PARLEMENT & WETENSCHAP

Preventie van onlinefraude, lessen uit het buitenland

21 mei 2025 | prof. dr. Marianne Junger (Universiteit Twente), Ken Palla MBA, ing. Wiebe Fokma, prof. dr. ir. Bernard Veldkamp (Universiteit Twente)[1]

Dankwoord. De auteurs zijn Sandra Peaston (Cifas, UK), Henriëtte Bongers (Fraudehelpdesk) en Peter Hagenaars (Nationale Politie) erkentelijk voor hun adviezen en informatie.

Leeswijzer:
- De cijfers tussen [blokhaken] verwijzen (linken) naar de bronnen, in de laatste paragraaf.
- De aanduiding (§0) – paragraafteken + cijfer tussen haakjes – verwijst (linkt) naar een (sub)paragraaf.

Samenvatting

In Nederland is onlinefraude inmiddels het meest voorkomende delict onder de veelvoorkomende (offline en online)criminaliteit: een derde van alle incidenten is onlinefraude [1]. Met de mogelijkheden van AI en deepfake zullen de frauduleuze praktijken waarschijnlijk alleen maar toenemen [2, 3] (§2).

Als gevolg van de toename van onlinecriminaliteit verandert er veel voor politie en justitie: wij beschrijven twee belangrijke ontwikkelingen: 1) De relatie tussen publieke en private partijen verandert: er wordt steeds meer geregistreerd en bestreden door private partijen. 2) Opsporen wordt steeds moeilijker door de enorme omvang van het aantal incidenten, de complexiteit van de delicten en het gegeven dat de daders regelmatig in het buitenland zijn. De politie doet hierdoor relatief minder aan opsporing, maar is wel steeds meer betrokken bij preventieve activiteiten, zoals eraan bijdragen dat frauduleuze websites offline worden gehaald. De politie kan ook van cruciaal belang zijn bij het terugvorderen van geld, vooral van cryptocurrency-uitwisselingen (§1).

Hierdoor neemt de noodzaak van preventie toe. Gelukkig zijn er tal van mogelijkheden om incidenten vroegtijdig op te sporen en om wegen voor fraudeurs af te snijden. Preventieve maatregelen zijn vaak zeer succesvol. Dit blijkt ook uit het feit dat bedrijven steeds meer preventieve maatregelen nemen en dat, vermoedelijk als gevolg hiervan, slachtofferschap van cybercriminaliteit

[1] Marianne Junger is emeritus hoogleraar Cybersecurity aan Universiteit Twente. Zij is gespecialiseerd in onderzoek naar onlinefraude, naar *social engineering* en cybercrime en in onderzoek naar de preventie van fraude. Ken Palla is gepensioneerd directeur van de MUFG Union Bank. Hij werkte aan de security-systemen van banken. Hij onderzoekt en schrijft over consumentenfraude wereldwijd. Wiebe Fokma is *fraud detection strategist* bij SurePay, Hij werkt aan de preventie van onlinefraude in de financiële sector. Bernard P. Veldkamp is vicedecaan van de Faculteit Gedrags-, Management- en Maatschappijwetenschappen van de Universiteit Twente. Hij is gespecialiseerd in onderzoeksmethodologie, metingen en data-analyse. Zijn belangstelling richt zich op optimalisatie, *text mining* en computergestuurde beoordeling.

bij bedrijven fors is afgenomen (§3). Helaas is, in contrast hiermee, slachtofferschap van onlinefraude bij individuen beduidend toegenomen (§2).

Deze factsheet behandelt maatregelen gericht op de zogenaamde 'geautoriseerde betalingen'. Dit betekent dat de betalingen aan fraudeurs door de slachtoffers zelf zijn uitgevoerd. Dan gaat het bijvoorbeeld om bankhelpdeskfraude, investeringsfraude of onlinedatingfraude. Wij bespreken maatregelen gericht op potentiële slachtoffers en maatregelen gericht op het voorkomen van specifieke incidenten en het verstoren van een modus operandi.

Bij preventie gericht op potentiële slachtoffers gaat het om betere informatie voor gebruikers en aandacht voor kwetsbare groepen, zoals ouderen (§4). Technische en organisatorische maatregelen zorgen ervoor dat deze gebruikers beter worden beschermd. Denk bijvoorbeeld aan het opzetten van 'money locks' waar geld wordt gestald dat niet op korte termijn kan worden opgenomen, en het vertragen van het overmaken van grote bedragen. In het VK worden ouderen in meer gevallen door banken gecompenseerd voor verliezen door fraude.

Voor het voorkomen van incidenten bestaan verschillende opties (§5).

Paragraaf 5.1 behandelt de gegevensuitwisseling tussen private partijen (§5.1). Daarbij moet men zich realiseren dat fraude een '*predicate offense*' is: het is vaak onderdeel van een grotere keten van misdrijven, zoals georganiseerde criminaliteit, witwassen of belastingontduiking. Daarom is een gezamenlijke aanpak nodig om de fraude te bestrijden .

Er bestaat een veelheid aan privaat-private verbanden waar gegevens worden uitgewisseld via onlineplatformen (§5.1.1). Het delen van gegevens is ontzettend belangrijk. En er zijn talloze manieren waarop gegevens effectief kunnen worden gedeeld om fraudeurs te bestrijden, met inachtneming van overheidsregelgeving en privacywetgeving. Meestal blijkt dat wetgeving nodig is om het delen van gegevens over (bank)fraude op een correcte manier mogelijk te maken. Het VK, de VS, Singapore, Australië, Estland en Zwitserland zijn voorbeelden van landen waar private partijen onderling gegevens delen [4]. Landen waar de Algemene Verordening Gegevensbescherming (AVG) geldt en waar platformen voor gegevensuitwisseling bestaan zijn het VK en Estland. In het VK delen de platformen fraude-informatie onderling op basis van de 'gerechtvaardigd belang'-vermelding in artikel 47 van de AVG. Er zijn meerdere manieren waarop gegevens kunnen worden gedeeld (§5.1.2): a) banken delen gegevens onderling; b) banken delen gegevens met een derde partij die is opgericht als een goedgekeurde/gereguleerde gegevensopslag, de platformen; c) banken delen gegevens met nationale antifraudecentra en vice versa; d) leveranciers vormen dataconsortia binnen hun klantenbestand; e) operators van betalingsnetwerken die interne netwerkgegevens gebruiken; f) landen delen fraudegegevens binnen een geografische regio. Het aantal landen dat vooruitgang boekt met het delen van bankgegevens zijn onder meer het VK, Australië, Zuidoost-Azië en misschien binnenkort ook de EU .

We bespreken een aantal beleidsopties in het kader van gegevensuitwisseling: a) de experimentele omgevingen (de 'zandbak' waarin met innovatieve regelgeving wordt geëxperimenteerd, §5.1.1 a); b) het voorstel om in de regelgeving onderscheid te maken tussen personen en bedrijven, om zo fraudeurs sneller te herkennen en op te sporen (§5.1.2 b); c) de verantwoordelijkheid neerleggen daar waar iets fout gaat, zoals bijvoorbeeld bij internetserviceproviders (ISP's, §5.1.2 c); d) de rol van sociale media onderzoeken, omdat veel fraude daar begint (§5.1.2 d).

Benadrukt wordt dat gegevens delen een breed scala aan gunstige effecten heeft, waaronder een betere preventie tegen onlinefraude, grotere sommen geld die kunnen worden teruggehaald en extra bescherming voor organisaties die deelnemen aan een platform, zoals Cifas (§5.1.4), We geven aan dat de maatregelen tegen fraude en tegen witwassen overlap vertonen (§5.1.5) en bespreken een aantal aandachtpunten voor de uitvoering (§5.1.6).

Paragraaf 5.2 bespreekt vervolgens publiek-private partnerschappen (§5.2). Voor bestrijding van onlinefraude is samenwerking van belang. Beide typen organisaties hebben elkaar vaak nodig en kunnen van elkaar leren. Geen enkele afzonderlijke organisatie heeft een totaalbeeld, het samenbrengen van informatie is essentieel. Meerdere auteurs leggen er de nadruk op dat goede wetgeving en governance nodig zijn om samenwerking goed te laten verlopen. In het buitenland bestaan dergelijke vormen van samenwerking, Europol speelt in Europa een belangrijke rol (§5.2). We geven een praktisch voorbeeld van de concrete effecten van gegevensuitwisseling bij de Fraudehelpdesk in de situatie voor de invoering van de Uitvoeringswet Algemene verordening Gegevensbescherming in 2018 (§5.2.1).

De beste vormen van gegevensuitwisseling, met de meeste impact op fraude, komen van leveranciersconsortia en detectieoplossingen die in het netwerk van de financiële transacties zijn geïntegreerd. Hun kracht ligt in het samenbrengen van gegevens van een groot aantal organisaties uit de financiële sector, zoals banken, retailbanken, fintechbedrijven en aanbieders van betalingsdiensten, die veilig en beveiligd, direct of indirect verbinding maken met de centrale infrastructuur die betalingen checkt. Hoe meer deze betalingsnetwerken netwerkanalyses maken en fraudewaarschuwingen bieden, hoe groter de kans dat fraude afneemt.

Banken en andere financiële instellingen spelen een essentiële rol in de preventie en detectie van fraude (§5.3). Zij kunnen zich richten op een aantal maatregelen: het actief bestrijden van geldezels (§5.3.1), detectie van 'afwijkende' transacties (§5.3.2), gedragsbiometrie op de uitgaande transactiestroom (§5.3.3), en het checken of de klant ook aan het bellen is tijdens afwijkende transacties (§5.3.4). De 'money lock' wordt beschreven in §5.3.5; een aantal andere matregelen wordt besproken in §5.3.6.

Een interessant punt is het compenseren van verliezen van klanten (§5.4). Door organisaties te verplichten verliezen te compenseren, worden ze geactiveerd om meer preventieve maatregelen te nemen. In het VK, bijvoorbeeld, worden de meeste verliezen gecompenseerd door de banken, bij alle vormen van geautoriseerde fraude, [5].

Een nieuwe ontwikkeling is dat de compensatie voor verliezen wordt gesplitst tussen de verzendende *en* ontvangende banken. De ontvangende bank is de bank met geldezels en/of die de geldezelrekeningen beheert. Sommige banken rekenen aanzienlijk meer geldezels tot hun klanten en/of beheren meer geldezelrekeningen dan andere. Dit systeem van gesplitste vergoeding is geïmplementeerd in het VK (§5.5). Het blokkeren van frauduleuze oproepen en sms-berichten wordt besproken in §5.6.

We bespreken de aanbevelingen om fraudepreventie beter te organiseren (§5.8). Deze zijn ook opgenomen in Tabel 1 (hieronder). Interessant is dat in het VK nu een minister voor de bestrijding van fraude is geïnstalleerd (§5.7)[6].

Tabel 1: Aanbevelingen om onlinefraude bestrijding beter te organiseren, vanuit internationaal perspectief[1]

