POLITIEKUNDE 99

POLITIE & Wetenschap

Aankoopfraude vanuit het buitenland

Alternatieven voor opsporing

Jurjen Jansen, Saskia Westers, Suzanna Twickler en Wouter Stol

NHL STENDEN hogeschool

Aankoopfraude vanuit het buitenland: Alternatieven voor opsporing

J. Jansen
S. Westers
S. Twickler
W. Stol

POLITIE & Wetenschap

NHL STENDEN hogeschool

In opdracht van: het programma Politie en Wetenschap van de Politieonderwijsraad.

Meer informatie over deze en andere uitgaven kunt u verkrijgen bij:
Sdu Klantenservice
Postbus 20025
2500 EA Den Haag
tel.: (070) 378 98 80
website: www.sdu.nl

Omslagontwerp: Joris Clappers | Elgersma Reclame en Media
Illustratie omslag: Tymo Grijpma, Groningen

ISBN: 9789012405164
NUR: 600

Verantwoording

	Cybersafety Research Group
	NHL Stenden Hogeschool / Politieacademie
	www.cybersciencecenter.nl
Opdrachtgever	Politie & Wetenschap
Vraagarticulatie	Landelijk Meldpunt Internetoplichting (LMIO)
Auteurs	Dr. Jurjen Jansen Saskia Westers MSc Mr. Suzanna Twickler Prof. dr. Wouter Stol
Met medewerking van	Kim Zijlstra (student, NHL Stenden Hogeschool)
Met dank aan de klankbordgroep	Monic Blauw (Rabobank) Clemens Braber (Politie, Internationaal Rechtshulpcentrum) Frederik Cousin (Federale Overheidsdienst Economie, België) Bjorn Deutekom (Betaalvereniging) Jan-Willem te Gussinklo Ohmann (Marktplaats) Harmen van Genderen (Openbaar Ministerie) André van Heel (Politie, Horizontale fraude) Freek Kelderman (Politie, Landelijk Meldpunt Internetoplichting) Thijs Koyen (Federale Overheidsdienst Economie, België) Gijs van der Linden (Politie, Landelijk Meldpunt Internetoplichting)

Met dank aan de leescommissie Prof. dr. Marianne Junger (Universiteit Twente)
Dr. Johan van Wilsem (Algemene Rekenkamer)
Dr. Rutger Leukfeldt (Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR), Haagse Hogeschool)
Mr Dirk ten Boer (Openbaar Ministerie (OM) Noord-Nederland)
Drs. Richard Nijeboer (Politie, Landelijke Eenheid)
Niels van Dam (Politie, Noord-Holland)

Inhoudsopgave

Samenvatting

In dit onderzoek wordt gekeken naar verstoringsmogelijkheden van online aankoopfraude vanuit het buitenland (hierna aankoopfraude). Bij aankoopfraude wordt door het slachtoffer geld overgemaakt naar het buitenland voor een product of dienst, zonder deze te ontvangen. Aankoopfraude is een lucratief verdienmodel voor oplichters door een lage pakkans en hoge winstmarge. Het doel van dit onderzoek is om meer inzicht te krijgen in deze specifieke vorm van fraude en daarmee inzicht te geven in bestrijdingsmogelijkheden, anders dan met opsporing. De centrale vraag van dit onderzoek luidt: Hoe kan internationale aankoopfraude worden bestreden, anders dan met opsporing?

Om de crimescripts c.q. aanvalsstrategieën van aankoopfraude in kaart te brengen zijn 150 meldingen van het Landelijk Meldpunt Internetoplichting (LMIO) geanalyseerd. Aanvullend zijn 20 semigestructureerde interviews afgenomen met slachtoffers. Dit was nodig om meer context en diepgang te geven aan de aanvalsstrategieën die zijn gedestilleerd uit de analyse van de meldingen. Bovendien kon daarmee inzichtelijk worden gemaakt welke partijen een rol spelen in aankoopfraude. Daarnaast zijn verstoringsmogelijkheden van aankoopfraude geïdentificeerd aan de hand van interviews met 16 experts en een brainstormsessie met de klankbordgroep. Tot slot is het juridische kader, afgebakend tot de zorgplicht van partijen die een rol spelen in de verschillende aanvalsstrategieën, in kaart gebracht middels deskresearch.

In dit onderzoek worden vier aanvalsstrategieën onderscheiden: (1) het plaatsen van een advertentie; (2) het opzetten van een valse webshop; (3) het misbruiken van een account; en (4) het reageren op een zoekadvertentie. Voor de eerste – en tevens meest voorkomende – strategie plaatst de dader een advertentie online, bijvoorbeeld op Marktplaats. Zodra contact is gelegd met een slachtoffer wordt overeengekomen tot koop en laat de dader het slachtoffer geld overmaken naar het buitenland. De dader stuurt vervolgens geen product of dienst. Voor de tweede strategie lanceert de dader een valse webshop waar slachtoffers producten of diensten kunnen aanschaffen, om vervolgens niets te leveren. In de derde strategie misbruikt de dader een account of de naam van een bedrijf, bijvoorbeeld door deze te hacken of te spoofen. De dader misbruikt de betrouwbaarheid van het account om een product/dienst te verkopen zonder iets te leveren. Bij de vierde strategie reageert de dader op een zoekadvertentie van een slachtoffer. De dader biedt het gezochte product of de dienst aan en laat het slachtoffer geld overmaken naar het buitenland zonder te leveren. Het reageren op een zoekadvertentie is de minst voorkomende aanvalsstrategie in deze studie.

De geïdentificeerde verstoringsmogelijkheden van aankoopfraude zijn gekaderd volgens het raamwerk voor situationele criminaliteitspreventie. Uiteindelijk worden drie strategieën aangedragen die het meest kansrijk lijken om aankoopfraude te verstoren. De eerste strategie is gericht op het weerbaarder maken van internetters. Hierbij wordt aanbevolen om in vervolgonderzoek de effectiviteit van digitale weerbaarheidsprogramma's te toetsen. De tweede strategie richt zich op het versterken van controles. Voor deze strategie spelen enerzijds de partijen in het fraudeproces een belangrijke rol. Deze partijen moeten maatregelen nemen die betrekking hebben op preventieve controle van verkopers; waarbij handelingsmogelijkheden van fraudeurs onmogelijk worden gemaakt. Anderzijds is een rol weggelegd voor overheids- en/of brancheorganisaties en wordt ingezet op het invoeren van echtheidskenmerken. Het invoeren van echtheidskenmerken kan effectief zijn, omdat het bepaalde acties van fraudeurs moeilijker maakt en/of eerder aan het daglicht brengt. Ook kan het controle/toezicht door anderen stimuleren. De derde strategie richt zich op het versterken van Europese samenwerking. Hierbij wordt gedoeld op een grensoverschrijdende, integrale aanpak in de vorm van het instellen van een Europees meldpunt en het versterken van Europese publiek-private samenwerking.

Proactieve verstorings- en preventiemogelijkheden moeten de geprefereerde methode zijn om fraude aan te pakken – boven opsporing – omdat het voorkomt dat grote aantallen mensen slachtoffer worden van fraude. Het is daarom belangrijk dat de politie – in samenwerking met partners c.q. betrokken partijen – voortdurend op zoek gaat naar mogelijkheden om daders en de aanvalsstrategieën die zij gebruiken te verstoren. De drie gepresenteerde strategieën geven een handvat daarbij. Dit onderzoek biedt een reeks maatregelen die gebruikt kunnen worden om elk van die strategieën uit te werken bij de verstoring van online aankoopfraude vanuit het buitenland.

1. Inleiding

'Als het te mooi is om waar te zijn…' Dit onderzoek gaat over online aankoopfraude gepleegd vanuit het buitenland. Criminelen hebben in online aankoopfraude vanuit het buitenland een lucratief verdienmodel gevonden met een geringe pakkans. Door het virtuele karakter en de internationale dimensie is het opsporen van deze fraude een lastige aangelegenheid. Dit onderzoek heeft als doel om meer inzicht te krijgen in deze specifieke vorm van online fraude en op basis daarvan zicht te bieden op mogelijkheden om dit type delict te bestrijden, anders dan met opsporing.

1.1 Context

Online aankoopfraude (hierna aankoopfraude) betekent dat iemand online een goed of dienst heeft gekocht via internet, deze vooruit heeft betaald en wordt opgelicht doordat het bestelde niet wordt geleverd (Bloem & Harteveld, 2012; Domenie, Leukfeldt, Van Wilsem, Jansen & Stol, 2013; Van der Hulst & Neve, 2008; Van Wilsem, 2011).[1] Het gaat hierbij meestal om populaire producten, zoals elektronica, gadgets, schoenen en toegangskaartjes die voor een relatief laag bedrag worden 'aangeboden' (Bloem & Harteveld, 2012). 'Vanuit het buitenland' betekent dat het slachtoffer in Nederland de betaling heeft overgemaakt naar een buitenlands rekeningnummer. In het rapport van Bloem en Harteveld (2012) worden auto's en caravans genoemd als voorbeeld van producten die frauduleus worden aangeboden vanuit het buitenland.
Aankoopfraude vindt veelal plaats via online veiling- of handelsplaatsen zoals Marktplaats en eBay (Van Wilsem, 2011), maar kan ook plaatsvinden via sociale media zoals Facebook en Instagram (Borwell, 2017). Frauduleus handelende webwinkels vallen ook onder de definitie van aankoopfraude (Bloem & Harteveld, 2012). Wij kiezen er in dit onderzoek voor om ons niet op voorhand te beperken in de wegen waarlangs en de manieren waarop de delicten worden gepleegd. Wel is ons onderzoek anderszins begrensd. Omdat slachtoffers van aankoopfraude die melding doen bij de politie nage-

1 Andere benamingen voor aankoopfraude zijn: fraude met online handel, veilingfraude, fraude in e-commerce en marktplaatsfraude (Bloem & Harteveld, 2012; Leukfeldt, Domenie & Stol, 2010). Zie bijlage I voor aanvullende informatie over definities.

noeg altijd particulieren zijn, besteden we in dit onderzoek geen aandacht aan bedrijven als slachtoffer.[2]

1.2 Prevalentie en schadebedragen

Op basis van aangiften is aankoopfraude de meest voorkomende vorm van fraude met online handel (Centraal Bureau voor de Statistiek (CBS), 2017). Sinds 2010 heeft de politie een Landelijk Meldpunt Internetoplichting (LMIO) dat aangiften van online fraude verzamelt en analyseert. De meeste aangiften van aankoopfraude komen dan ook binnen bij het LMIO (Inspectie Veiligheid en Justitie, 2015).[3] Voor aankoopfraude zijn in 2016 ongeveer 45.000 aangiften gedaan, waarvan het in 821 gevallen gaat om aankoopfraude vanuit het buitenland (1,8%).[4] In 2017 ging het om ongeveer 38.000 aangiften, waarvan in 1.938 gevallen geld naar het buitenland werd overgemaakt (5,1%).

Het werkelijke aantal slachtoffers van aankoopfraude vanuit het buitenland is waarschijnlijk groter dan deze aantallen aangiften aangeven, aangezien slachtoffers van cybercrime in minder dan 20% van de gevallen aangifte doen (Domenie e.a., 2013). Reep (2017) schetst op basis van de data van de Veiligheidsmonitor 2016 (CBS, 2017) dat in 2015 ruim zeven keer zoveel slachtoffers zijn geregistreerd in het zelfrapportage-onderzoek dan bekend is op basis van geschatte politiestatistieken over internetoplichting. Hoewel zelfrapportage-onderzoek gevoelig is voor een overschatting van slachtofferschap, in het CBS-onderzoek naar schatting met een factor 1,6 à 2, tonen deze cijfers aan dat het werkelijke aantal slachtoffers van internetoplichting beduidend groter is dan het aantal aangiften.[5] Het 'dark number' van aankoopfraude is dus groot.

Diverse bronnen hebben cijfers over de omvang en schade van aankoopfraude. Zelfrapportage-onderzoek van het CBS (2017) toont dat 2,7% van de Nederlandse bevolking van 15 jaar en ouder in een jaar slachtoffer was van aankoopfraude.[6] Wanneer we

2 Dat bedrijven weinig melding doen, wil niet zeggen dat aankoopfraude voor hen geen probleem is, zoals het onderzoek van Veenstra, Zuurveen en Stol (2016) laat zien. Uit hun zelfrapportage-onderzoek onder 1.203 MKB-bedrijven blijkt dat 4,1% in een jaar slachtoffer was van online fraude, waar aankoopfraude onderdeel van is.

