Ministerie van Justitie en Veiligheid

Jaarbericht
2025

Integrale aanpak
online fraude

Inhoudsopgave

Voorwoord 3
Lisette de Bie

Verbinding 4
Léon Poffé

‘We laten zien dat de integrale aanpak werkt’ 6
Julia Smeekes

‘Er moet echt een langetermijnaanpak komen’ 8
Medy van der Laan en Leendert-Jan Visser

Goed kijken waar gegevensdeling echt zinvol is 10
Leonore Duiker

Van 13 naar 55 partijen die meedoen 12
Kirstin de Jong en Kees aan de Wiel

Online dashboard biedt zicht op online criminaliteit 14
Annette van Delden

Voorwoord

Nog niet zo heel lang geleden bestond er nog niet zoiets als ‘online fraude’. Nu is het de meest voorkomende vorm van criminaliteit waar onze burgers en bedrijven mee te maken krijgen, zo blijkt uit CBS-onderzoek. De schade in harde cijfers is groot. Zo meldde de AFM recent dat slachtoffers van beleggingsfraude aangifte deden voor in totaal 75 miljoen euro schade. De werkelijke schade ligt waarschijnlijk veel hoger, omdat we weten dat lang niet ieder slachtoffer aangifte doet. En dat is één vorm van online fraude. Achter de cijfers gaan verhalen schuil van trauma’s, schaamte en persoonlijke ontwrichting. Onderzoek laat zien dat de emotionele impact van online slachtofferschap minstens even groot kan zijn dan bij traditionele criminaliteit, of zelfs groter.

Juist daarom is de integrale aanpak online fraude relevanter dan ooit. Online fraude raakt de hele keten, van de grote sociale platformen en webshops tot financiële dienstverleners, telecomproviders, opsporingsdiensten, OM en slachtofferzorg. Geen enkele partij kan online fraude zelf oplossen en dat besef is er ook in de politiek. Ik vind het positief dat de aanpak van online fraude en de publiek-private samenwerking erachter wordt benoemd in het coalitieakkoord van het nieuwe kabinet. De ambitie is om die aanpak te verstevigen en de samenwerking te intensiveren. Ik zie die als een duidelijke opdracht aan onszelf bij JenV en aan iedereen die bij de integrale aanpak is aangesloten. We moeten nog meer ambitie tonen, voor nog meer samenhang zorgen en vooral nog meer resultaten boeken. Dat het kán, laten de mooie resultaten zien die we al samen hebben geboekt en die in dit jaarbericht terugkomen.

Vorig jaar hebben we met onze partners in de kerngroep aangekondigd dat we de integrale aanpak doorontwikkelen. We bereiken al veel, maar we kunnen en moeten nog meer doen om effect te bereiken. De werkconferentie van eind december 2025 liet zien hoeveel energie en gedeeld urgentiebesef er bij de publieke en private partners van de integrale aanpak is.

In 2026 gaan we daarom flinke stappen zetten. Op basis van het nieuwe actieplan voor dit jaar (dat in de maak is), werken we aan cruciale thema’s. Zoals gegevensdeling, een taai, maar essentieel onderwerp. Met de proeftuin van TNO willen we scherp krijgen of nieuwe mogelijkheden voor gegevensdeling nodig zijn. Tegelijk willen we sneller kunnen handelen als online fraude zich verplaatst. En we verkennen, op basis van ervaringen in andere landen, de mogelijkheden en effectiviteit van een nationaal anti-fraudecentrum als basis voor delen van gegevens, coördinatie en aansturing van partijen, analyse en onderzoek etc.,

Kortom: 2026 wordt het jaar waarin we toewerken naar een structurele, gezamenlijke aanpak van online fraude. Een aanpak die ook overeind blijft mocht dit programma tot een eind komen. We mogen niet loslaten; daarvoor is de maatschappelijke impact van online fraude te groot.

Lisette de Bie
Plaatsvervangend directeur-generaal Rechtspleging en Rechtshandhaving, ministerie van JenV

Verbinding

Eind vorig jaar nam Léon Poffé afscheid als programmamanager voor de integrale aanpak. Met hem blikken we terug op de groei die deze integrale aanpak heeft doorgemaakt.