Doel	Toelichting	Landen - voorbeelden	Impact
(1) Maak een nationale leider verantwoordelijk voor het voorkomen van onlinefraude (§5.7 & §5.8).	Er moet op nationaal niveau één persoon zijn die verantwoordelijk is voor het voorkomen van fraude.	In het VK is nu een minister voor fraude geïnstalleerd, David Hanson. In Australië is minister van Financiën Stephen Jones verantwoordelijk geweest. Hij ging recent met pensioen.	De succesvolste landen in de strijd tegen consumentenfraude hebben op regeringsniveau één persoon aangesteld om de inspanning te leiden.
(2) Vergroot het bewustzijn van de consument op nationaal niveau, eensgezind en permanent (§4). Er zijn maar weinig landen die een nationale strategie hebben voor het informeren van consumenten, manieren om consumenten te beschermen en hoe consumenten onlinefraude kunnen melden. In Nederland zijn met enige regelmaat campagnes, bijvoorbeeld van de banken en de Fraudehelpdesk.	Er is een uniform, nationaal en permanent bewustwordingsprogramma nodig op basis van internationale *best practices*, van de basisschool tot bejaardentehuizen, en gefinancierd in samenwerking met de industrie. Creëer een nationaal publiek-private partnerschap met deelname van alle geïnteresseerde organisaties, waaronder banken, telecommunicatiebedrijven, digitale platforms en consumentenbelangengroepen.	Het initiatief 'Friends Against Scams' in het VK is een voorbeeld op dit gebied. Dit programma heeft meer dan een miljoen burgers getraind met behulp van een zeer succesvolle 'Train the Trainer'-aanpak. Ook Australië heeft een goed nationaal programma.	Betere voorlichting consumenten is een basisvoorwaarde voor een nationale aanpak. Evaluaties zijn ook belangrijk: wat werkt, wat werkt niet [7].
(3) Faciliteer een nationaal, eenvoudig onlineplatform voor de fraudemeldingen (§5.8). In Nederland doet 12% van de slachtoffers aangifte van fraude [8]. Bepaalde vormen van fraude moeten worden gemeld aan afzonderlijke autoriteiten: politie, financiële autoriteiten of consumentenautoriteiten.	In Nederland kunnen slachtoffers naar het Landelijk Meldpunt Internetoplichting (LMIO), naar de Fraudehelpdesk, of naar Slachtofferhulp. Als er geld van de rekening is verdwenen, nemen slachtoffers vaak contact op met hun bank. Onderzocht kan worden of een geïntegreerd platform mogelijk is. In Nederland helpt de Fraudehelpdesk slachtoffer bij de juiste loketten terecht te komen.	• VS: Crime Complaint Center (IC3) van de FBI. • VK: Actie Fraude. • In Nederland is er het internetmeldpunt van de politie, dat echter alleen is bedoeld voor consumentenfraude (aankoopfraude, verkoopfraude en nepproducten). De fraudehelpdesk telt ongeveer 70 vormen van fraude waarvan de meerderheid niet onder consumentenfraude valt, zoals onlinedatingfraude, spoofing, investeringsfraude, goede doelen fraude, vriend in nood (vaak via WhatsApp), etc.	• Nuttig voor slachtoffers. • Betere kennis over fraude [9, 10]. • Meldingen van fraude kunnen sneller worden omgezet in signaleringen. Bijv.: https://www.politie.nl/aangifte-of-melding-doen/controleer-handelspartij.html
(4) Zorg voor organisatorische ondersteuning voor slachtoffers van fraude (§4). Doel: 1) hulp en ondersteuning, 2) Voorkomen van herhaald slachtofferschap.	**Wat**: hulp bij schadevergoeding regelen, bij sociaalpsychologische steun en hulp bij de toepassing van technische beschermingsinstrumenten. **Hoe:** een helpdesk voor fraudeondersteuning om de juiste organisaties te vinden.	In **Nederland** zijn er: https://www.slachtofferhulp.nl https://www.fraudehelpdesk.nl/ **VK:** https://www.thecyberhelpline.com/ **Australië**: https://www.idcare.org/	• Het bieden van ondersteuning. • Voorkomen dat slachtoffers opnieuw het doelwit worden van fraudeurs, onder andere omdat ze op 'ezellijstjes' van cybercriminelen terechtkomen.

(5) Maak fraude over de grenzen heen traceerbaar. De AVG is er voor het bevorderen van het recht op privacy van het individu, maar zou criminelen niet de mogelijkheid moeten geven om in het geheim te opereren.	Pas de bestaande AVG-wetgeving aan zodat er een onderscheid kan worden gemaakt tussen *bedrijven* en *individuen*. Als een dienst of product wordt verkocht, zijn de gegevens zakelijk, zelfs als het een persoon is die het bedrijf runt. Bedrijven moeten identificeerbaar en bereikbaar zijn.	Elke partij in de waardeketen moet een *'know your customer'*-beleid hebben. Regel dit via wereldwijde brancheverenigingen die fraude traceerbaar kunnen maken.	Dit zou de pakkans, en dus de relatieve straffeloosheid voor fraudeurs moeten verminderen.
(6) Laat landelijke organisaties beter samenwerken Op dit moment verzamelen een aantal instanties meldingen en informatie over fraude, zoals het landelijk meldpunt Internetoplichting (LMIO) van de politie, de Fraudehelpdesk, de banken. Voor een beter beeld en gecoördineerd beleid zou men kunnen inzetten op meer samenwerking en coördinatie (§5.1 & §5.2).	Richt een nationaal centrum voor fraude op. De rijksoverheid kan het handvest van het Nationaal Cyber Security Centrum of de Nationale Politie uitbreiden, of een aparte entiteit oprichten voor onlinecriminaliteit gericht op consumenten, en financiële middelen beschikbaar stellen. Bescherming op infrastructuurniveau is belangrijk. Het Nationaal Cyber Security Centrum kan dit, in samenwerking met banken, telecom- en internetproviders, opzetten. Een nationaal antifraudecentrum kan helpen bij het coördineren van het delen van gegevens tussen banken, telecommunicatiebedrijven, digitale platforms en de overheid (en misschien tussen landen).	Een uitstekende *best practice* is het Singapore Anti-Scam Command, waar alle belanghebbenden fysiek bij elkaar zitten, waardoor het mogelijk wordt om bankrekeningen, telefoonnummers en IP-adressen onmiddellijk te blokkeren. Ook het *Australian National Anti-Scam Centre* en het Canadian Anti-Fraud Centre zijn goede voorbeelden Belgisch anti-phishing schild, gebruikt om valse investeringswebsites uit de lucht te halen Quad9, een Zwitserse non-profit DNS-*resolver*, De Taiwanese Anti-fraude browser. De *Europese DNS-resolver* kan burgers in Europa beschermen. (Een *resolver* vertaalt voor mensen leesbare domeinnamen (zoals www.example.com) naar IP-adressen (zoals 192.0.2.1))	De effectiviteit van het Singaporese initiatief groeit: In 2024 heeft de politie van Singapore onder meer 57.700 mobiele lijnen, meer dan 40.500 WhatsApp-lijnen en meer dan 33.600 onlinegebruikersnamen en advertenties ontmanteld. Dit was een flinke stijging ten opzichte van 2023 [11].
(7) Breid regelgeving uit voor de controle op fraude door financiële instellingen (bijv. op gebied van compensatie) (§5.1.1, & §5.2),	Deze regelgeving maakt dat financiële instellingen een schriftelijke antifraudestrategie, controles op fraude en op geldezels(rekeningen) hebben, met inbegrip van strikte controles op het openen van rekeningen. Scamcontroles kunnen bestaan uit het detecteren van afwijkingen in transacties, gedragsbiometrie, waarschuwingsmeldingen voor klanten, het vasthouden van verdachte transacties en bevestiging van de begunstigde. Dezelfde regels zouden van toepassing moeten zijn op cryptocurrency-uitwisselingen. Maak een veilige haven (rechtsbescherming) mogelijk voor redelijke inspanningen van deze instellingen	In het VK hebben de Financial Conduct Authority en de Payment Systems Regulator specifieke vereisten voor financiële instellingen om fraude te voorkomen.	Hoewel fraude niet begint bij financiële instellingen, is dit waar het geld naartoe stroomt. Het stroomt uit in de vorm van contant geld, snellere betalingen, overschrijvingen en, recenter, naar cryptocurrency-uitwisselingen. Regulering kan preventie en terugbetaling omvatten. Er is momenteel een vergoeding voor *bank spoofing scams* door Nederlandse banken. In het VK zijn de vergoedingen veel ruimer.
(8) Maak digitale platforms en aanverwante diensten verantwoordelijk	Maak elke dienstverlener, of het nu gaat om een domeinnaamregistrator, hostingbedrijf, socialemediaplatform, datingsite, betaalmethode, of welke andere partij dan ook,	In het VK stelt de Online Safety Act duidelijke eisen aan deze dienstverleners om strafrechtelijke problemen te voorkomen.	De regulering van digitale platforms en aanverwante diensten kan preventie en vergoeding [12]omvatten.

en aansprakelijk voor het mogelijk maken van fraude (§5.1.2 c & §5.1.2 d). Fraudeurs hebben domeinnamen, servers, marketingkanalen en betalingsplatforms nodig om hun misdaden te plegen. Sommige van deze dienstverleners maken veel meer fraude mogelijk dan andere, bijvoorbeeld door het ontbreken van *Know Your Customer* (KYC)-processen.	verantwoordelijk en aansprakelijk om misbruik te voorkomen. Laat hen indien nodig de schade vergoeden die door hun diensten is veroorzaakt. Dienstverleners moeten dan wel een duidelijke procedure volgen voordat ze iemand of een website verwijderen: 1) de klant waarschuwen, 2) als er geen reactie komt, de eindgebruiker waarschuwen, 3) ten slotte kan de frauduleuze dienst volledig worden verwijderd.	In Australië vereist de wetgeving van het *Scams Prevention Framework* dat digitale platforms en aanverwante diensten, fraude detecteren, blokkeren en verstoren.	De Deense domeinnaamregistrator, DK Hostmaster, heeft de verplichting ingevoerd om een ID te tonen voordat een .dk-domeinnaam kan worden geregistreerd. Als gevolg hiervan daalde het aantal onlinewinkels dat verdacht wordt van inbreuk op intellectuele eigendomsrechten met een .dk-naam al in één jaar tijd met 85%.
(9) Maak telecomaanbieders verantwoordelijk en aansprakelijk voor het mogelijk maken van fraude (§5.1.2 c).	Het ter verantwoording roepen van telecomproviders betekent ook dat zij de vrijheid moeten krijgen om op te treden tegen (mogelijk) misbruik van hun diensten door fraudeurs. Maar dat moet wel op de juiste manier gebeuren. Maak elke telecomprovider verantwoordelijk en aansprakelijk om misbruik te voorkomen. Laat hen indien nodig de schade vergoeden die door hun diensten is veroorzaakt.	In Australië vereist de Scam Prevention Framework-wetgeving dat telecomproviders fraude detecteren, blokkeren en verstoren.	Het voordeel voor telecomproviders is de reputatieverbetering doordat zij bijdragen aan het veiliger maken van het internet. De regulering van telecomproviders kan preventie en vergoeding omvatten.
(10) Zet een internationaal netwerk voor fraudeopsporing en -vervolging op (§5.1.3). Fraude is vaak een internationaal misdrijf en een vorm van georganiseerde criminaliteit. De pakkans is laag en soms zijn de straffen (internationaal gezien) ook laag, aldus GASA [12].	Meer aandacht voor het internationaal aspect van fraude is nodig. Daarom is internationale coördinatie en meer eenheid in straffen wenselijk. Sommige landen hebben al een gespecialiseerde rechtbank opgericht om de technischer gevallen van onlinefraude te behandelen. In Nederland is slechts één onderzoek verricht naar straftoemeting en ICT, en dat laat zien dat 'high-tech skills' zwaardere straffen krijgen [13]. Dit gaat echter over cybercrime, niet zozeer fraude.	Een internationaal netwerk kan stappen ondernemen om coördinatie in het beleid ten aanzien van fraude te bevorderen. Het is daarom essentieel om het handvest van Europol, Interpol en aanverwante actoren uit te breiden om de opsporing naar, en de aanhouding van fraudenetwerken te verbeteren. In Zuidoost-Azië ligt de nadruk op het creëren van interregionale coördinatie van fraude en het voorkomen of vervolgen van zwendel.	Dit moet helpen om de relatieve straffeloosheid te voorkomen die tegenwoordig vaak geldt voor fraudeurs.

[1] Deze tabel is een combinatie van aanbevelingen van de auteurs van deze factsheet en van de Global Anti-Scam Alliance [12]

1. Inleiding

In deze factsheet bespreken wij een aantal methoden dat in het buitenland worden gebruikt om onlinefraude te voorkomen. We behandelen de vragen: *hoe wordt in het buitenland met onlinefraude omgegaan? Welke bevoegdheden zijn er, waarop wordt de focus gelegd en zijn er best practices waar de autoriteiten in Nederland van kunnen leren?* In het antwoord op deze vragen wordt in het bijzonder aandacht besteed aan welke mogelijkheden er naast het strafrecht kunnen zijn in Nederland om onlinefraude aan te pakken.

Het label 'fraude' dekt een breed scala aan activiteiten zoals belastingfraude, faillissementsfraude, telemarketingfraude, fraude met financiële diensten, zoals verzekeringsdekking; investerings- of bedrijfsregelingen en nep-liefdadigheidsinstellingen.

Belangrijk is het onderscheid tussen al dan niet door het slachtoffer geautoriseerde overschrijvingen: bij niet-geautoriseerde overschrijvingen wordt een bankrekening overgenomen door de crimineel, waarbij het slachtoffer in eerste instantie niets in de gaten heeft. Bij geautoriseerde overschrijvingen is het slachtoffer zodanig gemanipuleerd dat hij/zij zelf geld overmaakt naar een bankrekening van de fraudeur. Voor zaken als het vergoeden van verliezen is dit verschil belangrijk. Onder ‘onlinefraude’ worden in het algemeen de geautoriseerde overschrijvingen verstaan. Tegenwoordig is deze fraude meestal online [14]. Cybercriminaliteit is voor een groot deel 'onlinefraude'. Hacken of ransomware, daarentegen, zijn voorbeelden van cybercrime en niet van onlinefraude. Als slachtoffers van ransomware de crimineel betalen is dat afpersing, geen fraude. In deze factsheet gaat het om de geautoriseerde betalingen en om fraude van burgers tegen burgers, de zogenaamde horizontale fraude.[2]

Er verandert veel wanneer de criminaliteit van offline naar online gaat. Twee zaken worden hier genoemd. De verhouding tussen publieke en private partijen verandert waar het gaat om de kennis over, en de bestrijding van onlinecriminaliteit. In het verleden, bij een bankoverval, werd de politie gewaarschuwd. Zij handhaafde en had daarmee ook zicht op de aard van de criminaliteit. Online is dit anders. Banken merken dat geld verdwijnt van de rekeningen van hun klanten. Als de klanten zien dat hun rekening is geplunderd waarschuwen zij de bank. Als systemen worden gehackt, dan wordt een cybersecuritybedrijf gebeld. Zo verdwijnt het zicht van publieke partijen op de criminaliteit en worden belangrijke beslissingen meer dan vroeger genomen door private partijen [15].

