 op de 5 Nederlanders te maken heeft gehad met vormen van digitale criminaliteit, variërend van phishing en hacken tot online fraude.

Om online fraude effectiever aan te pakken adviseren experts, waaronder Europol, vooral om meer samenwerking te realiseren tussen private en publieke organisaties die onderdeel zijn van de online fraudeketen.[3] Deze publiek-private samenwerking wordt in Nederland sinds 2022 concreet ingevuld met het programma voor de integrale aanpak online fraude. Het kabinet ziet deze samenwerking die met partners is opgebouwd als onmisbaar in de strijd tegen online fraude en is daarom ook opgenomen in het coalitieakkoord.[4]

Ter uitvoering daarvan heeft de Minister van Justitie en Veiligheid (JenV) middelen vrijgemaakt om de aanpak steviger en structureler te borgen. Allereerst zetten we de huidige integrale aanpak online fraude, die

[1] IOCTA 2026 – The evolving threat landscape: how encryption, proxies and AI are expanding cybercrime - Internet Organised Crime Threat Assessment (IOCTA) 2026 | Europol

[2] Veiligheidsmonitor 2025, CBS

[3] IOCTA 2026 – The evolving threat landscape: how encryption, proxies and AI are expanding cybercrime - Internet Organised Crime Threat Assessment (IOCTA) 2026 | Europol, zie ook Global-Fraud-Summit-Outcome-Documents-English.pdf

[4] Coalitieakkoord, 2026–2030: «we versterken de aanpak van online fraude, intensiveren publiek-private samenwerking, en werken aan betere preventie en ondersteuning van slachtoffers bij schadeafhandeling.»

kst-29911-511
ISSN 0921 - 7371
's-Gravenhage 2026

gefinancierd was tot eind 2027, voort tot en met 2029.[5] En werken we in die tijd aan een effectieve vorm van structurele borging. Dat is nodig, want online fraude zal niet verdwijnen. Voorts investeert de Minister van JenV aanzienlijk in uitbreiding van de opsporing online, met uitbreiding van de recherchecapaciteit bij de digi- en cyber opsporingsteams van de politie. Ook de succesvolle uitvoering van de pilot Anti Phishing Shield biedt een krachtige technische interventie die slachtoffers van malafide weblinks en advertenties op grote schaal kan voorkomen.

In deze brief informeren wij uw Kamer over de resultaten en plannen van de integrale aanpak online fraude, met het Actieplan 2026 en het jaarverslag over 2025. Beide zijn als bijlagen aan deze brief toegevoegd. We zijn trots op de concrete resultaten die zijn bereikt en de afspraken die we hebben gemaakt voor dit jaar. In de vooruit- als terugblik zullen wij, zoals uw Kamer heeft verzocht, bijzondere aandacht schenken aan de stappen die gezet worden om gegevensdeling tussen partners te bevorderen. Daarmee doet de Minister van JenV ook zijn toezegging gestand om uw Kamer in de bijgesloten voortgangsrapportage online fraude, ook te informeren over informatiedeling en wat er op dat onderwerp te doen staat.

Vervolgens gaan wij in op het proces om tot besluitvorming te komen over de structurele borging van de aanpak na 2029. Bij die borging staat voorop dat het onze samenwerking optimaal ondersteunt en ons daarmee in staat stelt online fraude zo effectief mogelijk te bestrijden. Inspiratie voor wijzen van samenwerking kunnen wij halen uit het voorbeelden van buitenlandse anti-fraudecentra. Door Deloitte is in opdracht van de Minister van JenV onderzoek uitgevoerd naar voorbeelden van anti-fraudecentra. Dit onderzoek is als bijlage gevoegd bij deze Kamerbrief. Hiermee doet de Minister van JenV zijn toezegging aan u gestand om de Kamer te informeren voor de zomer 2026 over de verkenning van de aanpak online fraude in andere landen en het ontwikkelen van een anti-fraudecentrum

Tot slot gaan wij in deze brief in op de uitvoering van motie Mutluer waarin wordt verzocht om voor de zomer expliciet uit te werken hoe kan worden toegewerkt naar één centraal meld- en registratiepunt voor online fraude en daarbij tevens mee te nemen welke wettelijke verplichtingsscenario's voor banken, telecombedrijven en onlineplatforms mogelijk zijn, inclusief de consequenties van niets doen. In het verlengde daarvan informeert de Minister van JenV u over de uitvoering van de motie Michon-Derkzen voor de doorontwikkeling van de Fraudehelpdesk en welke scenario's als realistisch worden gezien.