3 Benadeelden kunnen tevens aangifte doen op het politiebureau. Dit gebeurt indicatief één of twee keer per week (Inspectie Veiligheid en Justitie, 2015). Online aangifte is niet mogelijk zonder DigiD. Slachtoffers uit het buitenland kunnen dus geen aangifte doen bij het LMIO. Slachtoffers zonder Nederlandse identiteit kunnen wel aangifte doen op een politiebureau, zie: https://www.politie.nl/themas/internetoplichting.html.

4 Juridisch gezien gaat het hier niet om aangiften, maar om meldingen, omdat voor aangiften een handtekening is vereist. Omdat de meldingen wel als aangiften worden behandeld, noemen we deze ook zo in dit rapport. Beide termen worden overigens wisselend ingezet.

5 Overschatting kan komen door 'telescoping'-effecten: opgeven dat een delict in de laatste twaalf maanden heeft plaatsgevonden terwijl het delict langer dan twaalf maanden geleden heeft plaatsgevonden (CBS, 2017).

6 We richten ons in dit onderzoek niet op verkoopfraude. Verkoopfraude komt namelijk onder particulieren weinig voor (0,2% volgens het CBS (2017)). Bij deze variant bieden criminelen (hoge) bedragen voor producten die mensen aanbieden, ontvangen deze producten, maar betalen daar vervolgens niet voor (Bloem & Harteveld, 2012). Andere varianten die we uitsluiten is het leveren van producten of diensten van slechtere kwaliteit dan beloofd (Van Wilsem, 2011) en valse investeringen (ECC, 2017).

dit omrekenen naar absolute aantallen komen we uit op ongeveer 335.000 slachtoffers.[7] Vooral jongeren en middelbaar en hoger opgeleiden zijn hiervan slachtoffer. Het CBS splitst de genoemde 2,7% niet uit naar daderschap in binnen- of buitenland. Aankoopfraude is na hacken (4,9%), vernieling aan voertuigen (4,1%) en fietsdiefstal (3,8%) het meest gerapporteerde delict in Nederland. Het slachtofferpercentage lijkt op basis van zelfrapportage-onderzoek niet veel te zijn veranderd in de afgelopen tien jaar. Van Wilsem (2011) vond namelijk in zijn studie dat 2,5% van de Nederlandse internetgebruikers middels aankoopfraude was opgelicht in 2007.

Domenie e.a. (2013) vinden op basis van een zelfrapportage-onderzoek dat 2,4% van de internetgebruikers (van 15 jaar en ouder) in een jaar slachtoffer was van aankoopfraude. Deze onderzoekers hebben wel een uitsplitsing gemaakt naar hoe vaak aankoopfraude is gepleegd vanuit het buitenland. Zij vonden dat niet 1,8-5,1% (LMIO-cijfers), maar 19,2% van de aankoopfraude vanuit het buitenland wordt gepleegd. Dit komt overeen met het onderzoek van Leukfeldt en collega's (2010) waarin 14,5% van de daders die online fraude hebben gepleegd uit het buitenland komt.

De producten die worden gebruikt bij internationale aankoopfraude waarvan in Nederland het meeste aangifte wordt gedaan bij het LMIO (in 2017) zijn (1) luierboxen, (2) elektronica, (3) tickets, (4) verhuur van vakantiewoningen/-appartementen en (5) kleding. Dit zijn overigens niet de producten die per geval de meeste schade berokkenen. De top 5 van gemiddelde schadebedragen in 2017 per productcategorie wordt uitgemaakt door: (1) vrachtwagens, (2) campers, (3) auto's, (4) motoren en (5) landbouwvoertuigen. Het CBS (2017) noemt een top vier van producten die het meest worden gebruikt bij zowel binnenlandse als buitenlandse aankoopfraude: (1) mobiele telefoons, (2) tickets en kaartjes, (3) kleding en sieraden en (4) spelcomputers.

De totale schade van aankoopfraude in 2016, zoals berekend door het LMIO, bedraagt 9 miljoen euro, waarvan 1,2 miljoen is toe te rekenen aan de internationale variant (13,3% van de totale schade). Internationale aankoopfraude wordt vooral gepleegd vanuit Duitsland (28,6%), België (21,9%), het Verenigd Koninkrijk (17,9%) en Italië (8,5%). Slachtoffers van binnenlandse aankoopfraude verliezen gemiddeld circa 175 euro, terwijl dit voor internationale aankoopfraude gemiddeld ruim 1.400 euro is. De gemiddelde schade voor aankoopfraude uit het buitenland is dus volgens deze cijfers meer dan acht keer zo groot.

Uiteraard is Nederland niet het enige land waar aankoopfraude gepleegd wordt. In België kreeg de Economische Inspectie voor 2017 in totaal 4.116 meldingen van aankoopfraude.[8] Ongeveer 30% van de meldingen betrof aankoopfraude vanuit het buitenland.[9] De meeste meldingen hiervan hadden betrekking op (1) Nederland, (2)

7 Dit aantal is berekend aan de hand van de bevolkingscijfers van 2016 van Nederlanders van 20 jaar en ouder. CBS Statline (2018). *Bevolking; kerncijfers*. Via: https://opendata.cbs.nl/statline/#/CBS/nl/dataset/37296ned/table?ts=1551259762695.

8 Algemene Directie Economische Inspectie – Dienst Analyse, Prioritering en Strategie (05-07-2018), via FOD Economie (persoonlijke communicatie, 31 juli 2018).

9 Het grote aantal 'binnenlandse' meldingen lijkt een incident. De oorzaak hiervoor ligt in 2.003 meldingen die gericht zijn tegen één Belgisch bedrijf dat luiers verkocht.

Frankrijk en (3) het Verenigd Koninkrijk. Binnen de Europese Unie heeft 12% van de internetgebruikers een vorm van internationale online fraude ervaren (European Consumer Centres Network (ECC), 2017). In de top vijf van meest voorkomende internationale online fraudevormen staan (1) oplichting via frauduleuze websites, (2) aankoop van gebruikte auto's en (3) verkoop van tickets. Daarnaast staan (4) het leveren van namaak-merkproducten en (5) zogenaamde 'gratis' proefpakketten in de top vijf, maar die vallen niet onder de in dit onderzoek gehanteerde definitie van aankoopfraude (zie par. 1.1). In een Eurobarometer-onderzoek is ook gevraagd naar slachtofferschap van online aankoopfraude (Europese Commissie, 2017). Op basis van dat onderzoek komt naar voren dat 16% van de Europese internetgebruikers hiervan slachtoffer is geworden (dit is inclusief het ontvangen van namaakproducten en producten die niet voldeden aan de omschrijving). Voor Nederland is het slachtofferpercentage 19%. De periode waarin slachtofferschap plaatsvond is echter onduidelijk.

1.3 Aanleiding en relevantie

De specifieke aanleiding tot dit onderzoek is een knelpunt in de bestrijding van aankoopfraude vanuit het buitenland. Bij aankoopfraude vanuit het buitenland lijden slachtoffers zoals we zagen relatief veel financiële schade (ruim achtmaal zoveel als bij binnenlandse fraude), terwijl de politie naar eigen zeggen vanwege de internationale component zelden of nooit overgaat tot opsporing, ook al gaat het vooral om aankoopfraude uit buurlanden. Zo werken rechtshulpverzoeken vertragend en leveren bovendien vaak weinig op.[10] Tevens worden dergelijke delicten volgens Bloem en Harteveld (2012) vaak gepleegd vanuit internetcafés, waardoor opsporing middels IP-adressen weinig zinvol is. Daarnaast leveren annuleringsverzoeken die Nederlandse banken doen aan banken in het buitenland nagenoeg niets op.[11] Voor criminelen ligt hier dus een lucratief verdienmodel met in hoge mate vrij spel. Gebrekkige bestrijding van aankoopfraude werkt criminaliteitsbevorderend, wat maatschappelijk gezien ongewenst is (Klerks & Kop, 2007).

In dit onderzoek wordt vooral aandacht besteed aan de manier waarop aankoopfraude vanuit het buitenland kan worden bestreden. De relevantie van het onderzoek is dat we kennis verwerven over hoe deze internationale criminaliteit kan worden bestreden ánders dan met opsporing, want vóóraf verstoren is beter dan achteraf opsporen van criminele activiteiten.

In dit onderzoek worden twee theoretische benaderingen gebruikt als kapstok. De eerste is de routine-activiteitenbenadering en wordt gebruikt om de kenmerken van aankoopfraude (en cybercrime in zijn algemeenheid) te beschrijven, zie hoofdstuk 2. Ook is er aandacht voor de crimescripts die criminelen toepassen om aankoopfraude te plegen. Crimescripts zijn een manier om de procedurele aspecten van misdaden in kaart te brengen (Cornish, 1994). De tweede is de situationele criminaliteitspreventie-

10 Projectleider LMIO (persoonlijke communicatie, 12 april 2017).
11 Klankbordgroep-bijeenkomst (persoonlijke communicatie, 28 maart 2018).

benadering die wordt gebruikt als kapstok voor mogelijkheden om aankoopfraude (en cybercrime in zijn algemeenheid) te bestrijden, zie paragraaf 3.3. Overigens wordt de routine-activiteitenbenadering ook gebruikt om mogelijkheden voor situationele criminaliteitspreventie te schetsen (Choo, 2011). Daarnaast is er aandacht voor het juridische kader. Specifiek wordt hierbij gekeken naar de zorgplicht van betrokken partijen.

De kennis die voortvloeit uit dit onderzoek kan organisaties – de politie en haar partners, zoals banken en beheerders van koop- en verkoopsites – helpen in de bestrijding/verstoring van criminele activiteiten. Daarvoor is dan om te beginnen wel een beter zicht op de problematiek vereist. Dit onderzoek heeft een toegevoegde waarde omdat het (a) dieper ingaat op een specifieke vorm van cybercrime, namelijk aankoopfraude en (b) gericht is op een specifieke vorm van criminaliteitsbestrijding, namelijk het tegenhouden/verstoren ervan. Inzicht verkrijgen in nieuwe methoden van het (samen met partners) bestrijden van criminaliteit is een belangrijk punt in de strategische onderzoeksagenda voor de politie (SOANP, 2015). Tevens sluit het onderzoek aan bij een van de landelijke prioriteiten van de Nationale Politie, te weten cybercrime (SOANP, 2015).[12]

Het onderzoek is ook belangrijk voor consumenten die online aankopen doen. Het voorkomen van online fraude is belangrijk, omdat dit soort criminaliteit veel negatieve gevolgen kan hebben. Naast financiële schade leidt dit ook tot psychologische en emotionele schade, zoals verlies van consumentenvertrouwen in online activiteiten en online commercie (Cross, Richards & Smith, 2016; Domenie e.a., 2013; Jansen & Leukfeldt, 2018). Uit onderzoek van Domenie e.a. komt naar voren dat de helft van de slachtoffers van aankoopfraude vertrouwen verliest in het handelen via een veiling- of verkoopsite waarop ze waren opgelicht. Bij ruim een kwart van de respondenten nam ook het vertrouwen in elke vorm van handel via het internet af (27%) en nam het algemene veiligheidsgevoel op het internet af (26%). Door oplichting ondervond 8% financiële problemen en 6% ondervond psychische problemen. Ook geven slachtoffers soms aan dat ze zich hulpeloos voelen omdat niemand de dader kan of wil pakken. Aannemelijk is dat deze gevoelens van hulpeloosheid groter zijn of vaker voorkomen bij slachtoffers van internationale aankoopfraude, vanwege de gebrekkige opsporing en hogere schade.

Internationale aankoopfraude heeft niet alleen effect op slachtoffers, maar weerhoudt mogelijk ook consumenten die geen slachtoffer zijn van internationale aankopen. De consumenten die geen internationale aankopen doen, doen dit vooral niet uit angst voor oplichting (Europese Commissie, 2016). Ook in een ander onderzoek uitte een op de vijf respondenten zorgen over het gestolen worden van betalingsgegevens (21%) of misbruik van persoonlijke gegevens (19%) na een internationale aankoop (Alleweldt e.a., 2011). Voorgaande resultaten laten zien dat de angst voor fraude in internationale

12 Cybercrime blijft voor de komende jaren een landelijke prioriteit voor de politie, zoals beschreven in de Veiligheidsagenda 2019-2022. Zie: https://www.tweedekamer.nl/downloads/document?id=a3827398-2163-4b04-ad1c-3b69aa33aa23&title=Veiligheidsagenda%202019-2022.pdf.

aankopen, en dus een gebrek aan consumentenvertrouwen, invloed heeft op koopgedrag. Dit onderzoek wil slachtofferschap en de negatieve gevolgen daarvan helpen voorkomen.