Een ander relevant verschil tussen offline en online is dat onlinecriminaliteit vaak schaalbaar is. Als een fraudesysteem eenmaal correct is opgezet, kan een onlinecrimineel dus meerdere slachtoffers tegelijk oplichten, terwijl de ouderwetse bankovervaller slechts één bank tegelijk kan beroven. Met Agentic AI zal dit naar verwachting alleen maar erger worden.

De overgang van offline- naar onlinecriminaliteit heeft daarmee grote implicaties voor het politiewerk. Eén aspect daarvan is dat steeds meer nadruk is komen te liggen op samenwerking met andere partijen ten behoeve van preventie. Een voorbeeld is het offline halen van ‘foute’ websites. Zo werkt het samenwerkingsverband Electronic Crime Task Force (ECTF) van de politie, het OM, DNB en enkele grote banken, aan het offline halen van phishingwebsites [1]. Daarnaast zet de politie in op verstoren/stoppen en (3) gerechtelijk afdoeningen [16]. Dit beleid is mede ingegeven door het feit dat daders zich vaak in het buitenland bevinden.

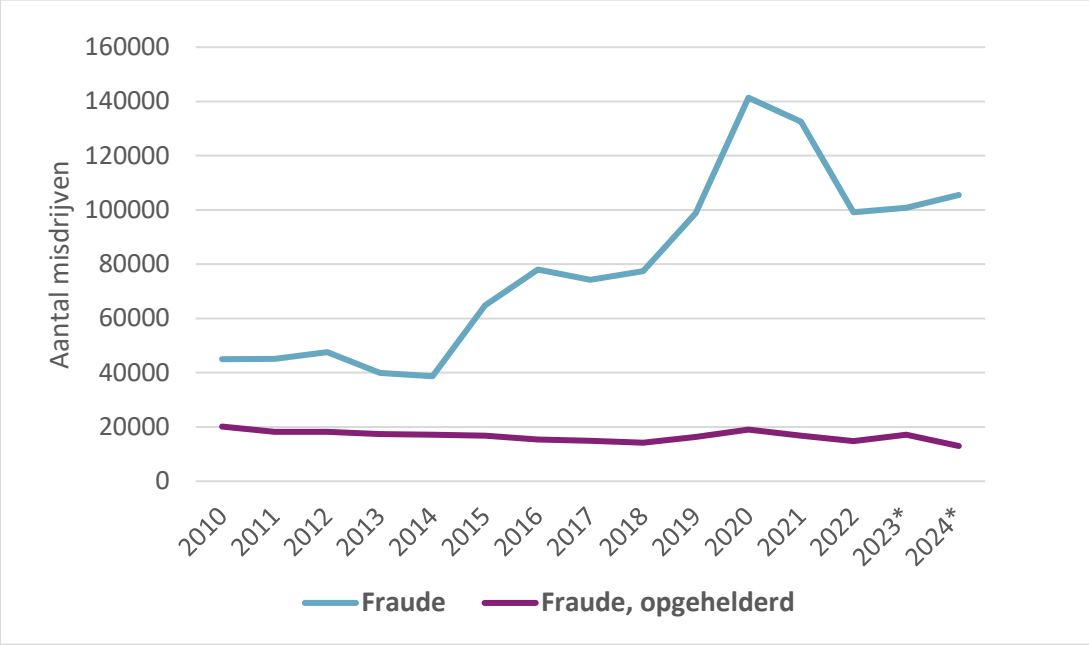
[2] Horizontale fraude betekent dat niet de overheid maar particulieren, bedrijven, financiële instellingen of organisaties slachtoffer worden. Bij verticale fraude is het de overheid die wordt gedupeerd.

Hieronder beginnen wij met enkele cijfers over de prevalentie van (online)fraude. Vervolgens worden de opties om onlinefraude te bestrijden uiteengezet. Daarbij wordt eerst gekeken naar persoonsgerichte benaderingen en vervolgens naar incidentgerichte benaderingen. [3]

Een korte uitleg van in de factsheet veelgebruikte begrippen is opgenomen in de bijlage.

2. Prevalentie van onlinefraude

De politie registreerde 12.210 maal computervredebreuk in 2023 en 7.065 maal in 2024. Dit is relatief gering. [17]. De meeste onlinedelicten worden echter als 'fraude' geregistreerd binnen het justitiële systeem [18, 19]. De fraudestatistieken laten sinds het begin van deze eeuw wereldwijd een enorme stijging zien, zowel in de VS [3] en het VK [20] als in Europa [21]. De schade loopt in de tientallen miljarden [22, 23]. In Nederland is geregistreerde fraude gestegen van 45.000 incidenten in 2010 naar 105.485 incidenten in 2024; daarvan werd opgehelderd 45% in 2010 en nog maar 12% in 2024 [17](figuur 1)[4]. Bij de Fraudehelpsdesk (FHD) zijn in 2023 57.780 meldingen van incidenten gedaan, waarvan een deel ook bij de politie wordt gemeld. Op dit moment bestaat een derde van de veelvoorkomende criminaliteit uit onlinefraude, aldus de politie [1].



Figuur 1: Geregistreerde fraudes die door de politie zijn geregistreerd en opgehelderde zaken (bron: CBS, 2025, eigen bewerking).

Statistieken laten verschillende trends zien voor bedrijven en particulieren. Onder bedrijven daalt sinds 2016 het aantal intern en extern veroorzaakte cybersecurityincidenten. Zo daalde onder de grootste bedrijven (250 of meer werknemers) het aantal ICT-veiligheidsincidenten door een aanval van buitenaf van 40% in 2016 naar 18% in 2022 [24]. Onder individuen is slachtofferschap van onlinecriminaliteit sinds 2016 juist gestegen van 11% in 2016 [25] naar 16,9% in 2021, een toename van 22% [26].[5] In 2024 was 15,7% van de Nederlanders slachtoffer van onlinecriminaliteit, waarvan 9,4% onlinefraude is [24]. Naar schatting is er in totaal in Nederland 2,75 miljard verlies door (meestal online)fraude [8].

[3] Een eenduidig beeld schetsen is lastig: sommige statistieken behandelen fraude, online of offline, waarbij gesteld moet worden dat de meeste fraude tegenwoordig online is; andere gegevens betreffen cybercrime of specifieke online delicten.
[4] De cijfers hebben betrekking op de volgende misdrijfcategorieën: bedrog, valsheidsmisdrijven, heling, afpersing en afdreiging en witwassen waarvan een groot deel online worden uitgevoerd.
[5] Dit was inclusief 'cyberpesten, het CBS presenteerde bij de eerste metingen voor cybercrime geen totalen voor online fraude.

Op basis van slachtofferstudies is het aantal fraude-incidenten veel groter dan het aantal geregistreerde misdrijven. Het CBS schat het aantal onlinefraude-incidenten op 1.722.000 (zeven vragen, zonder phishing) [27].

Voor veel slachtoffers zijn de gevolgen van slachtofferschap van fraude beperkt, maar voor 5 tot 15% van de slachtoffers veroorzaakt slachtofferschap financiële, mentale, fysieke of sociale problemen [8].

Helaas is de verwachting, zoals eerder gemeld, dat onlinefraude in de komende jaren zal toenemen. Door onder meer de stijging van onlinebetalingen, de recente explosie van IOT (het *internet of things)* en AI wordt fraude alleen maar makkelijker [2, 28, 29]. De oplossing is: meer preventie en meer security.

3. Preventie werkt

Omdat het aantal fraude-incidenten zo groot is, kan de politie het niet alleen. Preventie is noodzakelijk. Daarbij heeft preventie bijkomende voordelen: minder slachtoffers, minder verliezen, minder werk voor opsporingsinstanties en, ten slotte, ook potentiële daders worden hiermee beschermd tegen zichzelf.

Het goede nieuws is dat preventie werkt. Wetenschappelijke studies laten zien dat allerlei vormen van preventieve interventies, technische maatregelen of gebruikerseducatie kunnen helpen om onlinefraude te voorkomen [7, 30].

De praktijk laat zien dat praktische maatregelen een enorme impact kunnen hebben. Zo werd door de invoering van de EMV-chip in bankkaarten, in plaats van de magneetstrip, skimming bijna onmogelijk; ook *geoblocking*[6] hielp goed om skimming te voorkomen [31].

Bedrijven hebben sinds 2016 steeds meer veiligheidsmaatregelen genomen, zoals verbeterde authenticatiemethoden, het uitvoeren van risicoanalyses, het gebruik van data-encryptie en het toepassen van *network access control* [24]. Ook zien we, zoals hierboven vermeld, een afname in het aantal veiligheidsincidenten dat bedrijven treft; zowel incidenten met een interne als met een externe oorzaak. Het is plausibel dat de afname van slachtofferschap het gevolg is van de toename van preventieve maatregelen.

Er gaan veel zaken goed in Nederland. Zo lopen de meeste banken voorop met onlinefraudedetectie. Wij richten ons hieronder vooral op en wat wij zouden kunnen leren van het buitenland. Wij presenteren specifieke preventieve maatregelen en verwijzen naar evaluaties. Evaluaties zijn belangrijk om te weten wat wel en wat niet werkt en of maatregelen kosteneffectief zijn. Niet alle interventies helpen, er zijn veel 'feel good'-interventies [32]. Het is daarom zaak uit te zoeken wat de effectiviteit van een maatregel is. Ook is het nodig om uit te zoeken of er neveneffecten zijn. Zo daalde na de invoering van de IBAN-Naamcheck het aantal verkeerde overboekingen met 67% [33] en het aantal meldingen van factuurfraude met 81 procent [34]. Maar tegelijkertijd bleek dat betalingen van slachtoffers aan fraudeurs steeds vaker naar een buitenlandse IBAN-rekening gingen [35]. Over het geheel genomen is er waarschijnlijk een afname van fraude. Deze ontwikkeling laat echter ook zien dat fraudeurs flexibel zijn en dat handhavers internationaal moeten samenwerken.

4. Preventie gericht op gebruikers

4.1. Gebruikers beter informeren

[6] Geoblocking is het standaard blokkeren van bankpassen buiten Europa.

Preventie kan zich richten op het voorkomen van incidenten of op bewustmaking en/of educatie van potentiële slachtoffers. De meeste mensen denken dat ze fraude kunnen herkennen, in de praktijk lukt dat niet altijd en worden zij toch slachtoffer [36]. Dit fenomeen staat ook wel bekend als het Dunning–Kruger-effect [37]. Gebruikers moeten daarom betere voorlichting krijgen over vormen van fraude en hoe zich daartegen te beschermen. Internationaal onderzoek laat zien dat gebruikers die geïnformeerd zijn over fraude en die op de hoogte zijn van bankprocedures, minder vaak slachtoffer worden [8]. Ook blijkt dat adequate gebruikerseducatie kan helpen [12, 38].

4.2. Kwetsbare groepen

Groepen die extra hulp nodig hebben zijn onder meer kwetsbare ouderen, beïnvloedbare gebruikers, laaggeletterden, mensen met een andere moedertaal en meervoudige slachtoffers (herhaald slachtofferschap komt relatief vaak voor [8, 39-41]). Kwetsbaarheid kan ook worden veroorzaakt door medische aandoeningen, een echtscheiding of het overlijden van een partner. Voor deze groepen kan extra educatie nuttig zijn. Hieronder wordt een overzicht gegeven van een aantal maatregelen waarmee ervaring is opgedaan in het buitenland.

1. Men kan banken toestaan om (grote) transacties voor kwetsbare groepen langer vast te houden totdat een transactie is gecontroleerd. Indien men ouderen meer bescherming wil bieden, betekent dit dat banken bij de beoordeling van transacties rekening moeten houden met de leeftijd van de klant. In de VS worden, op basis van recente wetgeving, in bepaalde staten verdachte transacties van oudere klanten opgeschort tot aanvullende controle is uitgevoerd [42]. Deze transactie wordt vastgehouden totdat de bank gesproken heeft met de klant.
2. Banken zouden kunnen eisen dat alle oudere klanten de naam van een vertrouwd familielid of vriend bij hun bankrekening hebben staan voor ondersteuning bij het uitvoeren van verdachte transacties, bijvoorbeeld in het geval dat de bank een transactie (tijdelijk) wil stoppen. Sommige Amerikaanse staten hebben wetten die banken toestaan dit te doen.
3. Kwetsbare slachtoffers worden in het VK zonder eigen risico eerder en royaler gecompenseerd, ook als ze ernstig nalatig zijn geweest, zie ook §5.4. Voorwaarden die normaal gesproken gelden voor het toekennen van een financiële vergoeding, gelden voor hen niet, zie ook paragraaf 5.2.3 [43]. Het te vergoeden maximum is wel hetzelfde [44].