De Integrale Aanpak Online Fraude

Doelstelling en partners

Sinds 2022 werken publieke en private partijen samen in het programma de Integrale aanpak online fraude om het aantal slachtoffers van online fraude in Nederland te verminderen. Dat doen we in de eerste plaats door barrières op te werpen en interventies te plegen en door informatie en kennis met elkaar uit te wisselen om fraude zo snel mogelijk te stoppen. We vergroten de weerbaarheid van burgers en bedrijven, zorgen voor samenwerking rondom de aanpak van daders en ondersteuning van slachtoffers. Onder regie van het Ministerie van Justitie en Veiligheid stelt een kerngroep van partners bestaande uit VNONCW en MKB-Nederland,

[5] Voor 2026 en 2027 wordt het programma in belangrijke mate ondersteund door de Europese Commissie vanuit het Fonds voor Interne Veiligheid 2012–2027

de Nederlandse Vereniging van Banken (NVB), Consumentenbond, Vereniging Nederlandse Gemeenten (VNG), Politie, Openbaar Ministerie (OM), De Nederlandsche Bank, Veiliginternetten.nl, Fraudehelpdesk, COIN, Thuiswinkel.org, Ministerie van Economische Zaken en Klimaat (EZK), Ministerie van Financiën (Fin) en Ministerie van Justitie en Veiligheid (JenV), jaarlijks een actieplan vast. In totaal werken meer dan 50 partijen mee aan de realisatie van acties.

Actieplan 2026

In de bijlage bij deze brief treft uw Kamer het Actieplan voor het jaar 2026 aan. Het actieplan bevat de afgesproken resultaten op de zes lijnen van de integrale aanpak. Het actieplan van dit jaar staat in het teken van concrete resultaten en (uitproberen van) innovaties die de online fraudeketen in staat stellen om fraude zo veel mogelijk te voorkomen. Dat oefenen met pilots helpt ons in de ambitie om onze huidige publiek-private samenwerking te verstevigen. Tegelijkertijd geven de resultaten ons handvatten om keuzes te maken over de structurele samenwerking van de toekomst. Zo werken we dit jaar voor het eerst samen met een startup die privacy enhancing technology (PET) bouwt. Op pilot-basis gebruiken we deze technologie om real time modus operandi met elkaar te delen én te werken aan een laagdrempeligere meldvoorziening en ondersteuning voor slachtoffers. Op die laatste pilot gaan we later in deze brief in. Dat helpt de samenwerkingspartners op dit moment al om informatie met elkaar uit te wisselen en toe te passen in proefvorm, maar geeft ons na afronding ook informatie over hoe deze samenwerking structureel kan worden ingezet. Ook de wetenschappelijke proeftuin gegevensdeling (TNO-onderzoek) is een goed voorbeeld hiervan. Deze werpt nu al vruchten af door partijen samen te brengen om data-uitwisseling tegen fraude te bespreken. De uitkomsten van het onderzoek kunnen een belangrijke basis vormen voor toekomstige bestuurlijke besluiten over gegevensdeling.

Behaalde resultaten van 2025 en 2026

Uw Kamer is vorig jaar per brief geïnformeerd over het Actieplan 2025.[6] In 2025 en doorlopend in 2026 zijn er op de verschillende lijnen positieve resultaten behaald. Voor de resultaten van 2025 verwijzen wij u jaarbericht in de bijlage bij deze brief. Een aantal zaken lichten we graag uit.