1.4 Vraagstelling

Er kan worden geconcludeerd dat criminelen in aankoopfraude vanuit het buitenland een lucratief verdienmodel hebben gevonden met een geringe pakkans. De centrale onderzoeksvraag luidt: Hoe kan internationale aankoopfraude worden bestreden, anders dan met opsporing? Om de centrale onderzoeksvraag te beantwoorden zijn onderstaande deelvragen geformuleerd:

1. Uit welke stappen bestaan de crimescripts voor internationale aankoopfraude?
2. Welke partijen zijn betrokken bij de crimescripts en welke rol vervullen zij bij de totstandkoming van het delict?
3. Welke handelingsstrategieën tegen internationale aankoopfraude kunnen worden geïdentificeerd, anders dan opsporing, en welke partijen kunnen daaraan uitvoering geven?
4. In hoeverre hebben de betrokken partijen een zorgplicht jegens potentiële slachtoffers?

1.5 Leeswijzer

In hoofdstuk 2 staat het theoretisch raamwerk voor dit onderzoek centraal. Daarin wordt voornamelijk ingegaan op de verschillende onderdelen van de routine-activiteitenbenadering: daders (en hun werkwijzen), slachtoffers en beschermende maatregelen. Vervolgens worden in hoofdstuk 3 de onderzoeksmethoden verantwoord. De resultaten worden besproken in hoofdstuk 4 (crimescripts van internationale aankoopfraude), 5 (handelingsstrategieën tegen internationale aankoopfraude) en 6 (zorgplicht). Tot slot worden in hoofdstuk 7 de belangrijkste resultaten bediscussieerd en komen de beperkingen van het onderzoek aan bod. Ook bevat dat hoofdstuk antwoorden op de onderzoeksvragen.

2. Theoretisch raamwerk

In dit hoofdstuk wordt de routine-activiteitenbenadering van Cohen en Felson (1979) toegelicht. Dit raamwerk wordt toegepast om de context van aankoopfraude te duiden. Het tweede raamwerk dat wordt toegepast in dit onderzoek is de situationele criminaliteitspreventie-benadering (Cornish & Clarke, 2003). Clarke (2004) beargumenteert dat het bestuderen van hoe criminele activiteiten worden uitgevoerd en kunnen worden tegengehouden belangrijker is dan het identificeren wat de oorzaken zijn van die criminaliteit. Deze benadering wordt gebruikt voor het categoriseren van handelingsstrategieën tegen aankoopfraude. Meer informatie hierover volgt in paragraaf 3.3.

2.1 Routine-activiteitenbenadering en eerder onderzoek

De routine-activiteitenbenadering wordt reeds een aantal jaren gebruikt om slachtofferschap in een gedigitaliseerde wereld te duiden (Kigerl, 2012), met wisselende successen (o.a. Bossler & Holt, 2010; Leukfeldt & Yar, 2016; Ngo & Paternoster, 2011). De routine-activiteitenbenadering stelt dat slachtofferschap afhankelijk is van een gemotiveerde dader ('motivated offender'), een geschikt slachtoffer ('suitable target') en de afwezigheid van bescherming ('capable guardians') in een convergentie van tijd en ruimte.
Waar ander onderzoek vanuit deze benadering veelal aandacht besteedt aan een slachtofferperspectief, kiezen wij in eerste aanleg voor een daderperspectief. Eerder onderzoek laat namelijk zien dat hét slachtoffer van online fraude niet eenvoudig is te identificeren (o.a. Borwell, 2017; Jansen & Leukfeldt, 2016; Ngo & Paternoster, 2011). Daardoor is het lastig om te bepalen wie speciaal risico lopen, hen te lokaliseren en te beschermen. Omdat slachtoffers een essentiële rol vervullen in aankoopfraude laten we het perspectief overigens niet buiten beschouwing. In tweede aanleg wordt gekozen voor het perspectief van 'capable guardians': partijen die potentiële slachtoffers kunnen beschermen. Dit onderzoek heeft daarom aandacht voor:

1. hoe de daders te werk gaan (motivated offenders);
2. op wie zij hun crimescript richten (suitable targets); en
3. welke partijen het crimescript kunnen verstoren (potentiële capable guardians).

Deze drie aspecten worden hieronder verder uitgelicht, zie paragrafen 2.2-2.5. Eveneens worden daarbij resultaten uit eerder onderzoek vermeld. Het deel over capable guardians is opgedeeld in twee paragrafen: aanpak en opsporing (2.4) en bescherming (2.5).

2.2 Daders en hun werkwijzen

Daderkenmerken van online fraudeurs zijn met eerdere onderzoeken in kaart gebracht. Zo is door Leukfeldt en Stol (2011) onderzoek gedaan naar verschillen in daderkenmerken tussen online fraudeurs en klassieke fraudeurs. In totaal hebben zij 400 politiedossiers geanalyseerd, waaruit meerdere verschillen naar voren komen. Online fraudeurs zijn over het algemeen relatief jong (gemiddeld 27 jaar), man, meestal laagopgeleid en meer dan de helft heeft gemiddeld al drie antecedenten op zijn naam staan. In het proefschrift van Weulen Kranenbarg (2018) is onderzoek gedaan naar verschillen tussen 'klassieke' en 'cyber'-delinquenten (van criminaliteit waarbij ICT zowel het middel als het doelwit is), waarbij deze zijn afgezet tegen levensloop en persoonlijke en situationele risicofactoren. Uit het onderzoek komt bijvoorbeeld naar voren dat samenleven met een partner (met of zonder kinderen) de kans op daderschap verkleint. Hoewel dat ook voor traditionele criminaliteit geldt, is dat nog zwaarwegender voor cybercrime. Uiteraard is niet gezegd dat deze bevindingen ook gelden voor 'internationale' online/cyberfraudeurs. Daar is bij ons weten geen specifiek onderzoek naar verricht.

Het Europees Consumenten Centrum Netwerk heeft de frequentie van internationale aankoopfraude onderzocht.[1] Van de 30 Europese Consumenten Centra (ECC) – de landelijke dependances – die zijn uitgenodigd, hebben 27 een vragenlijst ingevuld. Van de meewerkende ECC's geeft 70% aan dat slachtoffers van aankoopfraude uit het buitenland zijn opgelicht via malafide webshops (ECC, 2017). Daarmee is dit een veelvoorkomende werkwijze van internationale aankoopfraude op Europees niveau.[2] In deze malafide webshops worden producten aangeboden tegen een onwaarschijnlijk lage prijs; voornamelijk elektronische producten zoals camera's en smartphones. In de meeste gevallen bestaat geen optie om met een creditcard te betalen of wordt hiervoor een hoge toeslag gerekend, waardoor de meeste benadeelden geld overmaken via de bank. Via de valse webshops worden zo veel mogelijk betalingen afgehandeld, waarna de webshops van het internet verdwijnen. De benadeelde is het geld kwijt en ontvangt dus geen product.

Aankoopfraude door het kopen van tweedehands auto's werd door 45% van de participerende centra benoemd (ECC, 2017). Opnieuw wordt een aantrekkelijk aanbod op internet geplaatst door de dader(s). De dader geeft vaak aan dat de prijs laag is vanwege een verhuizing naar het buitenland of financiële problemen. Het potentiële slachtoffer besluit vervolgens tot aankoop van de auto en ontvangt volledige informatie over de auto. Daaropvolgend wordt veelal aangedrongen op het gebruik van een transportbe-

1 Om het vertrouwen van de consument in de grenzeloze Europese markt te vergroten is in 2005 het European Consumer Centers Network (ECC-Net) opgericht. Sindsdien heeft elke EU-lidstaat, plus Ierland en Noorwegen, een eigen Europees Centrum voor de Consument. Bij een dergelijk centrum kunnen klachten met betrekking tot online aankopen uit het buitenland worden gemeld. Indien een consument een product heeft gekocht in een andere Europese lidstaat, kan het landelijke ECC steun bieden bij het inruilen of geld terugvragen.

2 Een kanttekening is dat de cijfers van ECC (2017) geen betrekking hebben op prevalentie.

drijf. Op afspraak betaalt het slachtoffer een voorschot aan het transportbedrijf, en de rest wordt betaald na ontvangst van de auto; volgens de fraudeur verzekert dit betalingsveiligheid. De voorschotbetaling wordt uitgevoerd via overschrijving of overboeking. Het slachtoffer krijgt vervolgens informatie over de levering van de auto. Als de auto niet wordt geleverd zoekt het slachtoffer contact met de dader. Deze vertelt dat de auto bij de douane is tegengehouden en dat een toeslag nodig is om de auto vrij te geven. Ongeacht of het slachtoffer nogmaals betaalt, verdwijnt de dader van het toneel en wordt het contact door de dader verbroken.

Een andere werkwijze van aankoopfraude, volgens het ECC (2017) veelvoorkomend in Europa, is het frauduleus verkopen van online tickets. Voor populaire concerten of sportevenementen kan het regelmatig moeilijk zijn om tickets te krijgen. Klanten kunnen onrealistisch hoge bedragen betalen voor tickets bij verkopers die geen garantie geven. Deze tickets zijn vals of worden überhaupt niet opgestuurd.

Aankoopfraude middels veilingen wordt ook regelmatig gemeld door slachtoffers (ECC, 2017). Van veilingfraude is sprake indien iemand het aangeboden product of dienst 'wint', ervoor betaalt, maar het niet geleverd wordt. Daarnaast kan de prijs van een artikel door de eigenaar kunstmatig worden opgehoogd (Leukfeldt e.a., 2010). Een van de manieren begint met een potentieel slachtoffer dat biedt, maar uiteindelijk niet wint op de veiling. Vervolgens wordt het potentiële slachtoffer benaderd door de handelaar dat de winnaar het product niet meer wil aanschaffen en dat het dus alsnog gekocht kan worden. De handelaar verkoopt vervolgens het product aan het potentiële slachtoffer. Zodra het slachtoffer betaalt, stelt de handelaar geen bedrag te hebben ontvangen of verbreekt deze de communicatie. Kortom, er is wel betaald maar geen product ontvangen.

Bij internationale aankoopfraude wordt regelmatig gewerkt met het zogenoemde 'many-little-principe', waar fraudeurs aanbiedingen plaatsen op online handelsplaatsen voor relatief lage bedragen, die te mooi zijn om waar te zijn (Bloem & Harteveld, 2012). Op deze manier worden veel (potentiële) slachtoffers bereikt en blijft het risico voor de fraudeur laag. Het many-little-principe wordt bijvoorbeeld toegepast bij malafide webshops, die na vele betalingen uit de lucht verdwijnen.

Bij het plegen van internationale aankoopfraude wordt ook gebruikgemaakt van massamarketingfraude en identiteitsdiefstal. Massamarketingfraude is de massale benadering van potentiële slachtoffers (Bloem & Harteveld, 2012). Hieronder valt ook het contact zoeken via advertenties op online handelsplaatsen zoals Marktplaats, Speurders en eBay. Identiteitsdiefstal kan bijvoorbeeld plaatsvinden door aan een potentieel slachtoffer te vragen om een digitale kopie van een identiteitsbewijs op te sturen, zoals een paspoort of rijbewijs, bijvoorbeeld als 'zekerstelling' voor de verkoper (de oplichter). Vervolgens misbruikt de oplichter dit identiteitsbewijs om vertrouwen te wekken bij volgende potentiële slachtoffers.

2.3 Slachtoffers

Hoewel slachtoffers – of benadeelden – niet het centrale uitgangspunt zijn van dit onderzoek, is een belangrijke vraag in de context van de routine-activiteitenbenadering wat iemand een geschikt doelwit maakt voor aankoopfraude. De geschiktheid van een doelwit wordt vanuit deze benadering meestal bepaald door iemands online gedrag. Voorbeelden hiervan zijn downloaden en actief zijn op sociale media (o.a. Bossler & Holt, 2009; Hutchings & Hayes, 2009; Pratt, Holtfreter & Reisig, 2010; Reyns, 2015; Van Wilsem, 2011). Hoewel we niet expliciet kijken naar kenmerken van slachtoffers en hun gedragingen, wordt hier wel rekening mee gehouden in het onderzoek. Immers, mogelijk richten daders hun crimescripts op specifieke (kenmerken van) internetgebruikers. Meer inzicht in kenmerken van slachtoffers kan van belang zijn voor het verstoren van deze criminaliteitsvorm. Op basis van de literatuur blijkt echter dat een eenduidig profiel van een online fraudeslachtoffer zich lastig laat opmaken. Wel wordt impulsiviteit of lage zelfcontrole veelal gelinkt aan risicovol online gedrag (Hadlington, 2017; Van Wilsem, 2011), wat weer van invloed is op slachtofferschap.