Toen Poffé in 2022 gevraagd werd of hij een programma voor de integrale aanpak van online fraude wilde leiden, hoefde hij niet lang na te denken: “Dat zag ik wel zitten, ja. Online fraude werd een steeds groter maatschappelijk probleem. En het was volstrekt helder dat je het probleem alleen kunt aanpakken door als publieke en private wereld samen te werken. De afgelopen 25 jaar heb ik allerlei opdrachten met partners buiten de overheid gedaan. Die ervaring kon ik goed inzetten. De uitdaging was dat de samenwerking op basis van vrijwilligheid moest plaatsvinden. Dit programma is er gekomen na politieke druk, waar weer druk achter zat van maatschappelijke organisaties. Zij zagen veel schade bij hun leden. Maar er zat geen wetgeving achter als stok achter de deur.”

Publiek-privaat samenwerken op basis van vrijwilligheid, dus. Hoe verliep dat?

“Het was belangrijk om een gezamenlijke start te maken. Iets bedenken op een ministerie en dat vervolgens opleggen, is nooit de beste weg naar succes. Al snel vormde zich een groepje organisaties die een belangrijke rol hebben in de aanpak van online fraude of die de belangen behartigen van maatschappelijke groeperingen vertegenwoordigen. Die partijen hebben we uitgenodigd voor een eerste bijeenkomst. We konden elkaar op inhoud vinden. Vervolgens zijn we gaan samenwerken op zes gezamenlijk gekozen thema’s. Onze partners wilden meteen aan de slag en dat heeft er onder andere toe geleid dat al heel snel een werkgroep gegevensdeling aan het werk ging, nog voordat er een kerngroep was.”

Merkte je dat partijen naar elkaar toe groeiden?
“Zeker. Door de samenwerking leerden partijen die altijd min of meer tegenover elkaar stonden, elkaar en elkaars positie kennen. Daardoor zag je beelden kantelen: dit doen jullie allemaal al en het is nog effectief ook. Dat heeft enorm geholpen in de samenwerking.”

Hoe kijk je terug op het werk op de zes thema’s?
“Als regievoerder hebben wij vanuit JenV nagedacht over een effectieve werkwijze. Die bleek op elk thema verschillend. Voor de kennisagenda was het relatief gesneden koek; je kijkt waar je extra kennis over wilt vergaren. Bij opsporing en vervolging hebben politie en OM private partners gevonden om naast strafrechtelijke opsporing en vervolging ook in te zetten op alternatieve interventies, zoals een aanpak via het civielrecht. Voor het thema gegevensdeling was de algemene teneur: JenV, geef ons nieuwe wettelijke grondslagen. Maar voordat je nieuwe wetgeving maakt, moet je eerst van alles geprobeerd hebben om aan te kunnen tonen dat het zonder wet niet lukt. Daarvoor hebben we een methodiek uitgewerkt om te komen tot oplossingen per knelpunt, met als uiterste mogelijkheid een nieuwe wet. In de actielijn barrières en interventies hebben de NVB en EY als trekkers fantastisch werk geleverd, met mooie gezamenlijke trajecten die al succesvolle interventies hebben opgeleverd. Op het thema preventie en weerbaarheid kwamen we er al snel achter dat er al veel goed lopende projecten en methodes waren. Daar hebben vooral ingezet op het beter bij elkaar brengen van vraag en aanbod. Bij hulp aan slachtoffers hebben we ervoor gekozen om alle organisaties waar slachtoffers zich melden, aan tafel uit te nodigen. Daar is het doel vooral om ervoor te zorgen dat slachtoffers door alle instanties de goede informatie krijgen en dat partijen hen doorverwijzen naar de juiste instanties.”

Het is begin 2026. Waar zijn de volgende stappen?
“In de kerngroep wordt nu het gesprek gevoerd over hoe de samenwerking in de toekomst bestendigd kan worden. Voor de regierol wordt daarvoor gekeken naar JenV. Verder is er een breed gedeelde wens om partijen te kunnen verplichten om afspraken na te komen. Dat kan bijvoorbeeld op basis van een convenant zijn. De ring van betrokken partners is veel groter geworden en dat heeft ook aandacht nodig. De focus moet blijven op inhoud en je hebt niet voor elk thema alle partners nodig. Om de samenwerking behapbaar te houden, werken we daarnaast aan de doorontwikkeling van onze online samenwerkingsruimte.”