5. Preventie gericht op incidenten: *best practices*

Hieronder worden maatregelen besproken die in het buitenland effectief zijn of lijken te zijn en, voor zover bekend, in Nederland niet of in beperkte mate worden toegepast. Er zijn niet altijd voldoende evaluaties om de effecten van preventieve maatregelen adequaat te meten [45-47]. Maar we kunnen regelmatig vaststellen dat maatregelen, gericht op een specifiek type fraude en die een bepaalde modus operandi ontwrichten, leiden tot een – soms grote – afname van de bewuste fraude, waardoor causaliteit heel plausibel wordt. Een voorbeeld is de introductie van de EMV-chip bij bankkaarten, zoals hierboven werd vermeld.

Wij beginnen met gegevensuitwisseling tussen private partijen. Gegevensuitwisseling is namelijk ook een voorwaarde voor sommige andere maatregelen. En de combinatie van informatie uit meerdere bronnen is vaak het effectiefst. Meestal heeft geen van de partijen het totaaloverzicht, nodig om fraude snel genoeg te kunnen herkennen.

5.1. Gegevensuitwisseling tussen private partijen

Er is een aantal redenen waarom private organisaties gegevens willen delen [4, 48, 49]:

- Fraude is vaak een onderdeel van een grotere keten van misdrijven, zoals georganiseerde criminaliteit, witwassen, belastingontduiking door particulieren en bedrijven, terrorismefinanciering, corruptie en omkoping, productnamaak/-piraterij, cybercriminaliteit,

drugshandel, milieucriminaliteit, mensenhandel/-smokkel van migranten en btw-fraude [4, 50-52]. In de juridische zin gaat het om '*predicate offenses*', dat zijn de 'onderliggende delicten' [53].[7] Het bestrijden van het ene type onderliggend delict is vaak ook behulpzaam bij het bestrijden van andere type. Zo is fraude een onderliggend delict voor het witwassen van geld en het voorkomen van het één is het voorkomen van het ander, bijvoorbeeld doordat beide gebruikmaken van geldezelrekeningen.

- Fraudeurs zijn vaak betrokken bij verschillende vormen van fraude, zoals bankhelpdeskfraude en betaalverzoekfraude, en bij 'traditionele' delicten zoals diefstal, heling of witwassen [1]. Zij fraudeerden relatief vaak ook bij de inkomstenbelasting [50]. Bij gevallen van verzekeringsfraude in het VK bleek dat in 82% van de gevallen ook fraude was gepleegd in een andere sector. Dit onderstreept volgens Dickinson (2015) de waarde van intersectoraal werken [51].
- Criminelen misbruiken bewust de versnippering van informatie door bijvoorbeeld bij meerdere banken te bankieren [48].
- Private organisaties krijgen te maken met een breed scala aan frauduleuze incidenten en witwassen en worden geacht maatregelen te nemen om die op te sporen en te voorkomen [4, 54].

Een voorbeeld van gegevens uitwisseling tussen private partijen is Cifas. Cifas is een non-profitorganisatie en beheert meerdere databanken, De *National Fraud Database* (NFD) bevat informatie over producten of diensten, zoals bankrekeningen en diensten die als frauduleus, inconsistent of verdacht worden beschouwd [55]. De *Insider Threat Database* bevat informatie over aanvragers of personeelsleden die frauduleus handelden, het gaat o.m. om diefstal, omkoping en corruptie [56]. Organisaties kunnen ook informatie uitwisselen over onschuldige slachtoffers van fraude, om hen zo te beschermen tegen verdere fraude. Leden zijn veelal banken en bouwverenigingen. Doel is om fraude en financiële criminaliteit te verminderen en te voorkomen.

5.1.1. Wettelijke basis wisselt per land

Verschillende landen binnen de EU gaan anders om met de AVG. Alle 'privaat naar privaat'-verbanden hebben een wettelijke basis. Landen die de AVG toepassen en waar platformen bestaan, zijn het VK en Estland [4]. In het VK delen de platformen fraude-informatie onderling op basis van de 'gerechtvaardigd belang'-vermelding in artikel 47 van de AVG: *"De verwerking van persoonsgegevens die strikt noodzakelijk is voor fraudevoorkoming is ook een gerechtvaardigd belang van de verwerkingsverantwoordelijke in kwestie. De verwerking van persoonsgegevens ten behoeve van direct marketing kan worden beschouwd als uitgevoerd met het oog op een gerechtvaardigd belang."*

De Britse fraudeplatformen, zoals Cifas[8], zijn door het Britse ministerie van Binnenlandse Zaken aangewezen als een *Specified Anti-Fraud Organisation* (SAFO) mede op grond van de *Serious Crime Act 2007*. In het VK wordt gegevensuitwisseling door de overheid sterk aanbevolen om fraude te voorkomen en slachtoffers te beschermen. Het Home Office [57] en de privacyautoriteit ICO leggen uit hoe dit verantwoord kan worden gedaan [zie ook 5, 58, 59].
De wijze waarop de platformen in het VK werken is in lijn met de AVG. Betrokkenen, ook wel '*data-subjects*' genoemd, behouden dan ook alle relevante AVG-rechten met betrekking tot geautomatiseerde besluitvorming [4, zie in het bijzonder sectie 3.13]. De ICO houdt toezicht op Cifas [4].

Er zijn, meer in het algemeen, verschillen tussen hoe EU-landen omgaan met persoonlijke gegevens. In Zweden staan van iedereen tal van persoonlijke gegevens online: men kan er, dankzij commerciële bedrijven, gratis informatie vinden over de *'geboortedatum, het geslacht, het telefoonnummer, het*

[7] Predicate offence means any criminal offence as a result of which proceeds were generated that may become the subject of an offence as defined in Article 9 of this Convention' aldus de Council of Europe Convention on Laundering, Search, Seizure and Confiscation of the Proceeds from Crime and on the Financing of Terrorism 53. COE, *CETS 198 –Laundering of the Proceeds from Crime and Financing of Terrorism, 16.V.2005*, in *Council of Europe Treaty Series - No. 198*, C.o.E. Convention, Editor. 2005, Council of Europe Convention: Strasbourg, France.

[8] Zie https://www.cifas.org.uk

adres, het aantal adreswijzigingen, de huisgegevens (grootte, bedrag of aantal kamers, etc.), de buren, het bedrijfseigendom, het voertuigeigendom en nog veel meer van elke geregistreerde persoon' [60]. Dit valt in Zweden onder de persvrijheid [60]. Ook in Finland is dergelijke informatie makkelijk vindbaar [61]. Finland en Zweden volgen, als EU-lid, ook de AVG en hebben een Autoriteit Persoonsgegevens. Deze voorbeelden geven aan dat de AVG op verschillende manieren in de praktijk kan worden gebracht.

5.1.2. Gegevensuitwisseling in het buitenland

Sinds 2021 hebben financiële instellingen in Nederland een vergunning van de Autoriteit Persoonsgegevens (AP) om informatie over fraude te delen (AP, 2021). In het buitenland is gegevensuitwisseling gebruikelijker. Het VK, de VS, Singapore, Australië, Estland en Zwitserland zijn landen waar private partijen onderling gegevens delen [4]. In Duitsland werken de banken nu samen om witwassen tegen te gaan [62]. Platformen die worden gebruikt voor het delen van gegevens zijn vaak niet alleen gericht op het voorkomen en opsporen van fraude, maar ook op de eraan gerelateerde delicten, zoals witwassen, georganiseerde criminaliteit en/of belastingontduiking. Deze delicten zijn nu eenmaal vaak onderdeel van eenzelfde criminaliteitsketen, zoals eerder beschreven. In Thailand wordt nu onderzoek gedaan naar mogelijkheden voor gegevensuitwisseling [63].

Er bestaan allerlei vormen van samenwerking tussen private partijen waarbij de mate waarin en met wie gegevens worden gedeeld, en de wijze van delen (eenmalig, per geval, of op dagelijkse basis) allemaal kunnen variëren. Maxwell [48] en Maxwell [4] geven een uitgebreid overzicht van de voordelen en de uitdagingen van het delen van gegevens. Voordelen liggen in de uitgebreidere mogelijkheden voor opsporing, het ontwikkelen van typologieën en het opsporen van criminele netwerken. Uitdagingen bevinden zich onder meer in de sfeer van het blijven garanderen van privacy, de kwaliteit van de gegevens en de contacten met publieke organisaties (meestal politie, justitie en andere handhaving- en opsporingsorganisaties). Gegevens worden meestal bewaard op beveiligde websites en daardoor meestal als 'platform' aangeduid [4, 48]. Hieronder beschrijven wij een aantal recente ontwikkelingen m.b.t gegevensuitwisseling.

a) De regelgevingzandbak

Interessant is de ontwikkeling van '*regulatory sandboxes'*.[9] In Zweden heeft IMY, de Zweedse privacyautoriteit, samen met de vier grote Zweedse banken[10] een regelgevingszandbak opgezet waarin nauw wordt samengewerkt tussen technici en juristen, cruciaal voor succes. [64]. Samen interpreteren innovatoren en toezichthouders hoe, met behulp van innovatieve producten en diensten, regelgeving voor gegevensuitwisseling in de praktijk kan werken. Ook in het VK bestaan *regulatory sandboxes*, die door ICO, de Britse privacyautoriteit, worden ontwikkeld. Deze *sandboxes* zijn een gratis service: organisaties worden ondersteund bij het ontwikkelen van nieuwe producten en diensten die op een geavanceerde en veilige manier gebruikmaken van persoonsgegevens en die de privacy waarborgen [65].

b) Onderscheid tussen personen en bedrijven

De *Global Anti-Scam Alliance* (GASA) [12] beveelt aan om gegevens ook internationaal te delen. GASA stelt voor dat de AVG onderscheid maakt tussen bedrijven en personen. Als een dienst of product wordt verkocht zijn de gegevens 'bedrijfsgegevens', ook al is de persoon die het bedrijf exploiteert of het product of de dienst levert een individu. In de rol van een bedrijf moet duidelijk zijn wie een product of dienst verkoopt, inclusief directe manieren om contact met die entiteit op te nemen [12].

c) Verantwoordelijkheid neerleggen daar waar iets fout gaat

[9] Een '*regulatory sandbox*' stelt innovatoren in staat om nieuwe producten, diensten en bedrijfsmodellen in een praktijkomgeving te testen zonder dat sommige van de gebruikelijke regels van toepassing zijn.
[10] De vier banken zijn: SEB, Nordea, Swedbank en Handelsbanken.

Het klinkt logisch dat organisaties waarvan fraudeurs misbruik maken verantwoordelijkheid krijgen voor wat er mis gaat [12]. Zo zouden internetserviceproviders (ISP's) verantwoordelijk moeten worden gesteld voor misbruik. Dit betekent ook dat ze de mogelijkheid moeten krijgen om op te treden tegen (potentieel) misbruik van hun diensten door fraudeurs. ISP's zouden wettelijke bescherming moeten krijgen tegen aansprakelijkstelling door hun klanten, mits ze een duidelijke procedure volgen om vergissingen te voorkomen. GASA [12] beschrijft een procedure om e.a. goed te laten verlopen.
De Australische regering integreert verschillende maatregelen [66]. Volgens het Australische *Scams Prevention Framework* [67] zullen banken worden belast met het toevoegen van specifieke controles, terwijl telecombedrijven frauduleuze oproepen en berichten moeten detecteren en verstoren, en socialemediabedrijven zullen worden belast met het verwijderen van zwendeladvertenties en het zorgen voor een betere verificatie van apparaten. Ook komt er een antifraude-informatiesysteem. Dit initiatief houdt in dat banken, telecommunicatienetwerken, internetproviders en socialemediabedrijven informatie moeten gaan delen om fraude te bestrijden. Hierbij is het doel onder meer '*het blokkeren van frauduleuze telefoonnummers en URL's en het verwijderen van nepwebsites en berichten op* sociale media PWC [66], [67]. Er komen zware straffen voor niet-naleving.

d) De rol van sociale media

Meerdere banken in het VK (TSB, Barclays) hebben laten weten dat 70-80% van de onlinefraude haar oorsprong kent op sociale media. De *UK Online Safety Act* die naar verwachting volgend jaar van kracht wordt, verplicht bedrijven zoals socialemediaplatforms om klanten te beschermen tegen frauduleuze content.

5.1.3. Internationale gegevensuitwisseling

De meeste platformen delen gegevens binnen de eigen landsgrenzen. Cosmic in Singapore maakt een uitzondering voor incidenten waarbij het gaat om de proliferatie van biologische, chemische en nucleaire wapens [4]. GASA [12] beveelt aan om gegevens over fraude internationaal te delen. fraude is, helaas, een internationale activiteit.