Onderzoek naar kenmerken van slachtoffers van aankoopfraude vanuit het buitenland is naar ons weten niet uitgevoerd. Wel is onderzoek gedaan naar kenmerken van slachtoffers van online fraude in algemene zin. Uit het onderzoek van Domenie e.a. (2013) blijkt bijvoorbeeld dat jongeren eerder slachtoffer worden van online fraude dan ouderen. Daarnaast worden alleenstaanden ook eerder slachtoffer dan mensen met een partner. Vermoedelijk staan deze twee verbanden niet los van elkaar, aangezien jongeren vaker alleenstaand zijn dan ouderen.[3]

In andere onderzoeken komen geen specifieke kenmerken van online fraudeslachtoffers naar voren. Uit het onderzoek van Jansen en Leukfeldt (2016) blijkt dat slachtoffers van phishing- en malware-aanvallen gericht op internetbankieren moeilijk zijn te identificeren – niet op basis van de routine-activiteitenbenadering en niet op basis van meer algemene demografische gegevens. Zij stellen dan ook, in ieder geval voor die fraudevormen, dat iedereen kans heeft om slachtoffer ervan te worden. Ook in het onderzoek van Borwell, Jansen en Stol (2018), waarin onder andere is gekeken naar online aankoopfraude (in algemene zin) komt op basis van demografische kenmerken geen eenduidig beeld naar voren wie speciaal risico lopen om slachtoffer te worden. Wel lijken persoonlijkheidskenmerken een rol te spelen. Borwell e.a. vonden dat slachtofferschap van online fraude, ten opzichte van de Nederlandse populatie, samenhangt met de persoonlijkheidsdomeinen extraversie, altruïsme, neuroticisme en consciëntieusheid.

De uitleg voor de eerste twee persoonlijkheidsdomeinen die zij geven is dat extraverte mensen zich vooral richten op voordelen (Modic & Lea, 2011) en daarom eerder geneigd zijn risico's te nemen. Een hoge score op altruïsme geeft een indicatie dat men geneigd is om anderen te vertrouwen. Dit betekent in deze context dat men eerder ge-

3 CBS (2018). *Honderd jaar alleenstaanden*. Via: https://www.cbs.nl/nl-nl/achtergrond/2018/26/honderd-jaar-alleenstaanden.

neigd is om te doen wat wordt gevraagd en gevoeliger is voor autoriteit (Parrish, Baily & Courtney, 2009). Hoewel de andere twee persoonlijkheidsdomeinen – neuroticisme en consciëntieusheid – tegengesteld aan de verwachting scoorden, kunnen deze wel worden verklaard. Slachtoffers van online fraude scoorden lager op neuroticisme dan de Nederlandse populatie. Een verklaring hiervoor is dat een hoge score op dit domein kan leiden tot problemen met het onderscheiden van verschillende vormen van aanbod (Halevi, Lewis & Memon, 2013). Daarnaast scoren slachtoffers van online fraude hoger op consciëntieusheid dan de Nederlandse populatie. De verklaring die Borwell en collega's (2018) daarvoor geven is dat mensen die hoog scoren op dit domein 'doen wat moet' en nalaten wat niet mag, waarbij opdrachten van fraudeurs mogelijk als 'iets wat moet' worden opgevat. Meer onderzoek is nodig om de exacte werking van persoonlijkheid op slachtofferschap te doorgronden.

2.4 Aanpak en opsporing

Voor een effectieve aanpak is het in kaart brengen van de aard en omvang van aankoopfraude vanuit het buitenland belangrijk (Chartered Institute of Public Finance & Accountancy (CIPFA), 2006). Tegen de verwachtingen in hebben de meeste Angelsaksische landen, waaronder de Verenigde Staten, een gebrekkig inzicht in fraude en oplichting (Verhage, 2014). Het inzicht in specifieke vormen van fraude, zoals internationale aankoopfraude, is dan nog minder. De huidige meting op mondiaal niveau is onbetrouwbaar, noch methodologisch onderbouwd. Zelfs de definitie van fraude verschilt per organisatie, land en wettelijke strafbepalingen (Schoorens, 2010). Zonder een eenduidige definitie is een juiste inschatting van de omvang van internationale aankoopfraude onmogelijk.[4]

Naast een betrouwbare meting is ook internationale samenwerking belangrijk voor een goede aanpak. De strategieën tegen fraude worden nu op nationale of nog kleinere schaal ingezet. Dit sluit niet aan bij de internationale 'grenzeloze criminaliteit' die het internet mogelijk maakt (Schoorens, 2010). Het gebrek aan internationale samenwerking verslechtert de kansen op een effectieve opsporing en berechting van fraudeurs. De complexiteit van de bestrijding van internationale fraude komt door een gecombineerde werking van globalisering, informatisering, anonimisering en individualisering van de samenleving en het wegvallen van sociale controlemechanismen (Schoorens, 2010). Door deze gebrekkige opsporing en berechting is het voor potentiële fraudeurs aantrekkelijk om deel te nemen aan dit verdienmodel.

Binnen Europa wordt een internationale samenwerking bewerkstelligd door het Europees Bureau voor Fraudebestrijding OLAF. De belangrijkste werkzaamheden van dit Europese anti-fraudebureau zijn het verrichten van (opsporings)onderzoek bij fraude met EU-gelden, bevorderen van samenwerking tussen autoriteiten in de lidstaten en verstrekken van hulp aan de EU-lidstaten bij activiteiten in het kader van het bestrijden van fraude met geld van de Europese Unie. In de periode van 2010 tot 2017 heeft

4 Zie ook bijlage I over de verscheidenheid van definities.

dit geresulteerd in 1.800 onderzoeken en de wederverkrijging van 6,6 miljard euro in het budget van de Europese Unie.[5] Internationale aankoopfraude betreft geen EU-financiën en wordt niet specifiek genoemd als focuspunt van de werkzaamheden van OLAF. In een recent rapport wordt echter wel aandacht geschonken aan de opkomende trend van internationale frauduleuze e-commerce, i.e. verkoop van nepproducten (OLAF, 2017). Deze vorm van fraude heeft invloed op EU-financiën omdat fraudeurs geen belasting en importrechten betalen. Daarnaast geeft het ontvangen van nepproducten sommige klanten een gevoel van wantrouwen in de online handel; en hetzelfde geldt voor buitenlandse aankoopfraude.

De opsporing van internationale fraude, en eigenlijk alle vormen van fraude, laat nog veel te wensen over. Langzamerhand werken landen samen bij enkele grote fraudezaken, maar er is geen internationale samenwerking aangaande de kleinere fraudezaken. Europol vervult hierin een belangrijke functie, maar ook bij Europol zijn weinig fondsen beschikbaar voor het ontwikkelen van efficiënte procedures (Van Geldrop & De Vries, 2011). Bovendien laten landen zich volgens deze auteurs door Europol niet zomaar de wet voorschrijven.[6] Wel worden door het European Cybercrime Centre (EC3) van Europol belangrijke stappen gezet als het gaat om internationale samenwerking.[7]

Naast de internationale samenwerking ontwikkelen landen op nationaal niveau strategieën om fraude tegen te gaan, waar we in Nederland dus bijvoorbeeld het LMIO hebben.

Zo is in Groot-Brittannië in 2006 de National Fraud Authority (NFA) opgericht, met twee doelen voor ogen. Ten eerste heeft het NFA een methodologie ontworpen om fraude eenduidig binnen verschillende sectoren te meten. Daarnaast coördineert de NFA de samenwerking tussen verschillende organisaties met het gezamenlijke doel om bewustwording en aanpak van fraudeurs te optimaliseren. De NFA is met het initiatief 'Fighting Fraud Together' gekomen, waarin nationale samenwerking van overheid en bedrijven van alle sectoren tot stand is gebracht met het doel om fraude te voorkomen en aan te pakken (NFA, 2011). Door de aangesloten partners wordt gebruikgemaakt van dezelfde meetmethoden. Door een continue samenwerking en het delen van kennis en 'best practices' wordt het fraudebewustzijn steeds hoger. Ook uit het meest recente rapport van CIPFA (2016) blijkt dat de overheid en de industrie samenwerken in het Verenigd Koninkrijk om fraude tegen te gaan en worden internationale samenwerkingen niet aangehaald. In beide strategieën wordt aankoopfraude overigens niet specifiek genoemd als focuspunt. (Nb. De NFA is in 2014 stopgezet.)

Ongeveer twintig jaar daarvoor, in 1988, is de non-profit antifraude-organisatie Cifas opgericht, die is gelieerd aan de Britse overheid.[8] Cifas is de grootste cross-sector orga-

5 European Union (2018). *OLAF in figures*. Via: https://ec.europa.eu/anti-fraud/investigations/fraud-figures_nl.

6 Interpol besteedt eveneens aandacht aan de opsporing van internationale financiële criminaliteit, maar richt zich niet op aankoopfraude zoals gedefinieerd in dit onderzoek. Interpol beschouwt het hacken van accounts wel als een van de aandachtspunten, wat ingezet kan worden om aankoopfraude te plegen.

7 Zie ook: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

8 Zoals staat beschreven op de website van Cifas: https://www.cifas.org.uk/.

nisatie in de strijd tegen fraude in het Verenigd Koninkrijk, waarbij zowel individuen, bedrijven, de publieke sector als de politie zijn aangesloten. Cifas exploiteert de grootste nationale fraudedatabase. Deze database delen zij met betrokken partijen om fraude te voorkomen.
Het laatste voorbeeld is het in 2016 in België opgerichte online meldpunt voor misleiding, oplichting en fraude, genaamd het Meldpunt.[9] Hier kunnen slachtoffers van misleiding, oplichting en fraude zich melden. Het Meldpunt is een samenwerkingsverband tussen de politie en verschillende agentschappen van de Belgische overheid. Het Meldpunt heeft als doel om oplichting en fraude te bestrijden door meldingen te verzamelen, te analyseren en hier gericht advies voor te geven aan de consument.

2.5 Bescherming

In Nederland wordt aankoopfraude aangepakt door meerdere partijen, zoals het LMIO en de Fraudehelpdesk. De aanpak is tot op heden vooral gericht op preventie. Zo is het doel van de Fraudehelpdesk, de nationale helpdesk voor vragen of meldingen over fraude, om burgers en bedrijven weerbaarder te maken voor oplichtingspraktijken en fraude.[10] De Fraudehelpdesk doet dit door informatie en adviezen te geven over (recente) oplichtingspraktijken. Daarnaast kan bij de desk melding worden gemaakt van fraude en oplichting. Indien sprake lijkt te zijn van oplichting wordt verzocht om aangifte te doen bij het LMIO.
Het LMIO is ontstaan door een publiek-private samenwerking (PPS) tussen Politie Kennemerland, Openbaar Ministerie Haarlem en Marktplaats met een preventief en repressief doel.[11] Het LMIO probeert op meerdere manieren internetoplichting aan te pakken. De eerste preventiemaatregel is dat aspirant-kopers op een online handelsplaats kunnen nagaan of het rekeningnummer, e-mailadres of telefoonnummer al door een andere benadeelde is gemeld.[12] Dit geeft een indicatie van de (on)betrouwbaarheid van de aanbieder. Bij het invullen van de gegevens krijgt de aspirant-koper een advies over de voorgenomen transactie (Bloem & Harteveld, 2012). Daarnaast kunnen potentiële slachtoffers een melding doen bij het LMIO. Omdat de melding online gemaakt kan worden, is de drempel tot melden verlaagd. Indien het product alsnog geleverd is, kan de melding worden ingetrokken.
De Autoriteit Consument en Markt (ACM) werpt ook drempels op tegen buitenlandse daders. Oplichters maken in hun aanvalsstrategie steeds vaker gebruik van sociale me-

9 Belgium.be (2016). *Meldpunt voor misleiding, fraude en oplichting*. Via: https://www.belgium.be/nl/nieuws/2016/meldpunt_voor_misleiding_fraude_en_oplichting.
10 Zoals staat beschreven op de website van de Fraudehelpdesk: https://www.fraudehelpdesk.nl/.
11 Infopolitie.nl (2010). *Landelijk Meldpunt Internetoplichting*. Via: https://www.infopolitie.nl/index.php/onderwerp/crim/50-crim/computer-criminaliteit/2146-landelijk-meldpunt-internetoplichting#1.
12 Politie.nl (z.d.). *Controleer verkopergegevens*. Via: https://www.politie.nl/aangifte-of-melding-doen/controleer-handelspartij.html?_sp=a7d856e1-38c8-4bdd-a724-48385d087dca.1540385536733.

dia.[13] Via sociale media worden bijvoorbeeld advertenties geplaatst die verwijzen naar frauduleuze webwinkels. In een korte tijd wordt een groot publiek bereikt met deze malafide advertenties. Daarom startte de ACM in 2017 een campagne om mensen te waarschuwen voor de gevaren van aankopen via sociale media.[14]

Een andere verstoringstechniek om aankoopfraude te verminderen is door het offline halen van frauduleuze webwinkels.[15] Ter illustratie, de Consumentenbond identificeerde na eigen onderzoek 2.000 webwinkels die namaakproducten, of helemaal geen producten, leveren. Deze frauduleuze webwinkels betreffen bijvoorbeeld (a) replica's van bestaande webwinkels, (b) zijn opgericht om in de decembermaand in korte tijd veel slachtoffers te maken, of (c) worden gerund door buitenlandse daders die hiervoor Nederlandse domeinnamen hebben opgekocht.[16] Onlangs heeft de Consumentenbond 850 van deze frauduleuze webwinkels offline laten halen.[17] Deze verstoringstechniek is niet altijd gemakkelijk toepasbaar. Zoals uit hetzelfde artikel duidelijk wordt, lukte het de Stichting Internet Domeinregistratie Nederland (SIDN), waar .nl-domeinnamen worden geregistreerd, bijvoorbeeld niet om 1.150 'Nederlandse' nepwinkels uit India en Amerika offline te halen. Ook andere partijen, waaronder het LMIO, steken energie in het offline (laten) halen van valse webshops. Daarbij dient men uiterst secuur te werk te gaan, bijvoorbeeld om claims te voorkomen en te voorkomen te worden beticht van censuur.