Op het gebied van kennis en innovatie is in 2025 de website van de integrale aanpak uitgebouw tot een breed kennisplatform. Deze ontwikkeling loopt door in 2026. Verder is in november 2025 het dashboard www.zichtoponlinecriminaliteit.nl gelanceerd. Dit dashboard biedt lokale en landelijke partners inzicht in de omvang van online criminaliteit en dader-/slachtofferprofielen per regio en gemeente. In 2026 werken we aan de uitbreiding van databronnen voor dit product.

Voor de actielijn barrières en interventies zijn in 2025 en 2026 barrièremodellen[7] en criminal journeys[8] ontwikkeld of herijkt voor bankhelpdesk-, verkoop- en beleggingsfraude. Deze hebben geleid tot de selectie van preventieve interventies die getest worden bij deelnemende bedrijven. In

---

[6] Actieplan 2025 - Integrale aanpak online fraude | Rijksoverheid.nl

[7] *Een barrièremodel is bedoeld om (criminele) bedrijfsprocessen in beeld te brengen. Op basis van het barrièremodel wordt inzichtelijke welke barrières (keten)partners kunnen opwerpen tegen criminele activiteiten.*

[8] *Een criminal journey is bedoeld om inzicht te verkrijgen in de fraudeketen, waarbij de stappen om online fraude te plegen en ook de diensten, producten en infrastructuur die daarbij worden gebruikt (ofwel de dienstverleners en gelegenheden) in beeld worden gebracht.*

het actieplan van 2026 hebben we afspraken gemaakt over de verdere verspreiding van ontwikkelde interventies. Ook heeft 2025 laten zien dat het gezamenlijk ontwikkelen van interventies wetgeving kan inspireren. Zo heeft de interventie «Line Busy» die gericht is op het delen van gegevens tussen telecomaanbieders en banken om o.a. bankhelpdeskfraude tegen te gaan, er mede aan bijgedragen dat er aanpassingen gedaan worden in de Telecommunicatiewet om telecomaanbieders meer ruimte te bieden voor gegevensverwerking ten behoeve van fraudebestrijding. Dit kent samenhang met de Europese *Payment Services Regulation* (PSR) welke specifieke bepalingen bevat omtrent gegevensdeling tussen betaaldienstverleners en aanbieders van elektronische communicatiediensten.

In de actielijn weerbaarheid en preventie zijn zowel op slachtoffer- als daderpreventie resultaten geboekt. Via aanwezigheid op beurzen, zoals de Seniorenexpo, Echt Niet Vandaag en de Huishoudbeurs zijn grote aantallen potentiële slachtoffers bereikt met praktische tips en informatie om online fraude te herkennen. Ter ondersteuning van (potentiële) slachtoffers is vanuit de pijler «Hulp aan slachtoffers» in 2025 een folder ontwikkeld met praktische tips voor slachtoffers en verwijzing naar het juiste aanspreekpunt of hulp. Deze folder wordt op de verschillende beurzen verspreid en door de verschillende partners gebruikt op hun websites. Deze inzet wordt in 2026 voortgezet. Ten aanzien van daderpreventie heeft het Ministerie van Justitie en Veiligheid samen met partners dit jaar de podcast *De Ronselroute* gemaakt, gericht op ouders en jongerenwerkers om te voorkomen dat jongeren online de criminaliteit in worden getrokken, bijvoorbeeld door hun bankrekening uit te lenen aan een fraudeur. De podcast heeft inmiddels rond de 1,5 mln. impressies gekregen en is daarmee een belangrijke bijdrage aan daderpreventie voor online fraude.

Binnen de pijler opsporing en vervolging zijn belangrijke resultaten behaald nu de afspraken en doelstelling uit de Veiligheidsagenda 2025 ruimschoots zijn gerealiseerd.[9] In 2026 worden heeft de politie met nieuwe succesvolle initiatieven deze lijn voortgezet. Van deze initiatieven spreekt de campagne «Game Over?!» het meest tot de verbeelding, waar de politie in één keer honderd verdachten van oplichting heeft getoond om ze op te sporen.[10] Medio juni 2026 zijn van de honderd verdachten inmiddels zeventig herkend.

