

Aan: cie.jv@tweedekamer.nl

Onderwerp: Preventie van onlinefraude, lessen uit het buitenland

Van: prof. dr. Marianne Junger (Universiteit Twente), Ken Palla MBA, ing. Wiebe Fokma, prof. dr. ir. Bernard Veldkamp (Universiteit Twente)

Datum: 12 september, 2025

Een derde van alle incidenten betreft online fraude, zo blijkt uit politiegegevens. Fraude vormt een bedreiging voor burgers en bedrijven, en is een gevaar voor de nationale veiligheid. Fraudebestrijding is daarom absoluut noodzakelijk. Ik stel vier principes voor fraudebestrijding voor: 1) preventie, samenwerking en coördinatie; 2) educatie; 3) detectie; en het overkoepelende principe: 4) fraudebestrijding als gedeelde verantwoordelijkheid.

1. PREVENTIE, SAMENWERKING EN COÖRDINATIE

Ik noem hier vier onderwerpen.

1) Gegevensuitwisseling. Gegevensuitwisseling is logisch: twee weten meer dan één. Op basis van meer en betere informatie kun je beter en sneller handelen. Het leidt tot ruimere mogelijkheden voor preventie, detectie en kennisontwikkeling.

Gegevensuitwisseling vindt veelvuldig plaats in het buitenland. Het Verenigd Koninkrijk, de VS, Singapore, Australië, Estland en Zwitserland zijn landen waar private partijen gegevens met elkaar delen. Dit gebeurt ook in landen waar de Algemene Verordening Gegevensbescherming (AVG) van toepassing is, zoals het Verenigd Koninkrijk en Estland. Artikel 47 van de AVG. De AVG beschouwt fraude – naast direct marketing – als een wettelijke basis voor gegevensverwerking.¹ Het delen van gegevens helpt: dankzij CIFAS, een Brits platform voor gegevensuitwisseling, werd in 2019 naar schatting £ 1,5 miljard aan fraude voorkomen.

2) Verantwoordelijkheid toewijzen daar waar iets misgaat. Een voorbeeld van een uitgebreid beleid werd in 2023 in Australië ingevoerd.² Enkele belangrijke punten zijn: a) banken moeten aanvullende controles implementeren. b) telecombedrijven moeten frauduleuze oproepen en berichten beter detecteren en verstoren, c) socialmediabedrijven zijn verantwoordelijk voor het verwijderen van frauduleuze advertenties en het zorgen voor betere apparaat-authenticatie. d) Er is een antifraude-informatiesysteem ontwikkeld: banken, telecomnetwerken, internetproviders en socialmediabedrijven delen informatie om fraude gezamenlijk te bestrijden. Dit programma is succesvol gebleken: van 2023 tot 2024 daalde het aantal oplichtingspraktijken met 17,8% en de verliezen met 25,9%.³

Een vergelijkbare optie in Nederland zou gegevensuitwisseling tussen banken en telecombedrijven omvatten met betrekking tot de vraag "*Is de klant in gesprek?*", wat een indicatie voor fraude is.

3) De rol van de banken. Banken kunnen verschillende technieken gebruiken om geldezelrekeningen op te sporen door te zoeken naar afwijkend gedrag op de rekening. Deze technieken zijn afhankelijk van – en werken beter met – voldoende data.

Een interessante ontwikkeling in het Verenigd Koninkrijk is de volgende: sinds 7 oktober 2024 vergoeden de banken, bij APP (geautoriseerde *push payments*) in beginsel nu alle verliezen van

¹ Artikel 47 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.*

² <https://thepaymentsassociation.org/article/crafting-security-australias-strategic-approach-to-combatting-fraud/>

³ Bron: <https://www.nasc.gov.au/news/australians-better-protected-as-reported-scam-losses-fell-by-almost-26-per-cent>

klanten.⁴ Tot op heden heeft dit niet tot problemen geleid in de financiële sector. Het heeft wel geleid tot een daling van een derde in het aantal claims in de eerste vier maanden na de invoering van de nieuwe regelgeving, vermoedelijk omdat banken nu meer investeren in de beveiliging van hun systemen. Deze compensatie wordt 50/50 verdeeld tussen de verzendende en ontvangende bank. De reden hiervoor is dat de ontvangende bank de geldezelrekeningen beheert. Zulke banken maken soms fouten, zoals onvoldoende controles bij het openen van een rekening en/of het negeren van waarschuwingen van detectiesystemen bij ongebruikelijke transacties.

4) Preventie werkt. De factsheet geeft verschillende voorbeelden die aantonen dat preventie effectief is. Zo zien we dat Nederlandse bedrijven steeds vaker preventieve maatregelen nemen op het gebied van cybersecurity. Tegelijkertijd zien we dat het aantal beveiligingsincidenten sinds 2016 is afgenomen. Helaas neemt het aantal incidenten bij individuen nog steeds toe.

Het zogenaamde "waterbedeffect" wordt in deze context vaak genoemd. Hoewel dit zeker soms voorkomt, is het niet absoluut. Online interventies en preventieve maatregelen kunnen effectief zijn, en arrestaties zijn ook nuttig. Wij verzetten ons tegen het idee dat "niets helpt" omdat er altijd volledige verplaatsing van criminaliteit zou plaatsvinden. Dat is niet het geval.

2. EDUCATIE

Het is belangrijk om gebruikers beter te informeren. Gebruikers worden vaak de "zwakste schakel" in de fraudeketen genoemd. Educatie kan effectief zijn als deze goed wordt geïmplementeerd. Het is meer dan alleen een website met wat informatie. Het doel ervan moet zijn om te informeren, niet om bang te maken. Onderzoek toont aan dat educatie beter werkt wanneer het interactief is.

Aandacht voor kwetsbare groepen is noodzakelijk. In het Verenigd Koninkrijk krijgt dit veel aandacht. Dit omvat ouderen, mensen met een beperking en mensen die eerder slachtoffer zijn geweest. Er zijn technische en organisatorische maatregelen beschikbaar om deze groepen te beschermen.

3. OPSPORING

Fraudeurs hebben vaak een gevoel van straffeloosheid. Dat kan niet oké zijn. Opsporing blijft essentieel. Ik begon met het feit dat een derde van alle geregistreerde misdrijven online fraude is. De mankracht bij de politie is vermoedelijk niet naar verhouding hiervan. Hier heeft de politie ook hulp van anderen nodig, van burgers en van de Fraudehelpdesk waar meldingen, laagdrempelig, als eerste binnen komen en die deze informatie verzamelt.

4. GEDEELDE VERANTWOORDELIJKHEID

De conclusie is dat online fraudebestrijding over de gehele breedte moet plaatsvinden, waar de fraude ontstaat en plaatsvindt en daarom breed moet worden aangepakt. Het is een gedeelde verantwoordelijkheid in de hele samenleving.

Het Verenigd Koninkrijk heeft nu een minister voor benoemd die onder meer voor fraudebestrijding verantwoordelijk is. Dit zal de coördinatie en samenwerking bevorderen. De minister is de Rt Hon Lord Hanson of Flint.⁵

⁴ <https://www.psr.org.uk/information-for-consumers/app-fraud-reimbursement-protections/>

⁵ <https://www.gov.uk/government/people/david-hanson>