Een internationaal initiatief voor het delen van gegevens is de '*Global Signal Exchange*' (GSE). Het GSE-platform biedt vertrouwde partijen tools om dreigingsinformatie te delen. Deze organisatie richt zich op *online scams, fraud and abuse*. Signalen zijn indicaties van kwaadaardige activiteit. De GSE ontvangt signalen van diverse opensource- en commerciële aanbieders en biedt gebruikers van het platform snelle toegang om deze signalen te bekijken en te exporteren, zodat ze actie kunnen ondernemen tegen diverse bedreigingen. Doel is real-time data-uitwisseling om onlinefraude te detecteren, voorkomen en bestrijden. Op het moment van schrijven werden, in de laatste 24 uur, 582.028 signalen waargenomen. Partners zijn onder meer grote onlinebedrijven (waaronder Google en Amazon) en securitybedrijven (waaronder de Anti-Phishing Working Group, Gasa, de Cyber Defense Alliance en de, DNS Research Federation) [68].

Halpin and Todd [29] beschrijft praktische voorbeelden van publiek-private en internationale samenwerking en concludeert dat je gezamenlijk betere uitkomsten bereikt dan alleen. Het ligt voor de hand dat de noodzaak voor internationale samenwerking alleen maar zal groeien [29].

5.1.4. Effectiviteit van het delen van gegevens

Gegevensuitwisseling leidt tot een breed palet aan positieve uitkomsten [4]. Het gaat hieronder om de globale positieve uitkomsten, met Cifas als voorbeeld.

- Verbeterde preventie.
- Toename van terugvordering van geld dat zowel het banksysteem als de aan Cifas deelnemende instellingen verlaat.
- Een reductie van pogingen om de bankrekeningen van aan Cifas deelnemende instellingen te gebruiken om geld te stelen.

- Verbeterde detectiepercentages van financiële criminaliteit en andere incidenten.
- Hogere reactiesnelheid.
- Vermindering van de neiging van criminelen om aan Cifas deelnemende instellingen als doelwit te kiezen.
- Vermindering van duplicatie van rechtszaken en kosten dankzij gebundelde aanpak.

Cifas rapporteerde voor 2015: *'Meer dan £1 miljard aan besparingen werd gemeld door leden in 2015 dankzij het gebruik van Cifas' National Fraud Database (NFD), [er was] £4 miljard bespaard in de afgelopen 4 jaar, [dat is] £200 bespaard voor elke £1 aan abonnementen' [69].* In 2019 werden bijna 365.000 gevallen geregistreerd en is meer dan £ 1,5 miljard aan fraudeverlies voorkomen [4].

5.1.5 De link fraude - witwassen

Hierboven is al vermeld dat fraude en witwassen sterk gerelateerde delicten zijn; fraude is een onderliggend delict voor witwassen. Wereldwijd heeft men het daarom vaak over '*Financial Economic Crime*' (FEC), een begrip dat beide delicten combineert. Banken hebben tegenwoordig vaak een afdeling FEC in plaats van twee gescheiden afdelingen. De praktijk laat zien dat de geldezelrekeningen vaak worden gebruikt voor zowel fraude als witwassen; de detectie ervan is identiek. Fokma [70] heeft beargumenteerd dat zowel qua wetgeving als qua bestrijding een gemeenschappelijke benadering mogelijk en efficiënter is. Zo is het nu al mogelijk om witwassen te bestrijden, voor private organisaties om informatie te delen, op dezelfde wettelijke basis als geldt voor fraude, namelijk artikel 47 van de AVG. Enkele banken, zoals HSBC, zijn al in staat geweest om hun detectiesystemen voor fraude en witwassen volledig te combineren [71].

5.1.6. Aandachtspunten bij instellen platforms voor gegevensdeling

Er zijn belangrijke aandachtspunten bij het instellen van een platform voor het delen van gegevens in privaat-privaat verband of in een publiek-privaat partnerschap. Per land en per platform worden verschillende benaderingen gehanteerd {Maxwell, 2022 #20770`, zie §5.2 voor een uitgebreide behandeling van het publiek-privaat partnerschap}. Hieronder wordt een aantal punten samengevat. Een aantal algemene aanbevelingen voor platformen worden door Maxwell [4] gegeven: 1) het belang van een gedeelde strategische visie tussen stakeholders uit de publieke en private sector, 2) het ontwerpen van heldere, stimulerende wet- en regelgeving, 3) een robuuste governance, dataethiek en verantwoordingsplicht. Een aantal meer specifieke punten is ook van belang.

a) Het informeren van data-subjects

Hier zien we veel variaties. Sommige platformen nemen rechtstreeks contact op met de betrokkene om hem of haar te informeren over opname van gegevens in de database, terwijl dit voor andere wettelijk verboden is. Slechts een minderheid van de platformen biedt expliciete ondersteuning aan iemand die om gegevenscorrectie vraagt. In AVG-rechtsgebieden komt dit doorgaans doordat het platform een gegevensverwerker is en de beslissing om informatie vrij te geven door de deelnemende partij (de verwerkingsverantwoordelijke) wordt genomen [4, 72]. Cifas zelf, bijvoorbeeld, waarschuwt de betrokkene niet. Maar bij COSMIC, de Singaporese FI-FI *Information Sharing Platform*, zal de *Monetary Authority of Singapore* (MAS) eisen dat een financiële instelling, voordat zij een klantrelatie beëindigt, de klant voldoende gelegenheid biedt om zijn onschuld aan te tonen. De financiële instelling moet tevens haar beoordeling en de resultaten van haar controles met de klant delen [4].

b) Financiële uitsluiting

Een kernvraag is of het doel van het delen van informatie is om bepaalde personen financieel uit te sluiten, ook wel '*de-risking'* genoemd. De *European Banking Authority* (EBA) stelt dat financiële uitsluiting van categorieën mensen (zoals asielzoekers) en/of non-profitorganisaties ongewenste consequenties kan hebben [73]. Het is belangrijk om hiervoor een gecoördineerd beleid te ontwikkelen en dit dus niet aan afzonderlijke private instellingen over te laten [4]. Om die reden is ook het recht op het corrigeren van gegevens belangrijk.

c) Technische problemen

De kritische evaluatie van Maxwell [4] laat zien dat technische problemen wel bestaan maar inmiddels oplosbaar zijn.

d) Complexiteit vermijden

Een les uit het VK is dat uitwisseling van gegevens niet nodeloos complex moet zijn. Door Pay.UK is een standaard voor *Enhanced Fraud Data* (EFD) ontwikkeld voor uitwisseling van fraudegegevens tussen banken. Deze is zo complex dat de invoering niet lukt. Het initiatief is zeer recent een jaar *on-hold* gezet. Commentaar van de banken is dat de invoering veel te duur zou worden.

5.2. Publiek-private partnerschappen (PPP)

Overheidsinstanties zijn verantwoordelijk voor wet- en regelgeving; private entiteiten zijn verantwoordelijk voor de bescherming van hun klanten, systemen en data. Om onlinefraude te voorkomen is samenwerking vruchtbaarder dan afzonderlijk werken. Voordelen van publieke-private partnerschappen (PPP's) bij de onlinefraudebestrijding zijn onder meer [29]:

- Overheden kunnen de expertise van de private sector gebruiken voor cybercriminaliteitsonderzoek (inclusief digitale forensische analyse), cyberbeveiliging en technologie. Een goed voorbeeld zijn banken die het bevriezen van rekeningen en het terugvorderen van fondsen faciliteren door bankpersoneel van het Anti-Scam Centre bij de Singapore Police Force (SPF) te plaatsen.
- Private instanties kunnen profiteren van de middelen en wetgevende bevoegdheden van de publieke sector.
- Samenwerking helpt de kloof tussen juridische en technische expertise te dichten.
- Samenwerking bevordert het delen van informatie en *best practices*, wat de cyberbeveiliging verbetert en helpt criminelen te identificeren en aan te pakken voordat ze slachtoffers kunnen maken.

De buitenlandse vormen van publiek-private samenwerking verschillen vooral in hun verhouding tot publieke organisaties. Soms is de samenwerking structureel en nauw, soms is er (bijna) geen contact. Verschillende tussenvormen komen ook voor [4]. Zo financiert de verzekeringsbranche in het VK een handhavingsorganisatie, de *Insurance Fraud Enforcement Department* (IFED) van de *City of London Police* [4]. Andere voorbeelden zijn de *Joint Money Laundering Intelligence Taskforce* (JMLIT, in het VK) en de *Joint Policing Cybercrime Coordination* Centre (JPC3, Australië) [29].
Partnerschappen kennen uitdagingen, zoals het risico van belangenconflicten, risico's voor de privacy, de noodzaak van toezicht en procedures om ethische bedrijfsvoering te waarborgen.

Daarom zijn robuuste governancekaders noodzakelijk om de geloofwaardigheid, legaliteit en effectiviteit van dergelijke partnerschappen te behouden [4, 29]. Daarbij helpt het wanneer publiek-private partnerschappen worden ondersteund door wetgeving, overeenkomsten, en protocollen voor gegevensuitwisseling die voldoen aan de regelgeving inzake gegevensbescherming. Ook kan een *security clearance* van de private partijen nodig zijn [4, 29].

5.2.1. PPP in Nederland

In Nederland werkt de politie op dit moment samen met verschillende private partijen. Staats, Meerts [74] onderzochten deze samenwerkingsverbanden en vond er 36. De Politie Eenheid Landelijke Expertise en Operaties [1] beschrijft een aantal samenwerkingsverbanden, zoals de Electronic Crimes Taskforce (ECTF, een samenwerking tussen politie en banken), het Landelijk Meldpunt Internetoplichting (LMIO, een samenwerking tussen politie en Marktplaats) en het Knooppunt Finec (expertiseknooppunt politie). Binnen deze samenwerkingsverbanden worden echter geen gegevens gedeeld.

De ervaring van de Fraudehelpdesk (FHD) in Nederland illustreert de effectiviteit van gegevensuitwisseling. Een groot deel van de melders is bereid om gedetailleerde informatie te verstrekken over de incidenten. Het gaat dan bijvoorbeeld om verdachte e-mails, (screenshots van) WhatsAppberichten en sms'jes, de URL van webwinkels of facturen waarbij (mogelijk) sprake is van fraude. Maar sinds de invoering van de Uitvoeringswet Algemene verordening gegevensbescherming (UAVG) in 2018 is het de Fraudehelpdesk echter niet meer toegestaan gegevens van vermoedelijke fraudeurs op te slaan. In de periode daarvoor kon de FHD nog wel informatie doorgeven aan de politie, hetgeen leidde tot, onder meer, de volgende resultaten:

- In 2017 werden vijf mensen aangehouden voor oplichting via Marktplaats, nadat de Fraudehelpdesk, het OM en de politie nauw samenwerkten om 400 gevallen te onderzoeken. De totale schade was geraamd op meer dan €200.000 [75].
- In datzelfde jaar werden in een grootschalig onderzoek naar bankpasfraude twee verdachten aangehouden. Zij waren onderdeel van een landelijk opererende criminele organisatie die vermoedelijk miljoenen buit maakte bij tientallen of zelfs honderden slachtoffers. In het onderzoek werkte de politie intensief samen met de banken en de Fraudehelpdesk [76].
- In het geval van een variant van factuurfraude bracht de FHS de zaak onder de aandacht van de politie. De financiële schade door deze modus operandi bedroeg toen al vele miljoenen euro's.

Op dit moment mag de FHD geen gegevens over mogelijk fraudeurs registreren en kan zij een dergelijke bijdrage niet meer leveren.

Er zijn meer gevallen geweest waarbij opsporing van fraudeurs mogelijk was door publiek-private samenwerking. Samenwerking kan verschillende vormen aannemen, zoals het delen van dreigingsinformatie, deelname aan gezamenlijke oefeningen, hulp bij het terugvorderen van fondsen en het coördineren van incidentresponsinspanningen.

Momenteel loopt een pilot waarbij een medewerker van de politie-eenheid Oost-Nederland is gedetacheerd bij de Fraudehelpdesk (FHD) en waarbij beperkt gegevens worden gedeeld. Een evaluatie toont 100% tevredenheid bij melders (slachtoffers) en laat zien dat het aantal aangiften met ruim 30% stijgt.

5.3. Controles door banken

Banken en andere financiële instellingen vormen het hart van de geldstromen en spelen daarmee een cruciale rol bij de preventie en detectie van fraude. Elke financiële instelling zou daarom consumentenfraude actief moeten bestrijden. Daarbij hoort het hebben van een schriftelijke fraudestrategie en fraudecontroles.

Hieronder beschrijven wij enkele belangrijke controles op fraude om door de klant geïnitieerde frauduleuze transacties, de zogenaamde 'geautoriseerde transacties', te detecteren en te blokkeren. In zijn overzichtstudie stelt Maxwell [4] dat het de combinatie is van de signalen van verschillende controles die het beste helpt om frauduleuze transacties te detecteren.

5.3.1. Het actief bestrijden van geldezels en geldezelrekeningen

Het aanpakken van geldezels en geldezelrekeningen is cruciaal om onlinefraude te bestrijden. Zonder geldezel(rekening) geen geld [77-79].