Om frauduleus geldverkeer te verstoren werpen banken een drempel op middels de IBAN-Naam Check.[18,19] Wanneer iemand middels internet- of mobielbankieren de naam en het IBAN van de ontvangende partij invoert, wordt de naam-rekeningnummercombinatie gecontroleerd vóórdat de overboeking wordt uitgevoerd. Indien afwijkingen naar voren komen, wordt een waarschuwing gegeven. Als de naam enigszins afwijkt van de naam die hoort bij het rekeningnummer, wordt de naam ter controle aan de gebruiker getoond. Als de ingevoerde naam sterk afwijkt van de naam die bij het

13 Europese Commissie (2017). *The European Commission and Member States consumer authorities ask social media companies to comply with EU consumer rules*. Via: http://europa.eu/rapid/press-release_IP-17-631_en.htm.

14 ACM (2017). *ACM waarschuwt consumenten voor impulsaankopen via social media*. Via: https://www.acm.nl/nl/publicaties/acm-waarschuwt-consumenten-voor-impulsaankopen-social-media.

15 Sinds 1 maart 2019 is de Wet Computercriminaliteit III van kracht, die mogelijkheden biedt aan het Openbaar Ministerie en de politie om websites en servers ontoegankelijk te maken als die worden gebruikt voor het plegen van strafbare feiten (art. 125p Sv (Wetboek van Strafvordering)). Bron: Openbaar Ministerie (2019). *Nepwebsites offline gehaald in onderzoek cybercrime*. Via: https://www.om.nl/@105408/nepwebsites-offline/.

16 NOS (2018). *Flinke groei valse webwinkels: 'oplichter gebruikt url bakker op de hoek'*. Via: https://nos.nl/artikel/2215583-flinke-groei-valse-webwinkels-oplichter-gebruikt-url-bakker-op-de-hoek.html.

17 De Volkskrant (2018). *Consumentenbond laat 850 frauduleuze webwinkels offline halen*. Via: https://www.volkskrant.nl/nieuws-achtergrond/consumentenbond-laat-850-frauduleuze-webwinkels-offline-halen~b8b50fba/.

18 Betaalvereniging (z.d.). *IBAN-Naam Check*. Via: https://www.betaalvereniging.nl/betaalproducten-en-diensten/iban/iban-naam-check/.

19 IBAN staat voor International Bank Account Number. In totaal maken 31 landen gebruik van IBAN; de 27 landen van de Europese Unie, Zwitserland, IJsland, Liechtenstein en Noorwegen. Zie: https://www.ibannl.org/sepa-nummer/. Het doel van de IBAN-Naam Check is het voorkomen van verkeerde overboekingen. Fraude is hier een onderdeel van.

rekeningnummer hoort, wordt de gebruiker gewaarschuwd voor mogelijke vergissingen of fraude. Voorlopig werkt deze IBAN-Naam Check alleen bij Nederlandse IBANs. Daarnaast zijn er tal van andere initiatieven die worden genomen door verschillende actoren om aankoopfraude te verstoren. Hierbij kan bijvoorbeeld worden gedacht aan initiatieven van Marktplaats, zoals het 'gelijk-overstekenprincipe' (i.e. een interne escrow-dienst[20]) om betalingen veiliger te maken, en het toevoegen van een ratingsysteem van kopers en verkopers waarmee een indicatie wordt gegeven van de betrouwbaarheid. Ook het geven van adviezen of tips over veilig online handelen en winkelen door dergelijke actoren kan helpen om klanten weerbaar te maken tegen fraudepogingen. Denk bijvoorbeeld aan de 'veilig handelen'-pagina van Marktplaats of de 'checklist veilig online winkelen' van ConsuWijzer.[21]
Niet alleen overheden, belangenorganisaties en online platformen kunnen drempels opwerpen voor fraudeurs, maar ook bedrijven en particulieren (Schoorens, 2010). Omdat het identificeren van verstoringsmaatregelen onderdeel is van het onderzoek – en om herhaling te voorkomen – gaan we hier nu niet dieper op in.

20 Een escrow(-rekening) is 'een geblokkeerde bankrekening die wordt aangehouden bij een neutrale en financieel betrouwbare derde'. Het geld op de geblokkeerde rekening wordt uitbetaald op het moment dat een overeenkomst tussen de koper en verkoper is voldaan. Bron: ABN-AMRO (z.d.). *Escrow & Settlement Services*. Via: http://www.merchant-banking.nl/Financial-Institutions/Dutch/Alternative-asset-managers-pfs/Product-and-Services/Trading-Risks/Escrow-Settlement-Services/page.aspx/14169.

21 Zie respectievelijk: https://www.marktplaats.nl/i/help/veilig-en-succesvol/ en https://www.consuwijzer.nl/online-winkelen/checklist-veilig-online-winkelen.

3. Methodische verantwoording

In dit hoofdstuk staan de onderzoeksmethoden centraal. Om de onderzoeksvragen te beantwoorden zetten we verschillende onderzoeksmethoden in:

1. analyse van meldingen van internationale aankoopfraude (dossieranalyse);
2. interviews met slachtoffers van internationale aankoopfraude (reconstructie);
3. interviews met experts/deskundigen op het gebied van (inter)nationale (aankoop) fraude en potentiële actoren in fraudebestrijding (expertinterviews);
4. analyse van de zorgplicht van bij de crimescripts betrokken partijen (deskresearch).

De onderzoeksmethoden zijn hierna verder uitgewerkt. Tabel 3.1 bevat een methodenmatrix waarin is weergegeven welke deelvragen met welke methoden worden beantwoord.

Tabel 3.1: Methodenmatrix

Deelvraag	Dossier-analyse	Reconstructie	Expertinterviews	Deskresearch
1: crimescripts?	X	X		
2: betrokken partijen?	X	X		
3: handelingsstrategieën?		X	X	
4: zorgplicht?				X

Tevens is voor dit project een klankbordgroep ingesteld bestaande uit personen met een relevante link naar de onderzoekscontext. De klankbordgroep is in 2018 driemaal bijeengekomen. De eerste bijeenkomst vond plaats in maart en diende als kick-off. De tweede bijeenkomst vond plaats in november, waarbij werd gereflecteerd op de eerste resultaten van het onderzoek. Ook werd tijdens deze bijeenkomst ingegaan op verstoringsmogelijkheden. De derde en laatste bijeenkomst vond plaats in december. Het doel van deze bijeenkomst was om te reflecteren op de uitkomsten van het gehele onderzoek en de implicaties ervan voor de praktijk. Eveneens is vanuit de opdrachtgever een leescommissie ingesteld die het concepteindrapport kritisch heeft gelezen. De bevindingen van de leescommissie zijn verwerkt in dit eindrapport. De leden van deze leescommissie zijn achterin het rapport weergegeven.

3.1 Dossieranalyse

De eerste onderzoeksmethode is dossieranalyse; meer specifiek het analyseren van meldingen van internationale aankoopfraude. De dossieranalyse geeft antwoord op deelvragen 1 en 2. Het voornaamste doel van deze methode was het op hoofdlijnen inzichtelijk maken van de crimescripts. Deze methode stelde ons in staat om – op enigszins gekwantificeerde wijze – een beeld te krijgen van de aanvalsstrategieën die criminelen toepassen. We hebben ons in dit onderzoek beperkt tot de vier landen die het LMIO het frequentst aantrof in de ontvangen meldingen, namelijk Duitsland, België, het Verenigd Koninkrijk en Italië. De meldingen voor analyse zijn gehaald uit het systeem 'IBase', het registratie- en analysesysteem van het LMIO, voor de jaargangen 2016 en 2017.

In totaal gaf het systeem 1.948 meldingen uit 2016 en 2017 voor de vier geselecteerde landen. Nadere analyse liet zien dat 167 van deze meldingen onbruikbaar waren. Het betrof bijvoorbeeld meldingen die waren teruggetrokken doordat het geld was teruggestort of dat het goed toch was geleverd.[1] Het netto aantal meldingen is daarmee 1.781.[2] In tabel 3.2 zijn het aantal meldingen, de totaal schadebedragen en gemiddelde schadebedragen (afgerond op hele euro's) gerapporteerd per land en totaal voor 2016 en 2017.[3]

Tabel 3.2: Meldingen en schadebedragen (in euro's) gespecificeerd per land en jaargang (N = 1.781)

Land	Aantal meldingen 2016	Totale schade 2016	Gemiddelde schade 2016	Aantal meldingen 2017	Totale schade 2017	Gemiddelde schade 2017
België	199	34.185	172	580	155.313	268
Duitsland	226	165.243	731	307	210.057	684
Verenigd Koninkrijk	167	468.321	2.804	137	262.339	1.915
Italië	77	166.492	2.162	88	179.148	2.036
Totaal	*669*	*834.241*	*1.247*[1]	*1.112*	*806.857*	*726*

1 Het gemiddelde schadebedrag in 2016 ligt met 1.247 euro iets lager dan de gerapporteerde 1.400 euro in par. 1.2. Dit verschil wordt veroorzaakt door de landenselectie.

1 Mensen die melding doen worden tijdens het meldproces en tien weken daarna door het LMIO erop gewezen dat intrekking in die gevallen noodzakelijk is.

2 Het is mogelijk dat hier meldingen tussen zitten van mensen die alsnog het product of het aankoopbedrag hebben ontvangen, maar die de melding niet hebben teruggetrokken.

3 Het valt op dat in sommige landen het aantal meldingen hoog is, terwijl de schadebedragen in verhouding relatief laag zijn. Zie bijvoorbeeld de meldingen van België en Italië in 2017. Het schadebedrag is ongeveer even groot, terwijl in België veel meer meldingen zijn gemaakt. Een nadere verkenning van de getrokken steekproef (N = 150; 2016-2017) geeft een indicatie dat de productcategorieën hier waarschijnlijk debet aan zijn. In de steekproefdata werd duidelijk dat in België de meeste meldingen gingen over luierboxen en elektronica. Voor Italië betrof dat (vracht)auto's, vastgoed en (vakantie)woningen.

Vervolgens is een gestratificeerde, willekeurige steekproef getrokken van 75 meldingen per jaargang, dus 150 in totaal. Deze data hebben de onderzoekers verkregen van het LMIO. De data zijn aangeleverd exclusief NAW-gegevens van de slachtoffers, waardoor screening van de onderzoekers niet nodig was. Voor het verkrijgen van data is vooraf toestemming gevraagd bij het Openbaar Ministerie (OM). De minister van Justitie en Veiligheid heeft via het OM laten weten hiervoor, onder voorwaarden, toestemming te geven.
De stratificatie is gebaseerd op het aantal meldingen per jaar per land. Dit betekent voor 2016 dat 22 meldingen zijn geselecteerd voor België, 25 voor Duitsland, 19 voor het Verenigd Koninkrijk en 9 voor Italië. De stratificatie voor 2017 kent de volgende verdeling: 39 meldingen voor België, 21 voor Duitsland, 9 voor het Verenigd Koninkrijk en 6 voor Italië. De gestratificeerde, willekeurige selectie is gemaakt met het statistische analyseprogramma SPSS (versie 21).
Voorafgaand aan de feitelijke dossieranalyse hebben we tien meldingen bestudeerd voor het ontwikkelen van een analyseprotocol en codeboek. Codes zijn een representatie van verschillende onderwerpen die geregistreerd zijn in een melding. Hierbij kan worden gedacht aan onderwerpen die verband houden met het crimescript, zoals wat voor online platform is gebruikt en met wat voor type producten/diensten is gefraudeerd. Tevens is inzichtelijk gemaakt welke partijen een rol spelen in het crimescript en op wie criminelen hun crimescripts richten. Door te werken met een analyseprotocol konden de data systematisch worden geregistreerd, verwerkt en geanalyseerd. De codering is gedaan door twee onderzoekers (elk een jaargang).
Vervolgens is het databestand verrijkt met variabelen die op basis van het bovenstaande zijn geïdentificeerd, zoals productcategorieën, hoedanigheid dader (privé of zakelijk) en crimescript-categorieën, waardoor statistische analyse mogelijk werd. Ook hierbij is gebruikgemaakt van SPSS. Tijdens de verrijking constateerden we dat achttien meldingen onbruikbaar waren. Oorzaken hiervoor waren bijvoorbeeld dat de fraudezaken buiten de definitie vielen, dat er geen inhoudelijke informatie was ingesloten of dat het ging om een poging in plaats van een voltooid delict. Derhalve zijn achttien aanvullende zaken uit het originele databestand gehaald. De selectie vond plaats door het aantal 'ontbrekende' aangiften per land en jaartal te delen door het totaalaantal. Dit betekent bijvoorbeeld dat voor drie nieuwe meldingen de 50ste, 100ste en 150ste zaak zijn geselecteerd uit een subtotaal van 150 meldingen (voor een land in en een bepaald jaar). Deze meldingen zijn direct gescand op bruikbaarheid. Indien een melding niet voldeed, is de eerstvolgende zaak geselecteerd.