Tot slot zijn er in 2025 en in de eerste maanden van 2026 positieve resultaten geboekt voor de actielijn gegevensdeling. Conform de toezegging van de voormalig Minister JenV in het Commissiedebat online fraude van 17 december jl. (Kamerstuk 29 911, nr. 494) wordt uw Kamer hieronder in meer detail geïnformeerd over de stand van zaken in deze actielijn.[11]

Uitgelicht: Actielijn Gegevensdeling

De integrale aanpak richt zich op de vraag hoe de gegevensdeling in de samenwerking vorm kan krijgen en of aanvullende wetgeving nodig is. De partners van de integrale aanpak ervaren beperkingen om persoonsgegevens te delen voor het treffen van interventies en het doen van analyses op vormen van online fraude. Dit belemmert volgens hen de integrale samenwerking en een effectieve (preventieve) aanpak van online fraude. In het actieplan van 2026 zijn de volgende acties en resultaten opgenomen

[9] Veiligheidsagenda 2023–2026
[10] Raadpleegbaar op: Game Over?! | politie.nl
[11] Kamerstukken II, 2025–2026, TZ202512-065.

die inzichten moeten bieden voor de beantwoording van de vraag en daarmee bouwstenen zijn voor effectievere gegevensdeling:
– Inzicht in de huidige kaders: Wat zijn de mogelijkheden en onmogelijkheden van sectorale en cross-sectorale gegevensdeling? Hiervoor is een analyse uitgevoerd op de huidige juridische kaders. De hoofdpunten van deze analyse zijn als bijlage toegevoegd en hieronder kort toegelicht.[12]
– Onderzoek naar de meerwaarde van gegevensdeling: TNO draait een wetenschappelijke proeftuin met sectorale en cross-sectorale gegevensdeling. De centrale vraag daarbij is: wat kan die gegevensdeling opleveren?
– Ook is TNO gevraagd advies uit te brengen over de bruikbaarheid van privacy vriendelijke technologie (Privacy Enhancing Technology, PET). In het najaar wordt uw Kamer geïnformeerd over de uitkomsten van dit onderzoek.
– Het komen tot oplossingsrichtingen: Met de verworven kennis over de kaders, de onderzoeksresultaten van TNO en proeven van PET zullen na de zomer met de deelnemers oplossingsrichtingen worden verkend. Dit zijn oplossingen die binnen de huidige kaders al gerealiseerd kunnen worden alsook verdergaan, namelijk waar het gaat over cross-sectorale gegevensdeling.

De actie omtrent inzicht in huidige kaders is afgerond. De twee centrale vragen waren: 1) Wat zijn volgens het huidige kader de mogelijkheden en onmogelijkheden in gegevensdeling over online fraude? en 2) Met welke waarborgen voor een betrokkene over wie gegevens gedeeld worden, moet rekening worden gehouden bij gegevensdeling en welke voorbeelden zijn er in de praktijk te zien?

Voor de beantwoording van de eerste vraag over het juridisch kader en de gebruiksmogelijkheden voor gegevensdeling zijn er enkele belangrijke bevindingen:
– De analyse laat zien dat er een diversiteit is in nationale en internationale regelgeving voor de private en publieke organisaties die gegevens verwerken over online fraude. We zien met name de impact van de Europese regelgeving op gegevensdeling voor de financiële sector toenemen, met name door de Europese Payment Services Regulation die eerder in deze brief aan bod kwam.
  In het algemeen is de conclusie dat de mogelijkheden binnen de huidige kaders beperkt zijn en dat de mate van gegevensdeling verschilt per sector.
– Als het gaat om gegevens van strafrechtelijke aard, biedt de Uitvoeringswet AVG (UAVG) meerdere uitzonderingen. Een sectorale wet of een vergunning van de AP liggen dan het meest voor de hand. Het beleid van de Autoriteit Persoonsgegevens is voor de vergunningverlening sectoraal ingesteld en in principe niet cross-sectoraal. De banken en de verzekeraars beschikken als enige van de bij online fraude betrokken partijen over een vergunning van de Autoriteit Persoonsgegevens.
– Uit de analyse komt handelingsverlegenheid naar voren bij de beoordeling van bijvoorbeeld het gerechtvaardigd belang of het strafrechtelijk persoonsgegeven. Partijen vragen hier om een duidelijke grondslag of guidance.
– Private partijen geven aan knelpunten te ervaren in de gegevensdeling met de politie als er nog geen sprake is van een aangifte. Bijvoorbeeld in de onderzoeksfase en als er nog onvoldoende feiten voorhanden zijn, zijn private partijen terughoudend in het delen van gegevens met de politie zonder aangifte. Dit beeld komt overeen met bevindingen uit