Een geldezel is iemand die (soms onbedoeld) geld witwast voor een crimineel door zijn bankrekening of pinpas uit te lenen [80]. Geldezels kunnen het geld fysiek van de rekening halen waar de fraudeur het naartoe heeft laten sturen, zodat die zijn identiteit niet hoeft te onthullen. De praktijk leert dat het tegenwoordig vooral gaat om geldezelrekeningen, die meestal digitaal zijn. Deze rekeningen worden door fraudeurs soms handmatig en soms volledig geautomatiseerd in grote aantallen geopend. Ook worden dit soort rekeningen geoogst, soms van nietsvermoedende burgers, soms gekocht. De ervaring van cybersecuritybedrijven laat zien dat circa de helft van deze geldezelrekeningen door fraudeurs zelf wordt geopend, bijvoorbeeld met gegevens van mensen uit datahacks. Circa 40% wordt geoogst, bijvoorbeeld door advertenties op sociale media voor eenvoudig administratief werk. Het kleine restant komt van rekeningovername door de fraudeurs (phishing, malware, etc.). Het is daarom handig als de verzendende bank de informatie over de risicoscore (bijv. hoeveel dagen oud is de ontvangende bankrekening?) van de ontvangende bank krijgt.

Britse banken zijn verplicht tot strenge geldezelcontroles [79]. De Britse *Financial Conduct Authority* heeft een aantal rapporten uitgebracht waarin *best practices* voor het opsporen van geldezels worden geïdentificeerd [78, 79]. Het gaat onder meer om strenge controles op het openen van rekeningen, analyses van inkomende transacties en van afwijkend gedrag, zoals snelle uitgaande transacties vanaf deze 'ontvangende' rekening. Deze maatregelen zijn vaak dezelfde als die om witwassen tegen te gaan. Recent zijn fraudeurs zich meer op crypto gaan richten, wat een extra uitdaging oplevert voor handhavers [3].

5.3.2. Afwijkend gedrag van de klant op zijn bankrekening

Detectie op basis van het gedrag dat men ziet op de bankrekeningen is inmiddels een standaarddetectiemethode die in Nederland die al in gebruik werd genomen tijdens de grote golf van onlinebankierenfraude in Nederland tussen 2010 en 2015. Doel is om afwijkend gedrag te detecteren in onlineactiviteiten op betalende en ontvangende rekeningen en zo geldezels op te sporen en transacties te stoppen. Men kan er bijvoorbeeld op letten of er voortdurend wordt ingelogd en ander ongebruikelijk gedrag. Het gaat bijvoorbeeld ook om onverwachte of onverklaarbare stortingen op rekeningen, snelle verspreiding van geld via netwerken van rekeningen, voor de klant ongebruikelijk hoge overboekingen waarbij het geld vervolgens vaak binnen enkele minuten na ontvangst wordt doorgesluisd; verplaatsing van geld naar internationale jurisdicties en snelle opnames van geld bij geldautomaten [81-83]. Deze vorm van detectie is zeer effectief gebleken.

5.3.3. Gedragsbiometrie op de uitgaande transactiestroom

Gedragsbiometrische metingen zijn moderne methoden om veranderingen te detecteren wanneer een klant online een transactie uitvoert op aanwijzing van een fraudeur [84, 85]. Het kan gaan om de wijze waarop het mobieltje vastgehouden wordt, welk deel van het scherm gebruikt wordt, hoe snel men typt en met welke vingers, hoe men swipet, hoe de muis wordt bewogen, etc. Geldezelrekeningen hebben vaak een aantal kenmerken waardoor ze met de juiste detectiemethodes al herkenbaar zijn voordat ze daadwerkelijk door de fraudeur worden gebruikt [70].

Gedragsbiometrie is zeer effectief gebleken bij een aantal banken in het VK en Australië [86]. Het VK beveelt gedragsbiometrie sterk aan voor banken [78, 79]. Het gebruik van gedragsbiometrie heeft financiële instellingen geholpen om tot 90% van de geldezelrekeningen te detecteren vóór de bestaande fraude- en antiwitwasmaatregelen [87]. Een grote bank in het VK zag, dankzij gedragsbiometrie, de fraudedetectiepercentages met 42% stijgen en kon naar schatting jaarlijks £ 1 miljoen aan fraude voorkomen [88]. Nieuw-Zeelandse banken starten met deze werkwijze [89].

Het is vermeldenswaard dat voor preventie van fraude technische maatregelen, indien mogelijk, vaak de voorkeur verdienen boven 'zachtere' maatregelen zoals educatie: ze zijn moeilijk te omzeilen door fraudeurs en dat is met name een voordeel bij kwetsbare groepen, zoals ouderen of mensen met een verstandelijke beperking, bij wie educatie waarschijnlijk minder goed aanslaat. Naarmate de verzamelde gegevens uitgebreider zijn, wordt deze methode wat privacygevoeliger.

5.3.4. 'Is de klant in gesprek?' Gegevensuitwisseling tussen banken en telecombedrijven

Banken in Nederland en elders hebben veel last van bankhelpdeskfraude ofwel '*bank spoofing*'. Bij bankhelpdeskfraude ofwel spoofing, lijkt het alsof de klant door de bank wordt gebeld omdat het telefoonnummer hetzelfde is als het nummer van de bank. De fraudeur houdt de klant aan de lijn met een angstwekkend verhaal en haalt hem over om geld over te maken naar een bankrekening waar hij als fraudeur controle over heeft. In Nederland zijn de verliezen als gevolg van spoofing €22.739.154 in 2024, op een totaal verlies voor de banken door het geheel aan onlinefraude van €29.258.933 [90]. Technisch gezien bestaat de mogelijkheid voor een bank om in samenwerking met een telecombedrijf te controleren of een klant een mobiel gesprek voert terwijl hij tegelijkertijd onlinetransacties uitvoert of geld opneemt bij een filiaal. In Groot-Brittannië bestaat *Scam Signal*. *Scam Signal* is een samenwerking tussen mobiele netwerkoperators EE, Virgin Media, O2, Three en Vodafone. *Scam Signal* wordt via een API[11] geleverd en stelt banken in staat om met behulp van realtimenetwerkanalyse verbanden tussen mobiele data en frauduleuze transacties effectiever te identificeren. Een experiment van drie maanden van Vodafone en een Britse bank leidde tot een daling van 40% in succesvolle scams [91]. Vergelijkbare maatregelen zijn genomen in de Filipijnen, Singapore, Australië [66] en Nieuw-Zeeland [89].

Ook de Nederlandse banken willen graag bij telecomaanbieders kunnen checken of iemand telefonisch in gesprek is tijdens het overboeken van geld. In 75% van de gevallen blijkt er sprake van fraude te zijn [92]. Deze gevallen kunnen dus mogelijk worden voorkomen. Hiertoe is een wijziging van de Telecomwet nodig [93].

5.3.5. 'Money lock'

Singaporese banken hebben een 'Money Lock'-functie. Hiermee kunnen klanten een bedrag op een rekening 'vergrendelen' zodat dit niet snel kan worden overgemaakt. Dit kan handig zijn bij een personificatie (criminelen doen zich voor als iemand van een bank, de politie of een andere vertrouwde organisatie), waarbij de fraudeur urgentie creëert voor actie [86].

5.3.6. Overige controlemaatregelen

a) Wordt de klant gebeld door de bank?

Verschillende banken hebben een functie aan hun mobiele app toegevoegd waarmee de klant kan verifiëren of het de bank is die de klant belt. Een aantal banken in Nederland heeft deze optie in de mobiele applicatie ingebouwd.

b) Is een bericht frauduleus?

Ask Silver, een bedrijf in het VK, experimenteert met Britse banken om een waarschuwing bij een transactie te plaatsen. Klanten kunnen dan informatie over de transactieactiviteit opgeven (bijv. URL of screenshot) om te bepalen of sprake is van fraude.

c) Training bankmedewerkers

Bankmedewerkers moeten specifiek worden getraind in hoe en met welke foefjes consumenten worden opgelicht. Zo'n training moet ook de psychologie van fraude omvatten. Deze kennis is

[11] Een API (Application Programming Interface) is een software-interface waarmee twee applicaties met elkaar kunnen communiceren.

cruciaal voor de interactie met klanten die slachtoffer zijn geworden van fraude en die vaak door een fraudeur zijn 'getraind' in wat zij moeten antwoorden bij vragen van de bank.

5.4. Het vergoeden van verliezen van klanten

In het VK worden sinds 7 oktober 2024 verliezen bij geautoriseerde fraude vergoed door de banken en andere financiële dienstverleners [5]. Dit staat in contrast met het beleid van de Nederlandse banken, die alleen slachtoffers van *bank spoofing* vergoeden [94].[12]

In het VK vergoeden de banken een breed scala aan scams waarbij slachtoffers worden misleid om de fraudeur te betalen, zoals aankoopfraude, beleggingsfraude, onlinedatingfraude, of factuurfraude (waarbij fraudeurs valse facturen sturen) [5]. Er zijn beperkingen: de vergoedingen gelden voor binnenlandse transacties, een aantal betalingsvormen is uitgesloten (bijv. cash en creditcards) en er is een maximumbetaling van £85,000 [5]. Belangrijk is dat, gegeven deze beperkingen, voor 99% van de claims een vergoeding wordt ontvangen, qua volume is dit 90% van de waarde [95].
Zoals hierboven vermeld worden kwetsbare klanten in het VK extra goed beschermd. Zij worden gecompenseerd zonder eigen risico (maar met hetzelfde maximum), ook wanneer zij voor fraude waren gewaarschuwd, slachtofferschap meerdere keren is voorgekomen en/of te laat is gemeld [43].

Een belangrijke motivatie voor dit beleid is dat het banken stimuleert om te investeren in betere detectie van fraude en financiële criminaliteit [95]. Zo worden door banken niet altijd voldoende controles uitgevoerd bij het openen van een bankrekening [78, 96].

De compensatieverplichting in het VK leidde tot op heden niet tot problemen in de financiële sector maar wel tot een daling met een derde van het aantal claims in de eerste vier maanden na de invoering van de nieuwe regeling, naar alle waarschijnlijkheid omdat banken nu meer investeren in de veiligheid van hun systemen [95]. Volgens UK Finance [97] was er in de eerste zes maanden van 2024 een schade door fraude van £571,7 miljoen, een daling van 1,5% ten opzichte van de eerste helft van 2023.

In Nieuw-Zeeland worden vanaf 30 november 2025 onder bepaalde voorwaarden alle frauduleuze transacties, geautoriseerd of niet-geautoriseerd, vergoed tot NZ$500,000 (€261.450[13]). De voorwaarden: de klant was te goeder trouw, nam normale voorzorgsmaatregelen, heeft het incident gerapporteerd aan de politie, en heeft de goederen of diensten niet gekocht via sociale media of een gelijksoortige onlinemarktplaats. De banken betalen de schade alleen terug als de door de bank gedefinieerde controles ter voorkoming van fraude niet goed werkten [89].

5.5. Nieuw vergoedingsprincipe: vergoeden van verliezen door de verzendende *en* de ontvangende bank

Wanneer banken slachtoffers compenseren gaat het meestal om de verzendende bank die de vergoeding betaalt (zie paragraaf 5.2). Een interessante ontwikkeling is de aandacht voor de rol van de ontvangende bank [98]. In het VK wordt de vergoeding aan slachtoffers nu 50/50 verdeeld tussen de verzendende en de ontvangende bank [99] – een betere spreiding van verantwoordelijkheden tussen beide banken.

Geconstateerd is dat ontvangende banken steken kunnen laten vallen in hun veiligheidsbeleid. Palla [96] laat zien wat er bij een CEO-fraude waar een bedrijf voor $700,000 werd opgelicht allemaal mis kan gaan bij de ontvangende bank (*Business Email Compromise* (BEC). Er waren tenminste tien

[12] In Nederland hebben de banken een coulance regime, waarbij zij alleen vergoeden bij bank *spoofing*, waarbij fraudeurs pretenderen namens de bank te bellen en hun eigen telefoonnummer er anders laten uitzien, zodat het lijkt alsof het slachtoffer door het telefoonnummer van de bank wordt gebeld. Op de website staat expliciet: '*De coulanceregeling geldt dus niet voor andere vormen van fraude waarbij klanten zelf de transacties goedkeuren*'. Dt staat dus in contrast met het beleid van banken in het VK.
[13] Waarde in Euro op het moment van schrijven, dd 27 april, 2025.

duidelijke gebreken bij de ontvangende bank die de transactie hadden kunnen tegenhouden. Enkele hiervan zijn: 1) de ontvangende bank opende een nieuwe persoonlijke rekening voor een klant maar verifieerde zijn adres niet; 2) de inkomende stortingen van het slachtoffer naar de ontvangende bank kregen een code mee van een 'business-to-business'-transactie maar werden verzonden naar een persoonlijke rekening bij de ontvangende bank; 3) de inkomende transactiebedragen waren afwijkend voor een dergelijke persoonlijke rekening; 4) de naam van de inkomende transactie kwam niet overeen met de rekeningnaam bij de ontvangende bankrekening; 5) de ontvangende bank had anti-witwassoftware die afwijkingen detecteerde maar deze afwijkingen werden genegeerd. Voor details, zie: Palla [96]. Deze casus laat zien dat de ontvangende bank een even belangrijke rol speelt als de verzendende bank, vooral met het oog op de detectie van geldezels en geldezelrekeningen.