3.2 Reconstructie

De tweede toegepaste methode is het reconstrueren van aankoopfraudes vanuit het buitenland. De reconstructie kende een kwalitatieve benadering en geeft antwoord op deelvragen 1 en 2 en aspecten van deelvraag 3. Het voornaamste doel van deze exercitie was om te achterhalen (a) waarom de fraude succesvol was en (b) wat mogelijke contra-strategieën zijn. De reconstructie kan voor een groot deel worden vergeleken met

crimescript-analyse, een methode die gebaseerd is op situationele criminaliteitspreventie theorie (Cornish, 1994; Tompson & Chainey, 2011). Tompson en Chainey hebben hierbij aandacht voor vier 'scènes' die het script uitmaken: (1) voorbereiding, (2) *pre*-activiteiten, (3) activiteit, en (4) *post*-activiteiten.

We beoogden de aankoopfraudes te reconstrueren aan de hand van politiedossiers waarin opsporing is gedaan,[4] aangevuld met interviews van betrokkenen (i.e. 'case officers' en slachtoffers[5]). Dit was echter niet mogelijk, omdat dergelijke dossiers niet voorhanden waren. Daarop is besloten een alternatieve strategie te hanteren, namelijk reconstructie op basis van slachtofferinterviews. Dit is een zinvol alternatief, omdat slachtoffers kunnen vertellen hoe ze het incident hebben beleefd en inzicht kunnen geven in de werkwijzen van daders, alsook waarom het crimescript 'werkt'. Benadeelden kunnen eveneens aangeven met welke partijen zij tijdens en na het incident contact hebben gehad, wat mogelijk nuttige inzichten oplevert voor nader onderzoek. Een mogelijke beperking van deze werkwijze is dat slachtoffers mogelijk niet weten of zich niet meer goed kunnen herinneren hoe zaken precies zijn voorgevallen (o.a. Jansen & Leukfeldt, 2018). Om de (semigestructureerde) interviews in goede banen te leiden is vooraf een interviewprotocol opgesteld, zie bijlage II. Omdat het onderzoek zich vooral richt op tegenhouden, hebben we benadeelden ook gevraagd om aan te geven wat ze met de kennis van nu anders hadden gedaan of in het vervolg anders zouden doen, of wat instanties anders zouden kunnen doen om de daders een voet dwars te zetten. Oftewel, met welke maatregelen het crimescript is te frustreren, zodat de benadeelde of een potentieel slachtoffer er in het vervolg niet meer intrapt of in kan trappen.

Op basis van de resultaten van de dossieranalyse (zie par. 4.1 en 4.2), is bepaald welk type zaken we wilden reconstrueren. We wilden graag met benadeelden spreken die waren opgelicht met: (1) de aankoop van auto's; (2) de aankoop van elektronica; (3) de aankoop van tickets; (4) de huur van vakantiewoningen; (5) de huur van woningen; (6) een aankoop waarbij het eerste contact verliep via sociale media; (7) aankopen via een luierbox-webshop; (8) aankopen via een willekeurige valse webshop, maar geen luierbox-webshop; (9) een 'gezocht'-advertentie; en (10) een aankoop waarin hacken een rol speelde.

We wilden in eerste instantie met benadeelden spreken die in de laatste twaalf maanden waren opgelicht. Dit is standaard in criminologisch onderzoek (Van Wilsem, 2011). Een dergelijk tijdsblok is wenselijk, omdat mensen bijvoorbeeld belangrijke details over langere tijd kunnen vergeten. Omdat de werving van interviewkandidaten tevens via het LMIO verliep, hebben we het tijdsblok bijgesteld naar het afgelopen halfjaar (vanaf 1 januari 2018). Daarmee konden we voorkomen dat dezelfde mensen

4 Het bestuderen van politiedossiers is waardevol omdat ze informatie bevatten over de beweerde feiten, de verdachten, de slachtoffers, getuigenverklaringen, transcripties van politieondervragingen, evenals informatie over het politieonderzoek zelf (Kruisbergen, Van de Bunt & Kleemans, 2012; Kruisbergen, Leukfeldt, Kleemans & Roks, 2018). Dit zou ons kennis kunnen verschaffen over de werkwijze van daders (Van de Bunt, Kleemans, e.a., 2007) en mogelijk over de betrokken partijen.

5 Het voordeel van aanvullende interviews is dat politiedossiers informatie bevatten die gericht is op het bewijzen van criminele activiteiten. Mogelijk dat andere, voor onze analyse relevante informatie niet in de dossiers te vinden zou zijn (zie ook: Leukfeldt (2016)).

werden benaderd voor een interview die mogelijk ook al in de willekeurige selectie van de meldingen zaten.[6]
De werving liep van 28 mei tot en met 2 juli 2018. In totaal zijn 67 benadeelden door het LMIO per e-mail uitgenodigd om deel te nemen aan een interview (zie bijlage III). Tevens zijn twee herinnering-e-mails verstuurd om de respons te verhogen. Omdat slachtofferschap uiteenlopende impact heeft op mensen, is aan een contactpersoon bij het LMIO gevraagd om het eerste contact te leggen met slachtoffers. Het doel hiervan was om vrijwillige toestemming ('informed consent') te verkrijgen van benadeelden om deel te nemen aan een vrijwillig en geanonimiseerd interview. Bovendien stelde het de potentiële interviewkandidaat in staat om vragen te stellen over de zaak.
In totaal hebben 25 mensen positief gereageerd op het verzoek. Eén persoon reageerde negatief op de uitnodiging en de overige personen hebben niets van zich laten horen. Op basis van de positieve reacties zijn vervolgens afspraken gepland voor een telefonisch of face-to-face interview, afhankelijk van de voorkeur van de kandidaten. Uiteindelijk is met het beoogde aantal van twintig personen een interview afgenomen in de periode van 13 juni tot en met 20 september 2018.[7] Vijf personen die positief reageerden op het verzoek, hebben ten tijde van het maken van een concrete afspraak niets meer van zich laten horen of hebben in verband met persoonlijke omstandigheden afgezien van een interview. De uiteindelijke respons is dus 30%.
In totaal zijn twaalf interviews afgenomen via de telefoon en acht bij de benadeelden thuis of op hun werkplek. De interviews duurden gemiddeld 43 minuten (SD = 17; Min. = 20; Max. = 75) en zijn – met toestemming – opgenomen met een opnameapparaat voor uitwerkingsdoeleinden. Eén interview is afgenomen in het Engels, de overige in het Nederlands. De interviews zijn vervolgens per onderwerp uitgewerkt en geanalyseerd.
Een overzicht van de interviewkandidaten is opgenomen in tabel 3.3. De kandidaten bestaan uit zowel mannen als vrouwen, hebben een gemiddelde leeftijd van 42 jaar, uiteenlopend van 22 tot 66 jaar en zijn gemiddeld (n = 7) en hoog (n = 13) opgeleid. Het gemiddelde schadebedrag waarvoor de interviewkandidaten zijn opgelicht is 1.600 euro, met een range van 100 tot 9.000 euro. Omdat we afhankelijk waren van vrijwillige deelname hebben we niet alle typen zaken die we wilden analyseren kunnen includeren. We hebben namelijk geen benadeelden kunnen interviewen uit de categorie 'luierbox'.[8] De platformen waarlangs kandidaten zijn opgelicht zijn divers, zoals Marktplaats, valse webshops en sociale media. Deze diversiteit geldt ook voor de producten.

6 Een beperking van deze werkwijze is dat we geen garantie hadden dat de interviewkandidaten zijn opgelicht vanuit de landen die centraal zijn gesteld in het onderzoek.
7 Door moeizame werving van kandidaten en een tussenliggende zomervakantie is deze periode relatief lang.
8 De wijze van oplichting met webshops die luierboxen aanbieden staat uitvoerig beschreven in openbare bronnen op internet. Een korte beschrijving hiervan is opgenomen in par. 4.2.

Tabel 3.3: Samenvatting van interviewkandidaten (n = 20)

Interview	Geslacht	Leeftijd	Educatie	Type zaak	Platform	Product	Financiële schade
01	Man	61	HBO	Hacken	Ebay.de	Gitaar	650
02	Man	66	MBO	Vakantie	Sunsetjavea (website)	Vakantiehuis	1.000
03	Man	53	HBO	Huurwoningen	Markplaats, Airbnb	Huurhuis	2.400
04	Man	48	MBO	Hacken	Marktplaats, website	Ventilator	300
05	Vrouw	51	HAVO[1]	Vakantie	Short-stay-apartments (website)	Appartement	1.450
06	Vrouw	23	MBO+	Huurwoningen	Huurexpert, Garantwonen (websites), Homeaway-services	Huurappartement	1.200
07	Vrouw	43	HAVO	Auto	AutoScout	Auto	9.000
08	Vrouw	26	HBO	Tickets	Marktplaats	Concertkaartjes (2)	150
09	Man	57	WO	Elektronica	SDI Craft Studio Solutions (website)	Camera	2.650
10	Man	22	HBO	Auto	AutoScout	Auto	2.200
11	Vrouw	36	WO	Elektronica	Marktplaats	E-reader	150
12	Vrouw	35	HBO	Gezocht	Marktplaats	Evenement-kaartjes (6)	200
13	Man	55	HBO	Auto	AutoScout	Auto	2.000
14	Vrouw	34	MBO	Vakantie	Airbnb	Luxe accommodatie	4.200
15	Vrouw	27	HAVO	Huurwoningen	Marktplaats	Huurappartement	1.000
16	Man	27	WO	Sociale media	Facebook	Klusmateriaal	350
17	Man	42	HBO (propedeuse)	Webshop	Vinomz (website)	Gereedschap	100
18	Man	53	WO	Vakantie	VPTenerife (website)	Vakantievilla	2.000
19	Man	38	HBO	Hacken	Marktplaats	Geluidsbox	150
20	Man	41	WO	Sociale media	Facebook	Concertkaartjes (1)	0

1 Mevrouw heeft een diploma behaald in secundair onderwijs volgens Oostenrijks systeem.
Notitie. De schadebedragen zijn naar boven afgerond op 50 euro. Benadeelde 20 heeft geen schade geleden, omdat de bank de betaling kon blokkeren. De initiële schade van benadeelde 20 was 110 euro.

De meeste interviewkandidaten zijn ervaren gebruikers van internet. De meesten (n = 13) gaven aan er sinds de algemene introductie ervan in Nederland gebruik van te maken. Anderen (n = 7) gaven aan internet al zeker tien tot vijftien jaar te gebruiken. De meeste interviewkandidaten doen regelmatig online aankopen. Negen zeiden dit wekelijks of vaker te doen, tien doen dit maandelijks of meerdere keren per maand, en één minder dan één keer per maand. De frequentie van het doen van online aankopen is bij de meesten niet gewijzigd door het slachtofferschap (n = 19). Zeven hiervan gaven overigens wel aan dat het (type) platform waarop ze zijn opgelicht daarop een uitzondering is; die wordt niet meer of in mindere mate gebruikt. Eén kandidaat gaf aan over het algemeen minder online aankopen te doen.