[12] De complete analyse is raadpleegbaar op www.integraleaanpakonlinefraude.nl

een eerder gepubliceerd WODC-rapport over gegevensdeling met politie binnen publiek-private samenwerkingen.[13] Het verzoek om guidance in de uitvoering geldt ook voor bestaande samenwerkingsverbanden met de politie.

Voor de beantwoording van de tweede vraag over waarborgen van betrokkenen wordt uitgelicht dat waarborgen de betrokkene beschermen tegen onterechte maatregelen als gevolg van gegevensdeling zoals uitsluiting. In de praktijk zijn meerdere voorbeelden te zien van gegevensdeling met de nodige waarborgen zodat een betrokkene bijvoorbeeld is geïnformeerd, inzage krijgt, een aanspreekpunt krijgt en audits gehouden worden. Een andere vorm van waarborg is het toepassen van Privacy Enhanced Technology (PET).

De uitkomsten van de bovenstaande analyse in combinatie met de uitkomsten van het TNO-onderzoek leiden tot gezamenlijke reflectie en vervolgacties met partners. Met een aantal punten gaat de Minister van JenV direct aan de slag. De duidelijke vragen omtrent guidance en handelingsverlegenheid als gevolg van de interpretatie van de AVG, zal het Ministerie van JenV bespreken met de Autoriteit Persoonsgegevens. Daarnaast zal het Ministerie van JenV met de functionarissen voor gegevensbescherming van de sectoren in gesprek gaan en onderzoeken wat werkt om de hindernissen in gegevensdeling op te lossen.

Structurele borging van publiek-private samenwerking

Onze integrale samenwerking is erop gericht om gezamenlijk het meest effectieve antwoord te bieden in de aanpak van online fraude. De aanhoudende dreiging van online fraude vraagt om een toekomstbestendige organisatie van die samenwerking als logische vervolgstap op het huidige programma dat onder regie van het Ministerie van JenV is opgezet. Het bijgesloten door Deloitte uitgevoerde onderzoek naar internationale voorbeelden biedt inspiratie voor het gesprek met partners over de doorontwikkeling van de huidige integrale aanpak. In verschillende landen bestaan verschillende modaliteiten van samenwerking. Afgezien van de precieze organisatievorm is als gemene deler een aantal functionaliteiten te herkennen:
– een centrale, agenderende en aanjagende rol het bundelen van informatie en het opwerken naar actuele waarschuwingen
– opvang van meldingen van slachtoffers
– stroomlijning van doorverwijzing naar slachtofferhulp en compensatiemogelijkheden.

Samenwerking op deze en andere functionaliteiten van fraudebestrijding zijn op dit moment belegd bij het programma. Doel is om dit jaar met partners de structurele samenwerking vanaf 2029 voor te bereiden. De Minister van JenV heeft met de partners van de integrale aanpak afgesproken om in de komende maanden met stakeholders in gesprek te gaan. Over de verschillende scenario's waar wij aan denken, zal de Minister van JenV uw Kamer rond de jaarwisseling informeren. Daarin worden de resultaten op gegevensdeling zoals hierboven omschreven meegenomen. Een belangrijke component daarin is ook of en zo ja, welke financiering daarvoor naar schatting nodig is.

[13] *Dekker, R. Feys, Y, Glebbeek, M-L. Lindeman, J. Loyens, K (2025).* Met vereende krachten? Wetenschappelijk Onderzoek- en Documentatiecentrum.