Als je één ding mag noemen, wat is jouw grootste wens voor de toekomst?
“Dit programma loopt vooralsnog nog enkele jaren. Ik zie graag dat de integrale aanpak belegd wordt in één organisatie die alle publieke en private partijen met elkaar verbindt. JenV laat vergelijkend onderzoek doen naar landen die al gewend zijn om zo te werken.”

Terugkijkend: waar ben je het meest trots op?
“Dat de partners blij zijn met elkaar in deze samenwerking. En dat we zoveel nieuwe partijen en bevlogen professionals bij elkaar hebben weten te brengen die allemaal stappen extra zetten om online fraude effectiever aan te pakken. Iedereen is echt intrinsiek gemotiveerd. Deze aanpak wérkt.”

“Een gezamenlijke start was belangrijk.”

Programmamanager Julia Smeekes:

‘We laten zien dat de integrale aanpak werkt’

Met Julia Smeekes heeft de integrale aanpak een bekend gezicht als nieuwe programmamanager gekregen. Tot voor kort leidde zij de actielijn Hulp aan slachtoffers en draaide zij een project om inzicht te krijgen in wat er moet gebeuren om succesvolle interventies binnen de integrale aanpak breder geïmplementeerd te krijgen. Julia is blij met de groei die het programma heeft doorgemaakt. En ze kijkt uit naar de komende twee jaar: met meer en breder geïmplementeerde interventies in aantocht én belangrijke stappen rond gegevensdeling.

Smeekes heeft de integrale aanpak in een paar jaar tijd zien uitgroeien tot een samenwerking waarin een groeiend aantal partijen elkaar weet te vinden: “En er komen nog steeds nieuwe partijen bij. Tijdens de werkconferentie afgelopen december heb ik veel mensen gesproken van partijen die ik nog niet eerder had gesproken. Onder hen zijn veel webwinkels die aansluiten. Alle partijen in de fraudeketen hebben we hard nodig om de aanpak aan te scherpen en te blijven voeden met nieuwe ideeën.”

Hoe verklaar je die groei van het aantal aangesloten partijen?
“We laten zien dat de integrale aanpak werkt. De samenwerking leidt tot succesvolle acties en die wekken vertrouwen bij andere partijen. Maar het zit ook in de manier waarop we werken. We hebben een vrij compacte kerngroep, maar de oplossingen liggen meer dan eens in handen van partijen die daar niet in zitten. Per uitdaging proberen we de juiste partijen erbij te trekken. Wat verder meespeelt, is dat onderwerp online fraude inmiddels veel aandacht krijgt; ook in de politiek. Waar het niet zo lang geleden als zij-onderwerp van cybercriminaliteit werd gezien, is dat nu echt anders. Afgelopen zomer hebben we een gesprek met de Tweede Kamer gehad dat alleen maar over online fraude ging.” Het sterkt enorm dat onze publiek private samenwerking nu onderdeel is van het regeerakkoord.

Het programma is verlengd tot eind 2027, mede dankzij Europese subsidie. Waar zet jij de komende twee jaar op in?
“Allereerst: er liggen nu mooie interventies die we samen met elkaar hebben gecreëerd. Die hebben een potentieel dat we nog breder kunnen benutten. En we bedenken nieuwe interventies met elkaar. Ook rond gegevensdeling zijn er belangrijke stappen gezet die op het punt staan om vrijgegeven te worden. Daarmee kunnen we de samenwerking de komende periode een extra zet in de rug geven. Maar ik zie de resultaten uit ons actieplan ook als bouwstenen voor de vraag: hoe moeten we de aanpak van online fraude structureel inrichten?”

Tipje van de sluier?
“Er zijn verschillende scenario’s denkbaar. We zouden de huidige samenwerking op een aantal onderdelen kunnen aanpassen, zodat er een structureel netwerk ontstaat. Een ander scenario is de inrichting van een nieuwe organisatie. Concreet wordt onderzocht of de inrichting van een nationaal anti-fraudecentrum de aanpak van online fraude mogelijk effectiever kan maken en welke randvoorwaarden daarbij horen.”