3.3 Expertinterviews

Voor het onderzoek zijn interviews gehouden met experts/deskundigen om tot effectieve handelingsstrategieën tegen internationale aankoopfraude te komen. Diverse experts zijn benaderd omdat ze (a) behoren bij organisaties die zich inzetten voor het verstoren en bestrijden van aankoopfraude en/of belangen behartigen van personen die hiervan slachtoffer worden en (b) behoren tot organisaties die een rol spelen in de crimescripts. De expertinterviews zijn nodig om deelvraag 3 te beantwoorden. Om de interviews in goede banen te leiden, is hiervoor een interviewprotocol ontwikkeld, zie bijlage IV.
We hebben acht interviews afgenomen met in totaal zestien experts. Deze interviews vonden plaats van 19 oktober tot en met 5 december 2018. Zes interviews zijn face-to-face afgenomen en twee telefonisch. De interviews duurden gemiddeld 72 minuten (SD = 16; Min. = 56; Max. = 105) en zijn – met toestemming van de kandidaten – opgenomen met een opnameapparaat voor uitwerkingsdoeleinden. Het overzicht van interviewkandidaten is opgenomen in tabel 3.4. Tevens hebben we met zes leden van de klankbordgroep hierover van gedachten gewisseld in een gezamenlijke bijeenkomst; twee leden gaven via e-mail hun input. We hebben getracht om met nog meer organisaties in gesprek te gaan, maar dat is niet gelukt. Het gaat hierbij om Europol (European Cybercrime Centre; EC3), Knooppunt FinEC van de Nationale Politie, Autoriteit Consument en Markt (ACM) en de Consumentenbond.

Tabel 3.4: Overzicht van expert-interviewkandidaten (in volgorde van afname)

Naam	Organisatie	Functie
Steven Goudberg	ING	CFE en Fraudespecialist; tevens werkzaam binnen het ECTF
Chiel van Spaandonk	SIDN	Specialist Registratie en Service
Tanya Wijngaarde	Fraudehelpdesk	Communicatiemedewerker
Cynthia Hukom	Fraudehelpdesk	Coördinator Front Office
Eva Calvelo Muiño	ECC	Projectleider
Marleen Ottens	ECC	Juridisch medewerker
Alexander Eristavi	City of London Police	Detective Sergeant | Business Stakeholder Manager NFIB
Holly Rattray	City of London Police	Intelligence Researcher
Gian Luca Berruti	Guardia di Finanza	Lieutenant Colonel – Anti Fraud Technical Unit
Koen Juffermans	ICS	Manager Investigations
Britta Meulenbroek	ICS	Investigator
Anoniem (N = 5)	EIB	-

Notitie. CFE (certified fraud examiner), ECTF (Electronic Crime Task Force), SIDN (Stichting Internet Domeinregistratie Nederland), ECC (Europees Centrum voor de Consumenten), NFIB (National Fraud Intelligence Bureau), ICS (International Card Services), EIB (Economische Inspectie België). NB: Alle kandidaten, met uitzondering van experts van de EIB, hebben expliciet toestemming gegeven dat hun naam en organisatie genoemd mogen worden in het onderzoeksrapport.

We hebben de handelingsstrategieën tegen aankoopfraude gecategoriseerd op basis van bestaande overzichten die zijn ontwikkeld voor situationele criminaliteitspreventie. In hun artikel schetsen Cornish en Clarke (2003) 25 technieken voor situationele criminaliteitspreventie die zijn geclassificeerd onder vijf categorieën. Deze categorieën zijn: (1) vergroten van inspanning om criminaliteit te plegen; (2) vergroten van het risico om criminaliteit te plegen; (3) beperken van de beloningen van criminaliteit; (4) verminderen van provocaties die uitnodigen tot criminaliteit; en (5) wegnemen van excuses voor crimineel gedrag. Het raamwerk met 25 technieken hebben we ten behoeve van dit onderzoek ingevuld met specifieke mogelijkheden om online aankoopfraude vanuit het buitenland tegen te houden dan wel te verstoren.

3.4 Deskresearch

Als uitkomst van de dossieranalyse en de reconstructie verwachtten we een lijst met partijen die bewust of onbewust betrokken zijn bij de crimescripts van internationale aankoopfraude (zie par. 4.4 voor het resultaat). Met deskresearch is onderzocht in hoeverre betrokken partijen voor onderhavige context een zorgplicht hebben jegens (potentiële) slachtoffers. Deze exercitie is nodig voor de beantwoording van deelvraag 4.

Dit onderdeel is gebaseerd op een literatuurstudie, waarbij gestart is vanuit de basis van het vraagstuk, te weten het EU-verdrag, het Burgerlijk Wetboek (BW) en de wetsgeschiedenis. Hiervoor is de database van Kluwer Navigator geraadpleegd, waar de meest recente informatie online te vinden is. Bij de behandeling van de Nederlandse wetsartikelen is gebruikgemaakt van de Groene Serie van het Verbintenissenrecht alsmede de daarbij aangegeven jurisprudentie en (tijdschrift)artikelen. Daarnaast is vakliteratuur geraadpleegd voor verdiepende commentaren. Actuele uitspraken, in lijn met de basisjurisprudentie, zijn gevonden op de websites van de Europese Unie (EU) en het Hof van Justitie van de Europese Unie (HvJ).[9]

In de volgende drie hoofdstukken worden de resultaten gepresenteerd. Allereerst worden de verschillende crimescripts in kaart gebracht en wordt stilgestaan bij de betrokken partijen in de crimescripts (hoofdstuk 4). Vervolgens staan de handelingsstrategieën tegen aankoopfraude vanuit het buitenland centraal (hoofdstuk 5). Tot slot komt de juridische zorgplicht die betrokken partijen hebben in relatie tot (het voorkomen en verstoren van) aankoopfraude aan bod (hoofdstuk 6).

9 Zie respectievelijk https://europa.eu/ en https://curia.europa.eu/.

4. Crimescripts van internationale aankoopfraude

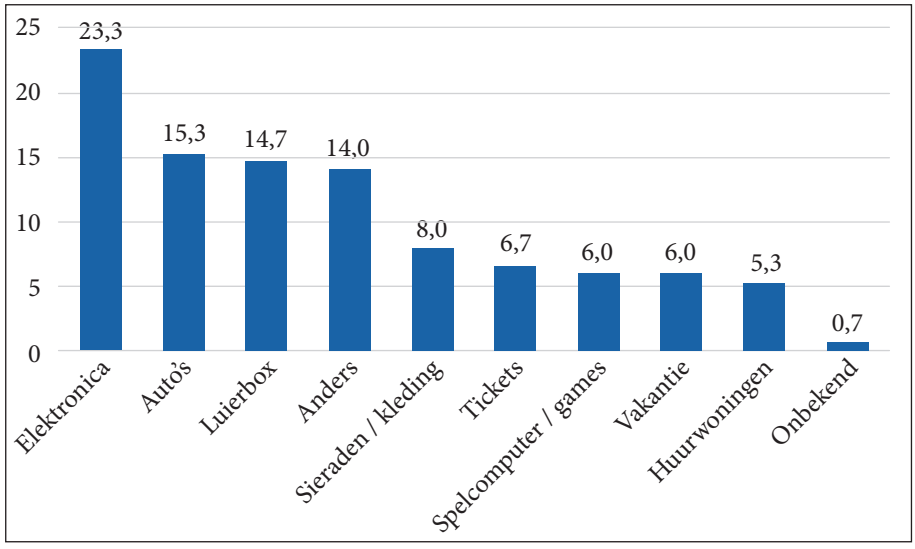
In dit hoofdstuk staan de crimescripts centraal. De inzichten zijn opgedaan aan de hand van de dossieranalyse (zie par. 4.2; globale werkwijze) alsook de reconstructie (zie par. 4.3; gedetailleerde werkwijze). Een overzicht van de bevindingen is gepresenteerd in paragraaf 4.4. Voordat we ingaan op de crimescripts staan we eerst stil bij de kenmerken van aankoopfraude vanuit het buitenland (par. 4.1).[1]

4.1 Kenmerken van internationale aankoopfraude

Allereerst bespreken we de productcategorieën waarmee is gefraudeerd (zie figuur 4.1). De categorie die op basis van de dossieranalyse het vaakst werd genoemd is elektronica. Hieronder vallen producten als smartphones, tablets en koffiemachines. Deze wordt gevolgd door de categorie auto's (hieronder vallen bijvoorbeeld ook vrachtwagens en caravans); luierboxen – een specifieke productcategorie die voorkomt in 2017 – en de categorie 'anders'. Onder die laatste categorie vallen zaken als speelgoed, gereedschap en medische tests. In één geval was het onbekend met wat voor product een benadeelde is opgelicht.

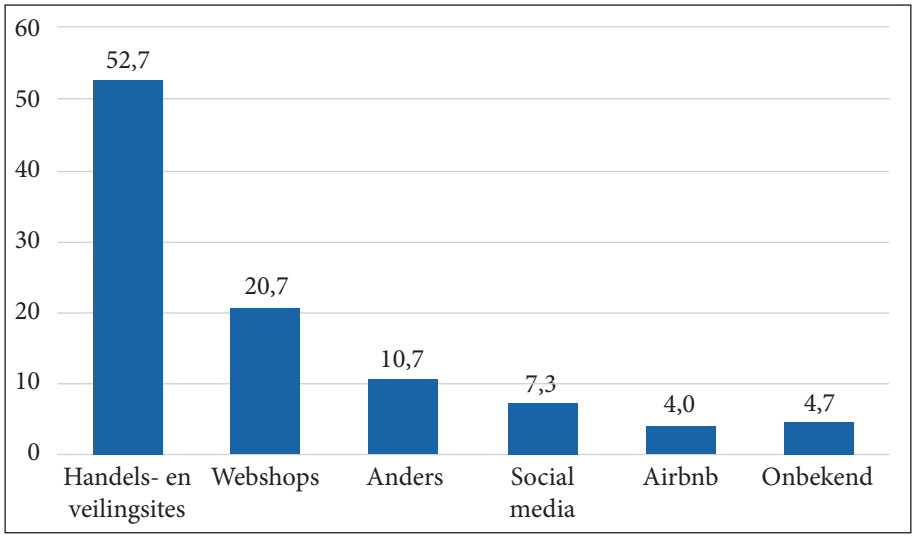
1 Het incident dat de geïnterviewde benadeelden hebben meegemaakt had voor allen financiële effecten. Bijna alle benadeelden hebben hun geld niet teruggekregen. Voor een groot deel van de benadeelden was het naast een vervelende ervaring niet veel meer dan dat. Voor ongeveer een derde van de benadeelden had het incident wel psychologische en emotionele effecten. Deze effecten bestonden onder andere uit slapeloze nachten, een slecht humeur en teleurstelling. Eén benadeelde ervaarde het incident als traumatisch. Meer informatie over de effecten en de impact van het incident op de slachtoffers is te lezen in bijlage V.

Figuur 4.1. Productcategorieën in percentages (n = 150)



Vervolgens hebben we gekeken via welk online platform benadeelden in contact zijn gekomen met fraudeurs (zie figuur 4.2). In meer dan de helft van alle geanalyseerde zaken vond het eerste contact plaats via online handels- en veilingsites. De meest voorkomende hierbij is Marktplaats (30,0%), gevolgd door eBay (8,0%), Speurders (3,3%), handelssites voor auto's (3,3%) – zoals AutoScout24 –, en overige handels- en veilingsites (10,7%). Onder deze laatste vallen sites zoals Tweedehands.nl/.be/.net, Marktplaza.nl en Subito.it. Daarnaast zijn een op de vijf benadeelden opgelicht via webshops; zowel door valse (bijvoorbeeld Luierbox.be) als via legitieme (bijvoorbeeld Groupon). Benadeelden zijn in mindere mate opgelicht via sociale media – met name Facebook – en Airbnb. In zestien gevallen verliep het eerste contact op een andere manier. Hierbij gaat het bijvoorbeeld om contact via online fora (bijvoorbeeld op de website Tweakers) of websites waarop huurwoningen worden aangeboden (bijvoorbeeld via de website Kamernet). In zeven gevallen is het eerste contactmoment onbekend.