Uitvoering motie Mutluer voor een centraal meld- en registratiepunt[14]

De uitvoering van de motie Mutluer bevat twee onderdelen. Samengevat gaat het om de vraag naar 1) een centraal meldpunt en 2) de mogelijkheid van wettelijke verplichtingsscenario's. Op beide onderdelen geeft de Minister van JenV een toelichting op de uitvoering.

Een centraal meld- en registratiepunt

Verzocht is om voor de zomer expliciet uit te werken hoe kan worden toegewerkt naar één centraal meld- en registratiepunt voor online fraude. Met uw Kamer is de Minister van JenV het eens dat goede ondersteuning van slachtoffers nadrukkelijk onderdeel van structurele samenwerking moet zijn. Omdat slachtofferschap van online fraude groot is, is hulp aan hen van belang of dit nu burgers of bedrijven zijn. Zoals geconstateerd werd in het WODC-evaluatieonderzoek naar de Fraudehelpdesk zijn er meer dan 50 meldpunten waar slachtoffers zich kunnen melden. In lijn met de motie Mutluer is een belangrijke vraag hoe het hulpaanbod voor slachtoffers overzichtelijker is te maken. Dat overzicht wil de Minister van JenV brengen door een duidelijke eerste ingang voor slachtoffers te verkennen. Een duidelijke eerste ingang en intake kan uitstel van een hulpvraag van of aangifte door slachtoffers voorkomen waardoor slachtoffers verstoken blijven van passende hulp en sporen en bewijs verloren gaan. De Minister van JenV start een onderzoek in de vorm van een pilot, die in de tweede helft van 2026 wordt uitgevoerd binnen het actieplan van de integrale aanpak. De Minister van JenV heeft de Fraudehelpdesk verzocht als landelijk opererende organisatie met specialistische kennis op het gebied van fraude en partner binnen de integrale aanpak om zich aan deze pilot te verbinden in een regisserende rol. De pilot wordt uitgevoerd in nauwe samenwerking met de meldpunten verbonden aan de integrale aanpak en gebruikt privacy enhanced technologie (PET) om het meldproces te stroomlijnen van eerste intake tot de gewenste hulp die door verschillende partijen geboden kan worden. Doel is om slachtoffers te ontlasten door te voorkomen dat ze meerdere keren hetzelfde moeten vertellen en om hen meer eigenaarschap en controle over hun melding en de te ontvangen hulp te geven. Doel en uitgangspunt van de Minister van JenV is niet om de bestaande publieke en private meldpunten samen te voegen. Volgens de werkgroep slachtofferhulp die onder de integrale aanpak is ingericht, met meldpunten en het CCV, is dat ook geen effectieve weg. De bestaande meldpunten hebben ieder waardevolle kennis en expertise, zoals de meldloketten bij de banken, die hulp bieden bij de vraag of geldtransacties gestorneerd kunnen worden of informatie bieden over schadeverhaal.

Afdwingbaarheid met wettelijke verplichtingsscenario's voor banken, telecombedrijven en onlineplatforms

Dit onderdeel van de motie betreken we bij de verdere uitwerking van structurele samenwerkingsvormen, zoals hiervoor benoemd. De huidige samenwerking binnen de integrale aanpak vindt plaats op vrijwillige basis. Geïnspireerd door voorbeelden van buitenlandse anti-fraudecentra uit de verkenning zal ik bij de toekomstscenario's ingaan op de vraag of, wanneer en hoe inzet van private partijen bij de aanpak van online fraude meer verplichtend moet en kan worden. Wij willen daarover eerst met de partners van de integrale aanpak in gesprek gaan, maar ook binnen het kabinet wordt overleg gevoerd over de verschillende verantwoordelijkheden van sectoren. Daarnaast speelt voor deze vraag nadrukkelijk de

[14] Kamerstukken II, 2025/2026, 29 911, nr. 496.

