

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

2937

Vragen van het leden **Mutluer** en **Kathmann** (beiden PvdA) aan de Ministers van Justitie en Veiligheid en van Economische Zaken en Klimaat over *online identiteitsfraude* (ingezonden 22 maart 2023).

Antwoord van Minister **Adriaansens** (Economische Zaken en Klimaat), mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties (ontvangen 19 juni 2023). Zie ook Aanhangsel Handelingen, vergaderjaar 2022–2023, nr. 2210.

Vraag 1

Kent u het bericht «Identiteitsfraude: Energiedirect scherpt beleid aan op aandringen van Radar»?¹

Antwoord 1

Ja.

Vraag 2

Beschikt u over gegevens waaruit blijkt hoe vaak het in Nederland voorkomt dat met behulp van het gebruik maken van identiteitsgegevens van een ander online contracten worden afgesloten of goederen worden gekocht? Zo ja, wat zijn die gegevens? Zo nee, bent u bereid dit te onderzoeken?

Antwoord 2

De gevraagde gegevens over fraude met identiteitsgegevens worden niet centraal verzameld, daarom ontbreken algemene cijfers. Fraudecasussen zijn ook vaak complex en kunnen tegelijk uit meerdere fenomenen bestaan (zoals kopie identiteitskaart misbruikt en/of nepprofiel aangemaakt en vervolgens bestelling op naam gedaan). Bij het vermoeden van identiteitsfraude kunnen burgers contact leggen met de organisatie waar hun gegevens misbruikt zijn of aangifte doen bij de politie of zich melden bij het Centrale Meldpunt voor Identiteitsfraude (CMI). Daarnaast zijn er gegevens uit de tweejaarlijkse Fraudemonitor van het Openbaar Ministerie.

Bij het CMI zijn de volgende gegevens bekend: het CMI heeft in 2022 in totaal 6.151 (6.397 in 2021) meldingen geregistreerd. 1.096 (1.759 in 2021) van deze

¹ Fragment Radar, 20 maart 2023, Identiteitsfraude: Energiedirect scherpt beleid aan op aandringen van Radar (radar.avrotros.nl/uitzendingen/gemist/item/identiteitsfraude-energiedirect-scherpt-beleid-aan-op-aandringen-van-radar/).

meldingen betroffen specifiek het fenomeen «bestelling op naam», waarbij gegevens van een burger misbruikt worden voor bestellingen bij diverse organisaties. Specifiek over het afsluiten van energiecontracten op naam zijn 23 meldingen gedaan in 2022 (49 in 2021).

In de tweejaarlijkse Fraudemonitor wordt door het Openbaar Ministerie verslag gedaan van het aantal opsporingszaken (verdachten) voor identiteitsfraude in het algemeen. De Fraudemonitor over de jaren 2021 en 2022 wordt naar verwachting rond de zomer door het Openbaar Ministerie gepubliceerd en zal vervolgens door de Minister van Justitie en Veiligheid aan de Tweede Kamer worden aangeboden. Het ging in 2019 om 655 verdachten van ID-fraude en om 118 verdachten van ID-fraude via internet. In 2020 ging het om 480 verdachten van ID-fraude en 145 verdachten van ID-fraude via internet². De Fraudemonitor bevat geen nadere uitsplitsing naar ID fraude in verband met het afsluiten van energiecontracten.

Vraag 3

Is er verband tussen het grootschalig hacken of stelen van onlinegegevens van Nederlanders en online identiteitsfraude? Zo ja, waar bestaat dat verband uit en hoe vaak komt het voor dat er met deze gegevens gefraudeerd wordt? Zo nee, kunt u dit verband uitsluiten?

Antwoord 3

Ja. Bij het inbreken in bepaalde systemen (computervrededreuk) kunnen grote hoeveelheden persoonsgegevens wederrechtelijk worden overgenomen. De aard en hoeveelheid van de gegevens kunnen sterk verschillen. Bepaalde gegevens kunnen worden gebruikt voor het plegen van diverse vormen van fraude, waaronder online identiteitsfraude. Er zijn gevallen bekend waarbij zeer grote hoeveelheden persoonsgegevens zijn overgenomen en vervolgens online zijn aangeboden. Daardoor worden deze gegevens voor veel kwaadwillenden bereikbaar en neemt het risico op misbruik voor fraude fors toe. Er zijn echter geen kwantitatieve gegevens bekend hoe vaak fraude wordt gepleegd met gegevens die na inbraak in systemen zijn verkregen.

Vraag 4

Deelt u de mening dat consumenten, die slachtoffer van online identiteitsfraude zijn en dus niet zelf een overeenkomst hebben gesloten, dit niet zelf zouden moeten aantonen, maar dat het aan de ondernemer is bij wie een overeenkomst is gesloten om aan te tonen dat die overeenkomst met de desbetreffende consument is gesloten? Zo ja, hoe is de geldende wet- en regelgeving dienaangaande en behoeft die aanpassing? Zo nee, waarom deelt u die mening niet?