Je bent net begonnen als programmamanager? Bevalt het?
“Zeker. Ik vind het mooi om samen slimme samenwerkingsvormen te bouwen en om partijen te verbinden aan een gezamenlijk perspectief. Online fraude gaat niet weg en het aanpakken van dit maatschappelijke probleem is een enorme drijfveer voor mij. Ik ben ook wel iemand die scherp kijkt naar resultaten. Ik heb heel veel zin in de komende periode.”

“De samenwerking leidt tot succesvolle acties en die wekken vertrouwen bij andere partijen.”

‘Er moet echt een langetermijnaanpak komen’

De Nederlandse Vereniging van Banken, VNO-NCW en MKB-Nederland staan aan de wieg van de integrale aanpak. In een interview vertellen Medy van der Laan (voorzitter Nederlandse Vereniging van Banken) en Leendert-Jan Visser (algemeen directeur MKB-Nederland) waarom structurele samenwerking nodig is: “Dit programma is eindig, maar online criminaliteit is dat niet.”

Waarom hebben de NVB, MKB-Nederland en VNO-NCW destijds het initiatief genomen voor de integrale aanpak?

Van der Laan: “Daar waren meerdere redenen voor. Allereerst maatschappelijke betrokkenheid: we zagen dat veel mensen trauma’s opliepen doordat ze werden opgelicht door criminelen die zich als bank voordeden. Daarnaast was er voor ons een financiële prikkel: doordat banken uit coulance schade door bankhelpdeskfraude vergoeden, was de schadelast groot. We hebben veel geld en menskracht geïnvesteerd in maatregelen, zoals een tijdslot bij het overboeken van geld van spaarrekening naar betaalrekening of het verhogen van limieten. Denk ook aan bewustwordingscampagnes en aan waarschuwingen in apps van banken. Maar we zagen ook dat we andere partijen nodig hebben om online criminaliteit echt goed aan te pakken.”

Visser: “Online criminaliteit is inmiddels de grootste vorm van criminaliteit en de schade voor ondernemers is enorm. Bedrijven kunnen erdoor stilvallen. Jaren geleden begonnen we heel praktisch met tips voor ondernemers over hoe zij hun weerbaarheid konden vergroten, welke afspraken je moet maken met IT-leveranciers en hoe je scheidingen tussen systemen aanbrengt. Maar we zagen al snel dat we ook andere stakeholders nodig hadden, waaronder de banken en de overheid.”

Medy van der Laan

Leendert-Jan Visser

Waarom moeten partijen meer doen dan maatregelen binnen hun eigen organisatie of sector?

Van der Laan: “Banken werpen barrières op om hun klanten te beschermen, maar als criminelen klanten overhalen om geld over te maken, is het meestal al te laat. Juist daarom is het zo belangrijk om met alle partners in de fraudeketen, dus zowel politie als banken, Consumentenbond, telecomsector, internetproviders en socialemediabedrijven, samen te kijken naar maatregelen om criminelen eerder tijdens hun ‘criminele reis’ dwars te zitten.”
Visser: “We hebben niet met hobbyisten te maken, maar met goed georganiseerde netwerken die ook geavanceerde AI inzetten. De trucs zijn zo verfijnd dat ik heel goed begrijp dat mensen slachtoffer worden. We moeten daar een goed georganiseerd netwerk tegenover zetten.”

Waar loopt de gezamenlijke aanpak het vaakst vast?

Visser: “Gegevensdeling. Het is raar dat een ondernemer die een crimineel opspoort diens naam niet mag doorgeven aan collega-ondernemers, omdat het botst met de privacywetgeving. In de praktijk maakt dat de ketenaanpak traag en minder effectief.”
Van der Laan: “Helemaal eens. Er moet meer mogelijk zijn dan alleen het delen van modus operandi of algemene daderprofielen. Als je als bank weet dat iemand verkeerde dingen aan het doen is, moet je andere partijen kunnen waarschuwen. Ook voor slachtoffers is het frustrerend: zij moeten dezelfde informatie steeds opnieuw doorgeven aan partijen. Ik vind dat storend; dat moet echt anders kunnen.”
Visser: “Privacy is belangrijk, maar de behoefte van alle partijen in de keten is helder: creëer de waarborgen die het mogelijk maken om cruciale gegevens te delen. Poortwachters zoals banken, notarissen, verzekeraars en accountants moeten alarmbellen zo hard kunnen laten rinkelen dat iedereen ze hoort en criminelen geweerd kunnen worden.”