internationale en Europese component van juridische kaders mee. Deze vorm van criminaliteit is nadrukkelijk niet aan grenzen gebonden. Vanuit de Europese Unie zijn inmiddels verschillende verplichtingen gecreëerd om partijen in staat te stellen preventieve maatregelen te treffen, zoals de eerdergenoemde Payment Services Regulation en verplichtingen daartoe, zoals in de Digital Services Act. Onderwerp van gesprek en afweging zal dan ook nadrukkelijk zijn of, als verplichtingen inderdaad effectief lijken en of deze nationaal of vooral via de Europese band georganiseerd moeten worden. Voor dat laatste is relevant het op handen zijnde Actieplan van de Europese Commissie tegen online fraude.

Doorontwikkeling van de Fraudehelpdesk[15]

Ondersteuning van slachtoffers speelt een belangrijke rol in de aanpak van online fraude. Daar is onder meer de Fraudehelpdesk voor opgericht. Door mijn voorganger is toegezegd om uw Kamer te informeren over de doorontwikkeling van de Fraudehelpdesk en in te gaan op het WODC-evaluatieonderzoek naar de Fraudehelpdesk.[16] In het onderzoek dat in 2024 met uw Kamer is gedeeld, zijn in de beleidsreactie vier ontwikkelrichtingen toegelicht. Dit betreft: (i) voortzetting op de huidige wijze; (ii) stoppen; (iii) focus op trends en ontwikkelingen op het terrein van fraude (iv) ontwikkeling en uitbouw van de huidige dienstverlening gericht op het (praktisch) ondersteunen van slachtoffers en het bij elkaar brengen van informatie.

De Minister van JenV wil de doorontwikkeling van de Fraudehelpdesk meenemen in de in deze brief aangekondigde uitwerking hoe de aanpak van online fraude structureel is te borgen. Dat kan betekenen dat de Fraudehelpdesk een andere rol of positie krijgt of opgaat in een nieuwe organisatie of samenwerking. Die keuze is niet morgen gemaakt. In afwachting daarvan heeft de Fraudehelpdesk stabiliteit nodig qua financiering. Zoals bekend heeft de Fraudehelpdesk met een subsidietaakstelling van het vorige kabinet te maken, van bijna een kwart van het huidige budget. Deze taakstelling ga ik de komende drie jaar compenseren, zodat de Fraudehelpdesk voldoende middelen heeft om meldingen van fraude op te vangen. Daartoe vult de Minister van JenV de subsidie van de Fraudehelpdesk aan tot het huidige niveau van 1,2 miljoen.

Zoals door uw Kamer verzocht, gaat de Minister van JenV in op de toekomstscenario's die kansrijk worden geacht. De onderzoekers van het WODC constateerden dat de Fraudehelpdesk in de praktijk niet de centrale rol heeft die bij oprichting voor ogen stond. Ook constateerden ze dat het aan praktische hulp voor het slachtoffer ontbreekt, waardoor Fraudehelpdesk eerder een melddesk dan een helpdesk is. De Minister van JenV onderschrijft de bevinding dat als de Fraudehelpdesk haar dienstverlening op de huidige wijze voortzet, het een zekere maar lastig vast te stellen bijdrage levert aan de preventie van fraude en de ondersteuning van fraudeslachtoffers. Doorgaan op de ingeslagen weg (i) ziet de Minister daarom niet als gewenste uitkomst van de verkenning. De maatschappelijke toegevoegde waarde ziet de Minister voor de toekomst dus vooral in de laatste ontwikkellijn (iv), namelijk dat de Fraudehelpdesk zich voor de dienstverlening meer gaat richten op het (praktisch) ondersteunen van slachtoffers. In die richting heeft de Fraudehelpdesk de afgelopen tijd al een aantal stappen gezet, waaronder het ontwikkelen van een webformulier, waarmee slachtoffers 24/7 een noodadvies kunnen krijgen over stappen die zij kunnen nemen om verdere schade te voorkomen. Ook is de Fraudehelpdesk een samenwerking aangegaan met de politie om

[15] Kamerstukken II, 2024–2025, 36 600 VI, nr. 82
[16] Kamerstukken II, 2023–2024, 36 410 VI, nr. 23.