Antwoord 4

Artikel 150 van de Wet van Burgerlijke Rechtsvordering stelt dat de partij die zich beroept op rechtsgevolgen van door haar gestelde feiten of rechten, de bewijslast daarvan draagt. Dat betekent in dit geval dat een ondernemer die betaling eist voor een overeenkomst, moet kunnen bewijzen dat hij die daadwerkelijk met de desbetreffende consument heeft gesloten. In het bericht van Radar wordt verwezen naar identiteitsfraude bij een energieleverancier. Wanneer consumenten een geschil hebben met een energieleverancier kunnen zij terecht bij de Geschillencommissie. Alle energieleveranciers die leveren aan consumenten zijn wettelijk verplicht om hierbij aangesloten te zijn.

Vraag 5

Deelt u de mening dat ondernemers die onlinegoederen of diensten aanbieden zelf moeten zorgen dat er op een laagdrempelige wijze de identiteit van een klant wordt geverifieerd, bijvoorbeeld door het online betalen van 1 eurocent? Zo ja, waarom en welke (andere) mogelijkheden ziet u voor zich? Zo nee, waarom niet?

² Bijlage bij Kamerstuk 17 050, nr. 600, p. 20.

Antwoord 5

In het antwoord op vraag vier is toegelicht dat de ondernemer die de betaling eist voor een overeenkomst de bewijslast draagt. Het is daarom denkbaar dat ondernemers binnen de grenzen die de wet op dit moment biedt, in specifieke situaties ervoor kiezen om een verificatiemethode toe te passen. Hierbij kan gedacht worden aan overeenkomsten waar bijvoorbeeld voor consumenten grotere bedragen zijn gemoeid.

De 1-cent methode waar naar wordt verwezen in deze vraag kan een optie zijn. Het is echter niet wenselijk dat deze methode bij elke aankoop wordt ingezet. Er zijn namelijk gevallen bekend waarbij fraudeurs op online handelsplaatsen ook met die methode fraude plegen. De Fraudehelpdesk wijst op dit risico en hoe hiermee om te gaan.³

Een andere mogelijkheid binnen de wet is het vragen van een handtekening. Dit kan tot gevolg hebben dat sommige overeenkomsten niet per direct gesloten kunnen worden. Hier staat tegenover dat een handtekening via het identiteitsbewijs geverifieerd kan worden in het geval de consument aangeeft de overeenkomst niet zelf gesloten te hebben.

Ten aanzien van de energiesector, waar naar wordt verwezen in het bericht van Radar, ontvangt de Tweede Kamer naar verwachting voor de zomer een brief van de Minister voor Klimaat en Energie over de Energiewet. Daarin wordt o.a. de nieuwe gegevensuitwisselingsentiteit in de energiesector toegelicht.

Het is in het algemeen onwenselijk dat ondernemers meer gegevens dan noodzakelijk ontvangen van burgers. Zoals bij het antwoord op vraag drie is toegelicht, kan deze informatie juist gebruikt worden voor het plegen van fraude, als wordt ingebroken in de systemen van ondernemers.

Vraag 6 en 7

Deelt u de mening dat als ondernemers zelf meer de identiteit van hun onlineklanten gaan verifiëren dat daarmee misdaad en onnodige belasting van de politie en andere actoren in de strafrechtketen kan worden voorkomen? Zo ja, waarom? Zo nee, waarom niet?

Bent u bereid om met ondernemersverenigingen en brancheorganisaties in overleg te treden om laagdrempelige wijzen van identiteitsverificatie te bevorderen? Zo ja, wilt u de Kamer van de uitkomst van dat overleg op de hoogte stellen? Zo nee, waarom niet?

Antwoord 6 en 7

Voor elke vorm van fraude en oplichting geldt dat de meeste winst te behalen is met het vergroten van het bewustzijn van risico's en met preventieve maatregelen om slachtofferschap zo veel mogelijk te voorkomen. In het geval van identiteitsfraude bij consumentenaankopen is het ook belangrijk dat ondernemers zich bewust zijn van identiteitsverificatie, mede omdat de bewijslast bij hen ligt (zie antwoord op vraag vier). Ondernemers die zijn opgelicht kunnen dit melden en aangifte doen bij de politie. Informatie is belangrijk voor de opsporing om snel zicht te krijgen op de aard, omvang en handelwijze van oplichting. Het informeren van ondernemers over identiteitsverificatie kan op verschillende manieren; algemene informatieverstrekking en sectorspecifiek wanneer aanvullende eisen worden gesteld aan identiteitsverificatie.

Ten aanzien van algemene informatie ondersteunt het CMI voornamelijk slachtoffers van identiteitsfraude met informatie en concreet advies, maar levert ook een bijdrage aan bewustwording en preventie van identiteitsfraude met presentaties, workshops en andere voorlichtingsactiviteiten. Ondernemers kunnen in het fysieke en in het digitale domein controle en verificatie toepassen om te voorkomen dat ook zij slachtoffer worden van oplichters die zich schuldig maken aan identiteitsfraude. Het CMI kan met organisaties meedenken over of en hoe er kans is op identiteitsfraude met de buitgemaakte gegevens. Daarnaast kan het CMI meedenken over hoe getroffen organisaties de slachtoffers van een hack of datalek kunnen informeren. Zo is het CMI te gast geweest bij meerdere online bijeenkomsten van de contactcentra van grote woningcorporaties. Tijdens deze bijeenkomsten heeft het

³ Fraudehelpdesk – Ik krijg een betaalverzoek voor 1 cent – Fraudehelpdesk.

CMI de medewerkers geïnformeerd en geadviseerd hoe zij konden antwoorden op mogelijke vragen van verontruste burgers/klanten.