Welke schakels geven nog te weinig thuis?

Van der Laan: “Socialemediabedrijven zijn nog te vaak afwezig aan tafel. Juist op hun platforms beginnen *criminal journeys* vaak. Ik vind dat zij hun verantwoordelijkheid kunnen nemen. Denk bijvoorbeeld aan preventie richting kwetsbare groepen die veel informatie online zetten. Ik nodig hen graag uit om mee te doen en samen slimme maatregelen te bedenken zonder dat die permanent veel tijd vergen.”
Visser: “De private sector is al heel ver. Ik zie graag dat de overheid tandjes erbij zet en online criminaliteit hogere prioriteit geeft als beleidsthema.”

De integrale aanpak loopt nu een paar jaar. Zijn jullie tevreden over de resultaten tot nu toe?

Visser: “Ik ben tevreden met de samenwerking die staat. Maar het fundament is nog dun. Zo wordt de financiering van jaar tot jaar vastgesteld en heeft de samenwerking nog een hoog pilotgehalte. Dit programma is eindig, maar online criminaliteit is dat niet. Er moet echt een langetermijnaanpak komen.”
Van der Laan: “Het afgelopen jaar was van doorslaggevend belang voor de integrale aanpak. Waar eerdere jaren voornamelijk gericht waren op het opbouwen van vertrouwen, het uitvoeren van onderzoek en het versterken van het netwerk, is in 2025 de overstap gemaakt van denken naar doen. Een mooi voorbeeld vind ik Line Busy waardoor banken straks bij telecomaanbieders kunnen checken of klanten in gesprek zijn tijdens het overboeken van geld.”

Wat mag er in de langetermijnaanpak van online fraude niet ontbreken?

Van der Laan: “Ik zie graag dat er over twee jaar een nationaal anti-fraudecentrum is ingericht waar publieke en private partijen onder één dak samenwerken. Zij moeten voldoende bevoegdheden krijgen om proactief gegevens te delen, zodat zij veel sneller kunnen ingrijpen. De Autoriteit Persoonsgegevens heeft al aangegeven beschikbaar te zijn om te kijken hoe dat kan. Met een centrum onder één dak kan het ook makkelijker zijn om waarborgen te creëren.”
Visser: “Ik ben ook een groot voorstander van één plek waar alle kennis en expertise samenkomen. Zo’n centrum kan ook direct nieuwe vormen van online fraude detecteren en dit doorgeven aan iedereen die risico loopt. Dat zou een grote stap vooruit zijn.”

Goed kijken waar gegevensdeling echt zinvol is

In de aanpak van online fraude worden de beperkte mogelijkheden tot gegevensdeling vaak als groot knelpunt genoemd. In samenwerking met de private en publieke partners van het programma worden in de actielijn gegevensdeling de kaders en de noodzaak van gegevensdeling binnen en tussen sectoren onderzocht. Leonore Duiker, privacy-adviseur bij het Ministerie van JenV en trekker van de actielijn, praat ons bij over de stand van zaken.

In oktober 2025 gaf de Autoriteit Persoonsgegevens aan positief te staan tegenover onderzoek door TNO naar de effectiviteit van gegevensdeling in de aanpak van online fraude. Daarmee werd voldaan aan de nadrukkelijke wens van verschillende partijen om bevestiging van de AP te krijgen.

Juridische kaders

Eind 2025 is het concept van de analyse van de huidige juridische kaders rond gegevensdeling opgeleverd. Deze ligt nu voor review bij juristen, fraude-experts en ICT-experts van banken, politie en de betrokken ministeries. “Het is een feitelijke beschrijving aan de hand van casuïstiek bij 15 organisaties uit verschillende sectoren: wat zijn de mogelijkheden en onmogelijkheden? De analyse bevestigt dat de verschillende kaders niet goed op elkaar aansluiten, maar dat er binnen sectoren beperkte mogelijkheden zijn om gegevens te delen. Als je grootschaliger *privacy-enhanced* technologie wilt toepassen, bijvoorbeeld gericht op de inzet van verdachte apparaten, dan zegt de AVG dat daarvoor aparte wetgeving nodig is. In het Verenigd Koninkrijk is die wetgeving er, maar in Nederland niet.”