Het spreiden van de verantwoordelijkheden tussen de verzendende en ontvangende banken met betrekking tot de vergoeding voor slachtoffers is een belangrijke motivatie voor de betrokken instellingen om hun beleid aan te passen om fraude te voorkomen. De banken die hun (detectie)processen niet op orde hebben en daardoor veel geldezelrekeningen hebben, lopen met de huidige regelgeving geen enkel risico omdat ze niet aansprakelijk zijn. Dit tot grote frustratie van de banken die hun zaken wel op orde hebben. In het VK worden nu lijsten gepubliceerd met de namen van banken die relatief veel geldezels hebben: naming-and-shaming. Dit heeft zeer zeker sterk bijgedragen aan het positieve effect dat hierboven (paragraaf 5.2) werd genoemd. Lastig voor toepassing in Nederland is dat de politie waarneemt dat ontvangende (frauduleuze) rekeningen frequenter in het buitenland zijn gesitueerd [35].

5.6. Het blokkeren van frauduleuze oproepen en sms-berichten

Klanten ontvangen soms frauduleuze sms-berichten. Technische oplossingen helpen om dergelijke berichten te blokkeren, bijvoorbeeld door een *call-blocking app* te downloaden [100].

5.7. Fraudebestrijding op ministerieel niveau

Verschillende regeringen zijn van mening dat fraude een bedreiging is voor de nationale veiligheid [101]. Zweden legt momenteel om verschillende redenen meer nadruk op cybersecurity, waarbij ook wordt verwezen naar de geopolitieke situatie. Daarbij past in de Zweedse optiek ook gegevensuitwisseling [64].
In het VK is nu een minister voor fraude geïnstalleerd. Dit mede omdat de vorige regering constateerde dat '*Fraud now accounts for over 40% of crime but receives less than 1% of police resource.*' [101].

5.8. Aanbevelingen om fraude bestrijding beter te organiseren

De Global Anti-Scam Alliance [12] heeft een reeks aanbevelingen gedaan, gebaseerd op de praktijkervaring van internationale organisaties die actief zijn in de strijd tegen fraude. Een aantal daarvan is eerder al genoemd. Daarnaast wordt aanbevolen:

- Faciliteer één nationaal, eenvoudig, onlinerapportageplatform.
- Creëer één centraal steunpunt voor slachtoffers.
- Ontwikkel meer technische middelen om gebruikers te beschermen.
- Zet een speciaal nationaal consumentencyberbeveiligingscentrum op.
- Zet een wereldwijde hub op voor het delen van fraudegegevens.
- Maak dienstverleners verantwoordelijk en aansprakelijk voor het mogelijk maken van fraude.
- Sta preventieve actie toe (waarschuwen, blokkeren, stoppen).
- Zet een internationaal netwerk op voor onderzoek en detectie van fraude.

In tabel 1 zijn die aanbevelingen grotendeels uiteengezet.

Bronnen

1. Politie Eenheid Landelijke Expertise en Operaties, *Online fraude 2024. Elf fraudevormen in beeld*. 2024: Driebergen, Nl.
2. EUROPOL. *Online fraud schemes: a web of deceit*. 2023; Available from: https://www.europol.europa.eu/cms/sites/default/files/documents/Spotlight-Report_Online-fraud-schemes.pdf.
3. IC3, *Internet crime report 2024*, F.B.o.I. (FBI), Editor. 2024, Federal Bureau of Investigation, Internet Crime Complaint Center: Washington, D.C.
4. Maxwell, N.J., *A Survey and Policy Discussion Paper: "Lessons in private-private financial information sharing to detect and disrupt crime"*. 2022, Future of Financial Intelligence Sharing (FFIS) research programme: London, UK.
5. UK Finance. *Authorised Push Payment Fraud Reimbursement*. 2024; Available from: https://www.ukfinance.org.uk/authorised-push-payment-fraud-reimbursement.
6. Gov.UK. *Minister of State (Lords Minister). The Rt Hon Lord Hanson of Flint* 2024; Available from: https://www.gov.uk/government/people/david-hanson.
7. Bullee, J.-W. and M. Junger, *How effective are social engineering interventions? A meta-analysis.* Information and Computer Security, 2020. **28**(5): p. 801-830.
8. Junger, M., B. Veldkamp, and L. Koning, *Fraudevictimisatie in Nederland (Fraud Victimization in the Netherlands)*. 2022, University of Twente: Enschede, Nl. p. 50.
9. Cross, C., K. Richards, and R. Smith, *The reporting experiences and support needs of victims of online fraud.* Trends and Issues in crime and criminal justice, 2016. **518**: p. 1-14.
10. Cross, C., K. Richards, and R.G. Smith, *Improving responses to online fraud victims: An examination of reporting and support.* 2016.
11. SPF, *Annual Scams and Cybercrime Brief 2024*. 2025, Singapore Police Force: Singapore.
12. GASA. *Ten recommendations to turn the tide on online scams*. 2023; Available from: https://www.gasa.org/global-anti-scam-summit-2022-gass.
13. Hartel, P., R. + Wegberg, and M. van Staalduinen, *Investigating sentence severity with judicial open data: A case study on sentencing high-tech crime in the Dutch criminal justice system.* European Journal on Criminal Policy and Research, 2023. **29**(4): p. 579-599.
14. DeLiema, M., G.R. Mottola, and M. Deevy, *Findings from a pilot study to measure financial fraud in the United States.* Available at SSRN 2914560, 2017.
15. Ilbiz, E. and C. Kaunert, *Cybercrime, Public-Private Partnership and Europol*, in *The Sharing Economy for Tackling Cybercrime*. 2023, Springer International Publishing: Cham. p. 13-28.
16. Rossieau, E. and D.M. Sanders, *Strategisch kader interventieaanpak*. 2022: Den Haag, Nl.
17. CBS. *Geregistreerde criminaliteit; soort misdrijf, regio*. 2025; Available from: https://opendata.cbs.nl/#/CBS/nl/dataset/83648NED/table.
18. Statistics Netherlands, *Cybercrime achterhalen in aangiften (Detecting cybercrime in reports)*. 2023, Centraal Bureau voor de Statistiek: The Hague, Nl.
19. Montoya, L., M. Junger, and P. Hartel *How 'Digital' is Traditional Crime?* European Intelligence and Security Informatics Conference (EISIC) 2013, 2013. 31-37.
20. Office For National Statistics, *Crime in England and Wales: year ending September 2022. Crime against households and adults using data from police-recorded crime and the Crime Survey for England and Wales (CSEW)*. 2023, Office For National Statistics: London, UK. p. 34.
21. Kemp, S., F. Miró-Llinares, and A. Moneva, *The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain.* European Journal on Criminal Policy and Research, 2020. **26**(3): p. 293-312.
22. PwC, *PwC's Global Economic Crime and Fraud Survey 2022. Protecting the perimeter: The rise of external fraud*. 2022, PricewaterhouseCoopers US.
23. Gee, J. and M. Button, *The Financial Cost of Fraud 2021. The latest data from around the world*. 2021, Crowe & University of Portsmouth: London, UK.

24. CBS, *Cybersecuritymonitor 2023*. 2024, Centraal Bureau voor de Statistiek (Statistics Netherlands): Den Haag, Nl. p. 65.

25. CBS, *Veiligheidsmonitor 2016*. 2017, Centraal Bureau voor de Statistiek, CBS. Ministerie van Veiligheid en Justitie: Voorburg/Heerlen.

26. CBS, *Minder traditionele criminaliteit, meer online criminaliteit*. 2022, Centraal Bureau voor de Statistiek (CBS): Den Haag, Nl.

27. CBS, *Schade van criminaliteit tegen burgers*. 2024, Centraal Bureau voor de Statistiek (Statistics Netherlands): Den Haag, Nl. p. 65.

28. Betaalvereniging Nederland. *Marktonderzoeken & infographics*. 2025; Available from: https://www.betaalvereniging.nl/actueel/achtergrondinformatie/infographics/.

29. Halpin, D. and S. Todd, *Public-Private Collaboration for Combatting Cyber Fraud*, in *Financial Crime, Law and Governance: Navigating Challenges in Different Contexts*, D. Goldbarsht and L. de Koker, Editors. 2024, Springer Nature Switzerland: Cham. p. 287-311.

30. Ho, H., R. Ko, and L. Mazerolle, *Situational Crime Prevention (SCP) techniques to prevent and control cybercrimes: A focused systematic review.* Computers & Security, 2022. **115**: p. 102611.

31. Betaal Vereniging Nederland. *Fraude betalingsverkeer blijft dalen*. 2014 23 september 2014 2025]; Available from: https://www.betaalvereniging.nl/actueel/nieuws/fraude-betalingsverkeer-blijft-dalen/.

32. Jensen, R.I.T., J. Gerlings, and J. Ferwerda, *Do awareness campaigns reduce financial fraud?* European Journal on Criminal Policy and Research, 2024: p. 1-36.

33. SurePay, *België gaat banken en hun klanten beschermen tegen fraude en fouten*. 2022.

34. Softwarepakketten.nl, *IBAN-Naam Check, afgelopen jaar 35.923.805 fraude waarschuwingen: 3 manieren om fraude te voorkomen*. 2022, Softwarepakketten.nl.

35. Rienties, M. and P. Hagenaars, *The Importance of Fraud Prevention in the Digital Age. Collaborating for Security under PSD3*, in *Toekomst van het betalingsverkeer*. 2025: Amsterdam.

36. Abraham, J., et al., *The Global State of Scams -2023*, in *4th Global Anti-Scam Summit (GASS)*, G.A.-S.A. (GASA), Editor. 2023, Global Anti-Scam Alliance (GASA): Lisbon, Portugal.

37. Dunning, D., *The Dunning–Kruger effect: On being ignorant of one's own ignorance*, in *Advances in experimental social psychology*. 2011, Elsevier. p. 247-296.

38. Bullée, J.-W. and M. Junger, *Social engineering: digitale fraude en misleiding.* Justitiële Verkenningen, 2020. **46**(2).

39. Snyder, J.A. and K.A. Golladay, *It Happened Again: Differences Between Single and Repeat/Poly-Victimization Among Financial Fraud Victims.* Journal of White Collar and Corporate Crime, 2024. **5**(1): p. 46-57.

40. Moneva, A., et al., *Repeat victimization by website defacement: An empirical test of premises from an environmental criminology perspective.* Computers in Human Behavior, 2021. **126**: p. 106984.

41. Statline, *Slachtofferschap online criminaliteit; persoonskenmerken*. 12 april 2024, Centraal Bureau voor de Statistiek: The Hague, Nl.

42. Palla, K., *US state governments take action to protect the elderly from scams*. 2023, BioCatch: London, UK.

43. PSR, *Authorised push payment fraud reimbursement. The Consumer Standard of Caution Exception Guidance*. 2023, Payment Systems Regulator.

44. PSR, *Policy statement, "Fighting authorized push payment scams: final decision*. 2023, Payment Systems Regulator.

45. Button, M., et al., *What really works in preventing fraud against organisations and do decision-makers really need to know?* Security Journal, 2024. **37**(3): p. 965-983.

46. Prenzler, T., *What works in fraud prevention: a review of real-world intervention projects.* Journal of Criminological Research, Policy and Practice, 2020. **6**(1): p. 83-96.

47. Gotelaere, S. and L. Paoli, *Prevention and control of financial fraud: A scoping review.* European Journal on Criminal Policy and Research, 2022: p. 1-21.

48. Maxwell, N.J., *A new era of private sector collaboration to fight economic crime*. 2025, Future of Financial Intelligence Sharing (FFIS) research programme: London, UK.

49. May, T. and B. Bhardwa, *What Do We Know About Organised Crime and Fraud?*, in *Organised Crime Groups involved in Fraud*, T. May and B. Bhardwa, Editors. 2018, Springer International Publishing: Cham. p. 11-29.

50. van Onna, J.H.R., V.R. van der Geest, and A.J.M. Denkers, *Rule-violating behaviour in white-collar offenders: A control group comparison.* European Journal of Criminology, 2018. **17**(3): p. 332-351.

51. Dickinson, H., *Fraud report 2015*. 2015, CIFAS: London, UK.

52. EUROPOL, *Why is cash still king? a strategic report on the use of cash by criminal groups as a facilitator for money laundering*. 2015, Europol financial intelligence group: The Hague, Nl.

53. COE, *CETS 198 –Laundering of the Proceeds from Crime and Financing of Terrorism, 16.V.2005*, in *Council of Europe Treaty Series - No. 198*, C.o.E. Convention, Editor. 2005, Council of Europe Convention: Strasbourg, France.