melders meteen ook aangifte te laten doen, zodat de politie in bepaalde gevallen ook over kan gaan tot inzet van interventies. Ondersteuning van slachtoffers wint gezien de schaal van online fraude aan belang. In een gedigitaliseerde maatschappij is het voor slachtoffers belangrijk om binnen het hulpaanbod terug te kunnen vallen op een persoonlijke bejegening en praktische ondersteuning bij het vinden en het daadwerkelijk ook snel verkrijgen van hulp. Nadrukkelijk is de verstrekte subsidie aan de Fraudehelpdesk ook bedoeld voor het bieden van (praktische) ondersteuning aan slachtoffers en melders van (online) fraude, zoals hulp bij het doen van aangifte of bij het verhalen van schade. Dit als versterking en aanvulling op hulp die andere partijen al bieden, zoals Slachtofferhulp Nederland die met subsidie van het Ministerie van JenV landelijk integrale dienstverlening biedt met o.a. psychosociale, praktische en juridische ondersteuning van slachtoffers van diverse vormen van criminaliteit, ook aan slachtoffers van (online) fraude.

Ook bleek uit het onderzoek naar meldpuntenlandschap dat de Fraudehelpdesk de enige organisatie is die zich richt op alle vormen van fraude en ook een overkoepelend beeld heeft van trends en ontwikkelingen op het terrein van fraude. Ketenpartners lieten in het onderzoek weten dat ze deze informatie nuttig achten, onder meer met het oog op preventie. Maar het alleen inzetten op deze derde ontwikkellijn (iii) ziet de Minister als te smalle basis voor de toekomst. Het enkel verzamelen van meldingen zonder vervolg helpt burgers te beperkt. De Minister ziet de bewerking en ontsluiting van informatie uit de meldingen dan ook niet als doel op zich, hoewel dit als secundair doel waardevol kan zijn. Wel heeft de politie mij laten weten dat de huidige rol van de Fraudehelpdesk als voorportaal voor de vele meldingen te waarderen, anders zouden al deze meldingen bij de politie terechtkomen. De Minister denkt daarom voor de toekomst eerder aan een situatie waarin het meldpunt kan opgaan in een nog te verkennen structurele samenwerking in de vorm van een anti-fraudecentrum dan wel een stevigere basis kan krijgen voor fraudespecifieke praktische ondersteuning van melders en slachtoffers.

Uitvoering verkenning

In reactie op de motie Michon en de subsidietaakstelling van het vorige kabinet heeft de Minister van JenV de Fraudehelpdesk gevraagd te verkennen of andere partijen bereid zouden zijn om taken te financieren. Het bestuur van Stichting Safecin heeft aangegeven dat haar verkennende gesprekken met stakeholders voor samenwerking en cofinanciering naar verwachting dit najaar (november) tot afronding komen. De voorlopige bevindingen benadrukken volgens de Fraudehelpdesk dat de maatschappelijke behoefte aan ondersteuning van slachtoffers van fraude, vroegtijdige signalering en effectieve samenwerking in de fraudeketen onverminderd groot is. Het aantal meldingen bij de Fraudehelpdesk is de afgelopen jaren sterk toegenomen en is ten opzichte van enkele jaren geleden verdubbeld. Deze groei wordt niet alleen veroorzaakt door een toename van het aantal slachtoffers, maar ook door de toenemende complexiteit van fraudezaken en de behoefte aan persoonlijke ondersteuning, hulp en doorverwijzing.

Slot

Een effectieve aanpak van online fraude samen met publieke en private partijen is een structurele noodzaak. Het kabinet investeert hier daarom

stevig in, door de continuering van de huidige integrale aanpak en het uitwerken van de beste structurele borging daarvan. Ook wordt de opsporing op dit terrein flink uitgebreid.

De Minister van Justitie en Veiligheid,
D.M. van Weel

De Minister van Financiën,
E. Heinen

De Staatssecretaris van Economische Zaken en Klimaat,
W.J.M. Aerdts