Uit de conceptanalyse kwam ook naar voren dat organisaties vaak geneigd zijn het zekere voor het onzekere te nemen. Terwijl er, mits goed onderbouwd, wel degelijk mogelijkheden voor gegevensdeling zijn. “Het zou goed zijn als er wat meer houvast komt, bijvoorbeeld door richtlijnen van de AP. Er is ruimte, maar de praktijk kan wel wat hulp bij de uitvoering van de regels gebruiken.”

PSR en Telecommunicatiewet

Ondertussen zijn er ontwikkelingen op wetgevingsgebied. De Payment Service Regulation (PSR) vanuit Brussel legt de basis voor financiële dienstverleners binnen de EU om straks fraudegegevens onderling te delen. “De PSR gaat echt een stap verder dan wat nu kan, legt Duiker uit: “Banken kunnen nu via het externe verwijsregister beperkt fraudegegevens met elkaar delen, maar PSR biedt ruimere mogelijkheden.”

Ook de Telecommunicatiewet wordt aangepast. De minister (van EZK) heeft aangekondigd deze wet aan te passen voor het delen van verkeersgegevens voor de bestrijding van online fraude, nog niet bekend is hoe de wijziging eruit komt te zien. “De gegevens die KPN heeft, zijn interessant voor banken, maar bijvoorbeeld ook voor webshops. Op grond van de huidige wet mogen verkeersgegevens niet gedeeld worden.”

Oplossingsscenario’s

De centrale vraag blijft volgens Duiker: waar ligt de noodzaak van gegevensdeling en hoe is voor een betrokkene wiens gegevens worden gedeeld, gewaarborgd?
Het komend jaar moet alles samenvallen, hoopt Duiker: “Ik verwacht dat we dit jaar oplossingsscenario’s in beeld krijgen en daar samen het gesprek over kunnen voeren. We moeten weten wanneer gegevensdeling duidelijk zin heeft en welk beleid nodig is om dat mogelijk te maken. Vervolgens kan de minister daarover een besluit nemen en dit voorleggen aan de Tweede Kamer. Ik hoop dat het TNO-onderzoek ons meer informatie geeft over waar winst te behalen is door samenwerking.”

Van 13 naar 55 partijen die meedoen

Een groeiend publiek-privaat netwerk werpt samen barrières op en ontwerpt interventies tegen online fraude. Kirstin de Jong (Nederlandse Vereniging van Banken) en Kees aan de Wiel (EY Forensic & Integrity Services) maken de balans op na tweeënhalf jaarbouwen, ontwikkelen en implementeren.

De actielijn technische barrières en interventies startte onder leiding van De Jong (projectleider van dit thema) en met ondersteuning vanuit EY Forensic & Integrity Services in de zomer van 2023 met de aanpak van bankhelpdeskfraude. In werksessies werd de *criminal journey* van de fraudeur in kaart gebracht en een barrièremodel ontwikkeld: op welke plekken in het fraudeproces kunnen er barrières worden opgeworpen? Vervolgens hebben de partijen gewerkt aan interventies. Dat gebeurde toen met 13 partijen. Inmiddels is het netwerk uitgegroeid tot 55 partners. En wat volgens Kirstin de Jong opvalt: “We zien nu dat partijen zelfs vrijwillig naar ons toekomen om te vragen of ze kunnen deelnemen.”

Scope verbreed

Na bankhelpdeskfraude werd de scope verbreed naar aan- en verkoopfraude en beleggingsfraude. De aanpak is dezelfde gebleven: eerst de *criminal journey* en het barrièremodel opstellen, daarna interventies definiëren én uitwerken. De Jong licht toe: “Inmiddels is een nieuwe fase gestart, waarin de gemaakte modellen voor de vier thema’s worden herijkt. Onderdeel hiervan is dat de partijen ieder kwartaal bijeenkomen om trends en ontwikkelingen te delen en de voortgang van de maatregelen te monitoren. Deze werkwijze is zeer effectief gebleken''
Ze merkt daarbij op dat banken pas laat in de ‘criminal journey’ voorkomen en kunnen ingrijpen, terwijl andere partijen eerder in het proces maatregelen kunnen nemen. ‘’Zo voorkom je dat de fraudeur überhaupt in contact komt met een potentieel slachtoffer.’’