54. DNB. *Witwassen en crimineel geld bestrijden*. 2025 [cited 2025; Available from: https://www.dnb.nl/betrouwbare-financiele-sector/witwassen-en-crimineel-geld-bestrijden/.

55. Cifas. *What is the National Fraud Database?* 2025; Available from: https://www.cifas.org.uk/fraud-prevention-community/combined-threat-protect/national-fraud-database.

56. Cifas. *Insider Threat Database*. 2025; Available from: https://www.cifas.org.uk/fraud-prevention-community/combined-threat-protect/insider-threat-database.

57. Home Office, *Data Sharing for the Prevention of Fraud Code of practice for public authorities disclosing information to a specified anti-fraud organisation under sections 68 to 72 of the Serious Crime Act 2007*. 2015, Her Majesty's Stationery Office: London, UK.

58. ICO. *Our purpose*. 2025; Available from: https://ico.org.uk/about-the-ico/our-information/our-strategies-and-plans/ico25-strategic-plan/our-purpose/.

59. ICO. *Sharing personal information when preventing, detecting and investigating scams and frauds*. 2025; Available from: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-sharing/sharing-personal-information-when-preventing-detecting-and-investigating-scams-and-frauds/.

60. Staso, D.D. *Why (some) personal data is open data in Sweden*. 2024; Available from: https://odeco-research.eu/?p=3856.

61. Wikipedia. *Resident registration*. 2025; Available from: https://en.wikipedia.org/wiki/Resident_registration.

62. SafeAML, *from data to discoveries: safeAML is changing the game for money laundering*, Spotixx, Editor. 2025.

63. Dharmaraj, S., *Thailand: International Cooperation to Combat Online Crime*. 2025, https://opengovasia.com/: Singapore.

64. Rockborn, N., A. Svensson, and A. Hansson, *Data Protection in Sweden: An Overview*. 2025, Chambers and Partner: Stockholm, Sweden.

65. ICO. *Regulatory Sandbox*. 2025 [cited 2025 26 April 2025]; Available from: https://ico.org.uk/for-organisations/advice-and-services/regulatory-sandbox/.

66. PWC, *How banks and telecoms can unite against fraud*. 2025, PricewaterhouseCoopers Czech Republic: Prague, Czech Republic.

67. The Treasury, *Scams Prevention Framework – Protecting Australians from scams*, A.G.T. Treasury, Editor. 2025: Canberra, Australia.

68. GSE. *A global clearing house for real-time sharing of scam and fraud signals*. 2025; Available from: https://www.globalsignalexchange.org/.

69. CIFAS, *Leaders in fraud prevention*, in *Fraudepreventie en datadelen*. 2017, CIFAS: Utrecht, Nl.

70. Fokma, W., *How to jointly use the EU laws on Fraud and Money Laundering for information exchange*. 2024, Surepay: Utrecht, Netherlands.

71. Calvery, J., *Harnessing the power of AI to fight financial crime*. 2023, HSBC: London, UK.

72. Cifas. *Complaints Form*. 2025 20-04-2025]; Available from: https://www.cifas.org.uk/contact-us/i-want-to-make-a-complaint/complaints-form.

73. EBA, *EBA alerts on the detrimental impact of unwarranted de-risking and ineffective management of money laundering and terrorist financing risks*. 2022, European Banking Authority: Paris, France.

74. Staats, W., et al., *Nieuwe manieren van samenwerken: Een systematische literatuurreview naar de (effectiviteit van) publiek-private samenwerking op het gebied van financieel-economische criminaliteit en cybercrime*. 2021, Free University Amsterdam: Amsterdam, Nl. p. 50.

75. AD, *Vijf jongeren aangehouden voor oplichting op Marktplaats*, in *Algemeen Dagblad*. 2017: Rotterdam, Nl.

76. Politie, E.Z.-W.-B., *Aanhoudingen in grootschalig onderzoek naar phishing*, in *Etten-Leurs Nieuws.nl*. 2017: Etten-Leur, Nl.

77. Bleau, H., *Mule Accounts: Ripping the Mask Off the Money Laundering Problem*. 2025, BioCatch Blog Channel: New York, USA.

78. Financial Conduct Authority, *Proceeds of fraud - Detecting and preventing money mules*, in *Multi-firm reviews*. 2023: London, UK.

79. Financial Conduct Authority, *Firms' use of the National Fraud Database (NFD) and money mule account detection tools*, in *Multi-firm reviews*. 2025: London, UK.

80. Veiliginternetten.nl. *Geldezels en bankhelpdeskfraude: NVB en Banken lanceren nieuwe campagne*. 2024; Available from: https://veiliginternetten.nl/geldezels-en-bankhelpdeskfraude-nieuwe-campagne/.

81. Dalsaniya, A., *AI for Behavioral Biometrics in Cybersecurity: Enhancing Authentication and Fraud Detection.* Int. Res. J, 2023. **10**: p. a108-a122.

82. Morake, A., L.T. Khoza, and T. Bokaba, *Biometric technology in banking institutions:'The customers' perspectives'.* South African Journal of Information Management, 2021. **23**(1): p. 1-12.

83. Finnegan, O., et al., *The utility of behavioral biometrics in user authentication and demographic characteristic detection: a scoping review.* Systematic Reviews, 2024. **13**(1): p. 61.

84. Onesi-Ozigagun, O., et al., *AI-driven biometrics for secure fintech: Pioneering safety and trust.* Journal Name Unspecified, 2024.

85. Kadena, E., L.C.R. Salvador, and Z. Rajnai. *Behavioral Biometrics for more (dis) trust and security*. in *2022 IEEE 16th International Symposium on Applied Computational Intelligence and Informatics (SACI)*. 2022.

86. Palla, K., *Role of Banks in Fighting Consumer Financial Scams*, GASA, Editor. 2025, Global Anti-Scam Alliance: https://www.gasa.org/post/role-of-banks-in-fighting-consumer-financial-scams.

87. Palla, K., *Taking Action on Money Mules. Four Key Components to Build an Effective Program. White paper*. 2024, BioCatch: New York, USA.

88. BioCatch, *Meeting the Hidden Cost of Strong Customer Authentication (SCA)*. 2022, BioCatch: London, UK.

89. East, S., et al., *Fraud and Scams Update: Banks commit to new protections – and reimbursement - for scam victims*. 2025, Bell Gully.

90. NVB. *NVB waarschuwt: 'Blijf opletten voor geniepige trucs bij bankhelpdeskfraude!'*. 2025 26 april 2025]; Available from: https://www.nvb.nl/nieuws/nvb-waarschuwt-blijf-opletten-voor-geniepige-trucs-bij-bankhelpdeskfraude/.

91. The Fintech Times, *Telecommunication-Born APP Fraud*. 5 November 2024: London, UK.

92. NVB, *Banken en telecombedrijven willen wijziging Telecommunicatiewet om fraude tegen te gaan*. 2025, Nederlandse Vereniging van Banken (NVB): Amsterdam, Nl.

93. Schermer, B.W. and T. Schop, *Cross-sectorale gegevensdeling tussen private partijen voor fraudebestrijding*, Ministerie van Justitie en Veiligheid, Editor. 2019, Considerati: Den Haag, Nl. p. 55.

94. NVB. *Toetsingscriteria voor coulance bij bankhelpdesk fraude (spoofing)*. 2021; Available from: https://www.nvb.nl/nieuws/toetsingscriteria-voor-coulance-bij-bankhelpdesk-fraude-spoofing/.

95. Frost, J. *The collapse of the UK fintech sector that wasn't: Insights from five months of mandatory reimbursement*. BioCatch Blog Channel 2025; Available from: https://www.biocatch.com/blog/insights-fintech-collapse-mandatory-reimbursement.

96. Palla, K., *Red Team Testing Part 2- Receiving Bank Activities*. 2023, Greenway Solutions: Charlotte, NC, USA.

97. UK Finance, *Over £570 million stolen by fraudsters in the first half of 2024* 2025, UK Finance: London, UK.

98. Palla, K., *The New and Surprising Role of Receiving Banks in Scam Reimbursement*, in *BioCatch Blog Channel*. 2023, BioCatch: New York, NY.

99. PSR, *Specific Requirement 1 on the Faster Payments Operator to insert APP scam reimbursement rules into the Faster Payments Scheme rules*, in *Specific Requirement 1 (July 2024) (FPS APP scam reimbursement rules)*, Payment System Regulator, Editor. 2024: London, UK.

100. FTC, *How To Block Unwanted Calls*. Consumer Advice. 2025, Washington, D.C.: Federal Trade Commission.

101. UK Government, *Fraud Strategy: stopping scams and protecting the public*, H. Office, Editor. 2023, Home Office: London, UK.

102. OM, *Cybercrime & gedigitaliseerde criminaliteit*. 2025, Openbaar Ministerie: Den Haang, Nl.

103. AP, *Rapportage Datalekken 2023*. 2024, Autoriteit Persoonsgegevens: Den Haag 2024.

104. CBS, *Cybersecuritymonitor 2017*. 2017, Centraal Bureau voor de Statistiek (CBS): Den Haag, Nl.

Deze factsheet is tot stand gekomen in het kader van de samenwerking van de Tweede Kamer met De Jonge Akademie, de Koninklijke Nederlandse Akademie van Wetenschappen (KNAW), de Nederlandse Federatie van Universitair Medische Centra (NFU), de Nederlandse Organisatie voor Wetenschappelijk Onderzoek (NWO), TNO en de Vereniging Universiteiten van Nederland (UNL).

Disclaimer

De Jonge Akademie, KNAW, NFU, TNO en UNL bemiddelen tussen parlementaire kennisvraag en wetenschappelijk kennisaanbod. De informatie in het kader van Parlement en Wetenschap is afkomstig van vooraanstaande wetenschappers, maar niet onderworpen aan peer review en niet door de wetenschaps-organisaties geverifieerd.

Bijlage

Definities van cybercrime, gedigitaliseerde criminaliteit, incidenten en cybersecurity

Onlinefraude wordt vaak besproken in de context van de begrippen cybercrime, gedigitaliseerde criminaliteit, cybersecurity en incidenten. Hieronder bespreken we de definities.

Politie en OM maken onderscheid tussen cybercrime en gedigitaliseerde criminaliteit:

1) **Cybercrime**: het doel is criminaliteit binnen ICT-systemen, zoals het overnemen van een computer, het platleggen van een netwerk of het stelen van gegevens [102] (ransomware of *Distributed Denial-of-Service*-aanval (*DDoS*-aanval));
2) **Gedigitaliseerde criminaliteit**: criminaliteit die al bestond, zoals diefstal en oplichting, maar die nu met behulp van ICT wordt gepleegd. Denk aan het niet leveren van goederen die je online hebt besteld, WhatsAppfraude of digitale stalking [102]. In dat begrippenkader is onlinefraude dus gedigitaliseerde criminaliteit.

Het CBS omschrijft cybercrime als '*alle delicten die gepleegd worden met behulp van ICT of de informatie die door ICT wordt verwerkt*'. Het omvat – in de definities van de politie en het OM – dus zowel cybercrime als gedigitaliseerde criminaliteit.

Het CBS heeft een aanpak die, afhankelijk van zijn databronnen, verschilt. De cybersecuritymonitor is gebaseerd op enquêtes bij bedrijven. Hier sluit het CBS aan bij de in cybersecurity gangbare term 'securityincidenten'. Securityincidenten zijn gebeurtenissen die schade aan een ICT-systeem toebrengen. Zij kunnen ontstaan door moedwillige acties (een misdrijf) of per vergissing, wanneer iemand per ongeluk op een phishinglink klikt. Het onderscheid is in de praktijk vaak een combinatie van een fraudeur die phishing verstuurt en een slachtoffer dat klikt.

Soms ontstaan problemen ook door fouten van de individuen die werken met het systeem. Zo zijn datalekken ook vaak het gevolg van fouten in een administratie, zoals verkeerd verzonden brieven, of worden persoonsgegevens per ongeluk gepubliceerd [103]. Omdat oorzaken niet gelijk helder zijn, spreekt men in het veld meestal over 'incidenten' [104]. In de cybersecuritymonitor presenteert het CBS daarom cijfers over 'cybersecurityincidenten' [24].

CBS-statistieken over meldingen en aangiften bij de politie sluiten echter aan bij de wettelijke categorieën en geven daarmee weer andere informatie, die niet direct kan worden gerelateerd aan de cijfers van de cybersecuritymonitor.

De factsheet zelf behandelt in hoofdzaak onlinefraude, wat een onderdeel is van de 'gedigitaliseerde criminaliteit' in politie-/OM-termen. We gebruiken het begrip incidenten voornamelijk als het gaat om onlinefraude, tenzij de bron waarnaar wordt verwezen een ander begrip hanteert. Dit sluit ook aan bij de literatuur over preventie, die een onderscheid maakt tussen activiteiten gericht op mensen en activiteiten gericht op situaties en het verstoren van een modus operandi.