Een voorbeeld van een effectieve interventie in de keten van aankoopfraude is dat het Landelijk Meldpunt Internetoplichting door SIDN als *trusted flagger* is aangewezen. “Dat betekent dat frauduleuze websites veel sneller offline gaan”, zegt De Jong. Bij beleggingsfraude pakt de Autoriteit Financiële Markten (AFM) boilerrooms actief aan, haalt deze samen met banken en cryptoaanbieders sneller offline en plaatst ze op de waarschuwingslijst.

Kirstin de Jong

Line busy

Gegevensdeling is nog een knelpunt. “Daar lopen we inderdaad tegenaan”, erkent De Jong: “Veel interventies die de partners in gezamenlijkheid definiëren, blijven liggen omdat partijen bepaalde gegevens niet gericht mogen delen. Een voorbeeld van een geselecteerde maatregel is line busy, een koppeling tussen bank en telecomprovider om te kunnen checken of een klant tijdens een overboeking aan het bellen is. Dat is een belangrijke fraude-indicator. We zien graag dat banken de betaling in dat geval mogen blokkeren, maar dat kan nu nog niet. Er wordt nu, mede dankzij de gezamenlijke lobby met de telecompartijen vanuit de integrale aanpak, gewerkt aan een wetsvoorstel om de interventie mogelijk te maken.”

Kees aan de Wiel

Ondertussen zijn er twintig veelbelovende interventies geselecteerd om online fraude te verstoren. Elk kwartaal komen de partijen in vertrouwelijke herijkingssessies bijeen om trends te delen en verder te werken aan interventies. Voor iedere interventie is een projectleider aangewezen. “Het blijft een vrijwillige samenwerking, maar deelname is ook weer niet vrijblijvend”, stelt Aan de Wiel: “Tijdens de herijkingssessies worden partijen wel gewezen op hun verantwoordelijkheid om voortgang te boeken.”

Nationaal Anti-Fraudecentrum

Alleen al de interventies rond bankhelpdeskfraude laten zien dat de aanpak succesvol is. “Maar”, waarschuwt Aan de Wiel: “online fraude beweegt zich als water. Als je maatregelen neemt tegen de ene vorm van online fraude, verplaatsen fraudeurs hun terrein naar andere vormen.” In de doorontwikkeling van de integrale aanpak zou de komst van een Nationaal Anti-Fraudecentrum dan ook een goede stap zijn, vindt hij: “Eén plek waar partijen expertise bundelen en proeftrajecten kunnen doen en gericht en rechtmatig gegevens kunnen uitwisselen, daar is grote behoefte aan.”

En dan zijn er nog partijen die ontbreken in de samenwerking. De Jong noemt socialemediabedrijven en digitale platformaanbieders als grote afwezigen: “Juist die partijen zijn in staat om aan het begin van de *criminal journey* maatregelen te nemen tegen bijvoorbeeld frauduleuze advertenties die fraudeurs anoniem kunnen plaatsen.”

Morele verantwoordelijkheid

Tot nu toe is het lastig om deze partijen aan tafel te krijgen, erkent ze. Dat speelt niet alleen in Nederland, maar ook in andere Europese landen. Daarom wordt er gewerkt om via Europese initiatieven om socialemediabedrijven en big tech aan te spreken op hun morele verantwoordelijkheid. Ze roept de sociale mediabedrijven en digitale platformaanbieders daarom op om zich aan te sluiten bij het netwerk.

Online dashboard biedt zicht op online criminaliteit

Op 4 november 2025 ging het online dashboard Zicht op online criminaliteit live. Dit is een openbare website met landelijke en regionale inzichten over online criminaliteit. Annette van Delden is namens ICTU de product owner van het dashboard, waarvoor de ministeries van JenV en BZK samen opdrachtgever zijn. Zij vertelt wat gemeenten, veiligheidsnetwerken en andere ketenpartners ermee kunnen.

“Het dashboard is een startpunt om een eerste beeld te vormen van online criminaliteit in een gemeente of regio”, legt Van Delden uit. “Het geeft een goed beeld van wat er speelt en je kunt zien hoe een bepaalde gemeente of regio het doet vergeleken met het landelijke beeld.”
Ze werkte lange tijd aan Zicht op ondermijning, een omvangrijk online platform dat met data en indicatoren bestuurlijke risico’s helpt te duiden. “Het begon met een idee dat we met behulp van CBS-data agile hebben uitgebouwd naar een dashboard.”

Die ‘Zicht op-werkwijze’ is voor bijna elke maatschappelijke opgave toe te passen, ontdekte ze. Zo kwam er ook een dashboard met inzichten over de aanpak van ondermijning en andere problemen op vakantieparken. En vorig jaar werd besloten ook een dashboard voor online criminaliteit te bouwen: “Dit thema was eerst ondergebracht bij het dashboard over ondermijning, maar we ontdekten gaandeweg dat het op zichzelf moet staan. Het is overigens iets breder dan online fraude alleen, omdat ook statistieken van cybercriminaliteit erin zijn opgenomen.”

Van Delden is blij met de divers samengestelde en zeer actieve groep stakeholders die aan het dashboard heeft bijgedragen. “In het begin hebben we samen met hen een lijst met onderzoeksvragen opgesteld en geprioriteerd. Daarnaast komen we elke maand een uurtje online bij elkaar om de voortgang met onderzoeken en andere wensen voor het dashboard te bespreken. Waar nodig wordt de lijst aangescherpt of

aangevuld. We proberen het dashboard aan te laten sluiten op de wensen vanuit de praktijk in plaats van dat we zelf verzinnen wat erin moet komen."

Data van CBS

Het dashboard wordt voor het grootste deel gevoed door data die het CBS al heeft, zoals politiedata over daderschap en type delict en de Veiligheidsmonitor voor gegevens over slachtofferschap. Ook andere databronnen kunnen in het dashboard worden ingeladen. Van Delden noemt een voorbeeld: "We zijn nu bezig met een onderzoek waarmee we daders op wel 130 kenmerken kunnen onderscheiden. En we kijken of we via het CBS ook geanonimiseerde data van de Fraudehelpdesk en het Landelijk Meldpunt Internetoplichting erbij kunnen krijgen. Op grond van de CBS-wet kunnen we voor onderzoek veel gegevens van het CBS gebruiken, zolang ze niet herleidbaar zijn naar een individu of een bedrijf."

Een voorbeeld van een andere databron komt van het WODC, dat periodiek onderzoek doet naar online criminaliteit door jongeren. "Dat zijn representatieve enquêtes op basis waarvan je kunt zien hoe online criminaliteit zich over Nederland verspreidt. De gegevens uit die bron laten weer andere patronen zien dan die uit politiedata. Voor ketenpartners is dat waardevol, omdat er simpelweg niet zo vaak aangifte van online fraude wordt gedaan."

Positieve feedback

Van Delden benadrukt dat het om een eerste versie gaat: "We zijn nog lang niet klaar met vullen, maar we krijgen al positieve feedback. Lokale en regionale overheden, maar ook landelijke stakeholders, vinden het fijn dat er nu één plek is waar lokale en regionale statistieken over online fraude openbaar beschikbaar zijn."

Na een goede start doemt onvermijdelijk de vraag op waar het dashboard landt als de integrale aanpak stopt. "Het liefst wil je natuurlijk dat het dashboard zich blijft ontwikkelen dankzij een actieve groep stakeholders. En dat er voor gemeenten, veiligheidsnetwerken en andere ketenpartners een structurele informatiebron blijft waarmee ze gericht beleid kunnen sturen."

www.zichtoponlinecriminaliteit.nl

Dit is een uitgave van:
Ministerie van Justitie en Veiligheid
Integrale aanpak online fraude

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag

Voor meer informatie:
integraleaanpakonlinefraude@minjenv.nl
integraleaanpakonlinefraude.nl

Mei 2026

Integrale aanpak
online fraude