Figuur 4.2. Platform in percentages (n = 150)



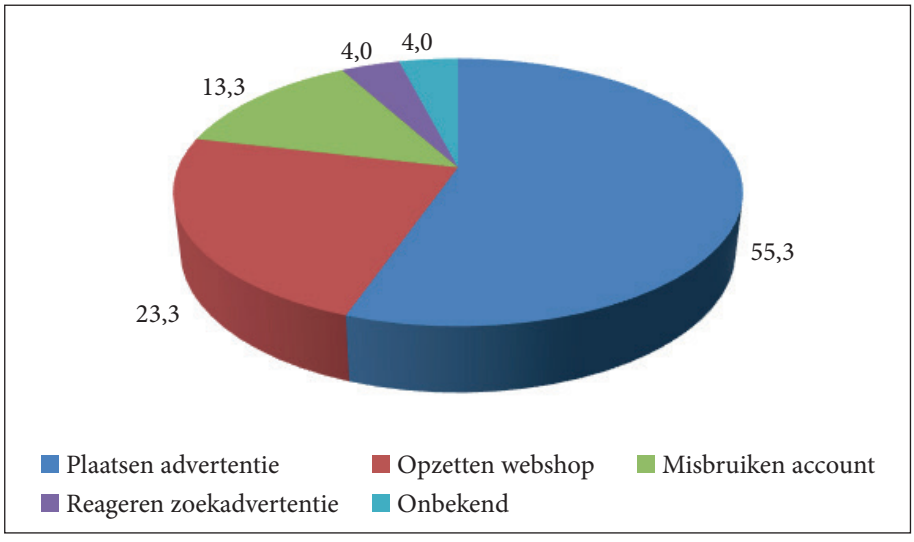
Daarnaast waren we geïnteresseerd of, en zo ja op welke manier, benadeelden en fraudeurs op andere manieren contact hebben gehad met elkaar; dus naast of na het initiele contact via het betreffende platform. In 62 gevallen hebben we hier geen weet van; dan is het niet geregistreerd door de aangever. In de resterende gevallen gaf ongeveer twee derde (62,5%) aan aanvullend contact te hebben gehad via e-mail en ongeveer een op de vijf (20,5%) via e-mail én aanvullende communicatiemiddelen, zoals sms, WhatsApp-berichten en telefoon. In de overige 17,0% van de gevallen was er óf geen verdere vorm van contact, óf verliep het aanvullende contact niet via e-mail, maar uitsluitend via WhatsApp, telefoon, sociale media en/of Groupon.
In veruit de meeste gevallen (94,7%) is het eerste contact gelegd door de benadeelde, bijvoorbeeld door te reageren op een advertentie of door een product of dienst 'aan te schaffen' via een webshop. In zeven gevallen werd duidelijk dat de fraudeur initiatief nam in het contact. In deze gevallen gaat het om een benadeelde die een 'gezocht-advertentie' heeft geplaatst. In één geval is onbekend wie het contact heeft geïnitieerd.

4.2 Globale werkwijze fraudeurs

Op basis van voorgaande resultaten blijkt dat het slachtoffer veelal in een val loopt die klaarstaat; een enkele keer wordt het slachtoffer actief door de dader opgezocht. In deze paragraaf gaan we dieper in op de algemene werkwijzen die fraudeurs toepassen om de poging tot fraude te laten slagen. De resultaten zijn gebaseerd op de dossieranalyse. In de volgende paragraaf (4.3) gaan we gedetailleerd in op een aantal specifieke

werkwijzen zoals we die hebben kunnen reconstrueren op basis van de slachtofferinterviews.
Nadere analyse van de meldingen laat zien dat in 32,7% van de gevallen de fraudeur zich voordeed als een zakelijke partij, bijvoorbeeld door een bedrijfsnaam te noemen in een advertentie op een handelssite of een product te verkopen via een valse webshop. In 30,7% van de gevallen weten we vrij zeker dat de fraudeur zich voordeed als een particuliere verkoper, bijvoorbeeld door uit 'eigen' naam een product aan te bieden op een veilingsite. In 36,7% van de gevallen was niet precies duidelijk vanuit welke hoedanigheid de fraudeur opereerde.
Hoewel dit onderzoek zich richt op betalingen die zijn overgemaakt naar België, Duitsland, het Verenigd Koninkrijk en Italië, is uit de data niet goed op te maken vanuit welk land de fraudeur opereerde. In meer dan de helft van de gevallen is dit onbekend. Het viel wel op dat buiten de vier genoemde landen, fraudeurs aangaven zich te bevinden in bijvoorbeeld Nederland, Spanje en Zweden.
Vervolgens hebben we gekeken naar de crimescripts. Op basis van de beschikbare data kunnen we op hoofdlijnen vier crimescript-categorieën identificeren, waarbij: (1) fraudeurs gebruikmaken van (de naam van) beschikbare platformen om producten 'aan te bieden', (2) fraudeurs een valse webshop opzetten waar ze producten 'verkopen', (3) fraudeurs misbruik maken van de betrouwbaarheid van een persoonlijk account of de betrouwbaarheid van een bedrijfsnaam, en (4) fraudeurs reageren op zoekadvertenties van anderen. In zes gevallen was het crimescript onbekend (zie figuur 4.3).

Figuur 4.3. Crimescripts online aankoopfraude vanuit het buitenland in percentages (n = 150)



In alle onderzochte landen is het plaatsen van een valse advertentie (categorie 1) het meest gebruikte crimescript (België 22,0%; Duitsland 16,7%; Verenigd Koninkrijk 9,3%; Italië 7,3% van het totaal aantal meldingen). Valse advertenties worden voornamelijk gebruikt om te frauderen met elektronica (18,0% van alle fraudes), auto's (14%), sieraden/kleding (6,7%) of andere producten (6,0%) zoals een kinderwagen, snijmachine of boek. De fraudeur plaatst in dit geval een valse advertentie van een product of dienst en wacht reacties af. Als iemand het product wil kopen, laat de fraudeur het geld overmaken en levert het product niet.

In de meeste gevallen wordt de advertentie vlak na de betaling verwijderd. In enkele gevallen blijft de advertentie enige tijd online, naar verwachting om meerdere betalingen te ontvangen. Dit is gebaseerd op enkele meldingen waar een vriend/familielid onder een andere naam op dezelfde advertentie reageert, waarna de fraudeur laat weten dat het product nog niet is verkocht. Deze wijze van oplichting vergt weinig specifieke IT-kennis of 'social engineering'-vaardigheden. Bij dit type crimescript kan het voorkomen dat de benadeelde het product wil ophalen. In meerdere meldingen werd aangegeven dat de fraudeur dan claimt dat de afstand tot de benadeelde te groot is om het product af te halen.

Het opzetten van een valse webshop (categorie 2) wordt voornamelijk gebruikt door fraudeurs met een ontvangend rekeningnummer in België (16,0% van het totaal aantal aangiften) en in mindere mate in Duitsland (4,7%) en het Verenigd Koninkrijk (2,7%). In de analyse is geen melding gevonden betreffende een valse webshop met een ontvangend rekeningnummer in Italië. De fraudeurs maken een valse webshop waar benadeelden een product kunnen bestellen en geld kunnen overmaken, waarna het product vervolgens niet wordt geleverd. Valse webshops zijn gemaakt voor het verkopen van merkmeubels (zoals eetkamerstoelen), soa-testen en keukens.

De meeste benadeelden zijn opgelicht door een valse webshop die luierboxen van Pampers verkocht (14,7% van het totaal meldingen). Via Groupon, Facebook of de websites luierbox.be en pamperbox.be werd een jaarcontract voor Pampers luiers aangeboden. In de meeste gevallen is een enkele doos of zijn de eerste paar dozen geleverd, waarna de levering uiteindelijk stopte.[2] Bij deze valse webshop wordt dus in de meeste gevallen een deel van het product wel geleverd. De webshop reageert in het begin op e-mails over verkeerde adressen, verkeerde maten of verlate leveringen en verbreekt vervolgens het contact. Een grote groep is slachtoffer geworden van deze valse webshop. Enkele benadeelden gaven aan lid te zijn van de Facebook-groep 'pamperboxgedupeerden' die meer dan 2.000 leden heeft. In januari 2017 heeft het FOD Economie in

2 Hoewel deze vorm van oplichting niet exact binnen onze definitie van aankoopfraude valt, hebben we oplichting met pamperboxen wel als zodanig geregistreerd. De reden hiervoor was dat het in de meldingen die wij hebben geanalyseerd ook voorkwam dat men geen enkele box heeft ontvangen, waardoor het wel binnen onze definitie past.

België 800 meldingen binnen gekregen en vroeg andere benadeelden om ook aangifte te doen.[3,4,5]

Door het misbruik maken van de betrouwbaarheid van een persoonlijk account of bedrijfsnaam (categorie 3), wordt in 6,0% van de geanalyseerde aangiften geld overgemaakt naar het Verenigd Koninkrijk, 4,7% naar Duitsland en 2,7% naar Italië. In de data is voor deze categorie geen melding gevonden waarin geld is overgemaakt naar België.

Bij misbruik van de betrouwbaarheid van een persoonlijk account wordt een account met een goede beoordeling gehackt om een frauduleuze advertentie te plaatsen. Eventueel wordt het contact voorgezet op het e-mailadres van de fraudeur en in alle gevallen wordt uiteindelijk een betaling gedaan naar het (aangepaste) rekeningnummer van de fraudeur. Hierbij wordt dus het vertrouwen gewonnen door de positieve beoordelingen van het gehackte account. Een voorbeeld is de zaak waarin een eBay-account met meer dan 50 positieve beoordelingen werd gehackt. Door de getoonde beoordelingen vertrouwde de benadeelde de tegenpartij om het geld over te maken. Na deze betaling kreeg de benadeelde een bericht van eBay dat de advertentie was verwijderd. Opnieuw is na betaling het contact verbroken en heeft geen levering plaatsgevonden.

Tevens wordt misbruik gemaakt van de betrouwbaarheid of reputatie van bedrijven. Hier wordt ook een advertentie geplaatst op een betrouwbare site om in contact te komen met potentiële benadeelden, maar dan vanuit de naam van een bedrijf. Vervolgens worden middels e-mailcontact verdere gegevens besproken en wordt uiteindelijk een betaling gedaan. De fraudeur stuurt een bevestigingsmail van betaling uit naam van het bedrijf, waarna het contact wordt verbroken.

Het reageren op een zoekadvertentie (categorie 4) wordt door een kleine groep fraudeurs toegepast. In 2,7% van alle geanalyseerde meldingen wordt geld overgemaakt naar Duitsland en in 0,7% wordt geld overgemaakt naar België en het Verenigd Koninkrijk. De dader reageert op een zoekadvertentie van de benadeelde. Vervolgens maakt de benadeelde geld over, maar krijgt het product niet geleverd. Drie meldingen betreffen het zoeken naar tickets, waarna het product niet geleverd is. Bij ticketfraude wordt een zoekadvertentie voor bijvoorbeeld een bepaalde voetbalwedstrijd gezocht. De fraudeur reageert op deze advertentie en laat geld overmaken.

Tot slot hebben we gekeken naar schadebedragen per crimescript-categorie, zie tabel 4.1. Het misbruiken van een account heeft de hoogste gemiddelde schade, gevolgd door het plaatsen van een advertentie. Het misbruik maken van een zoekadvertentie of valse webshop heeft een lager gemiddeld schadebedrag. Dit laatste kan vermoedelijk te

3 FOD Economie (2017). *Gedupeerden van luierboxen kunnen zich aanmelden via meldpunt FOD Economie*. Via: https://news.economie.fgov.be/163195-gedupeerden-van-luierboxen-kunnen-zich-aanmelden-via-meldpunt-fod-economie.

4 HLN (2018). *Groupon betaalt ruim duizend gedupeerden van Luierbox dan toch terug*. Via: https://www.hln.be/nieuws/binnenland/groupon-betaalt-ruim-duizend-gedupeerden-van-luierbox-dan-toch-terug~a7a3da4b/?referer=.

5 Het strafrechtelijk onderzoek tegen de dader liep ten tijde van het onderzoek (eind 2018) nog. Volgens de organisatie Test-Aankoop komen 1.269 benadeelden wel in aanmerking voor een vergoeding van Groupon, die de schadevergoeding als een overeenkomst ziet en niet als erkenning van schuld of tekortkoming.

maken hebben met het type product dat via valse webshops wordt 'aangekocht', zoals pamperboxen. Een statistische verkenning laat zien dat het verschil tussen de crimescript-categorieën significant is wat betreft de gemiddelde schadebedragen. Dit verschil is echter slechts een indicatie voor een werkelijk verschil. Om dit verschil reëel in kaart te brengen is een grotere steekproef vereist en zouden de categorieën meer evenredig verdeeld moeten zijn. Omdat de maximumschadebedragen grote invloed kunnen hebben op de gemiddelde schadebedragen is eveneens de mediaan gepresenteerd in de tabel. Het verschil tussen het gemiddelde schadebedrag en de centrummaat is bij 'advertentie plaatsen' het meest opvallend.

Tabel 4.1 Schadebedrag in euro's per crimescript-categorie (n = 150)

Crimescript-categorie	N	Gemiddelde	SD	Mediaan	Min.	Max.
Misbruiken account	20	1.596	1.878	1.166	80	8.700
Advertentie plaatsen	83	1.391	2.464	210	21	14.000
Opzetten valse webshop	35	474	542	350	17	2.500
Reageren zoekadvertentie	6	127	145	81	33	420
Onbekend	6	110	80	78	42	250

Notitie. N = aantal, SD = standaarddeviatie, Min. = minimum, Max. = maximum.

Betalingswijze

De meeste benadeelden hebben het gehele bedrag overgemaakt naar de fraudeur. Slechts twaalf benadeelden hebben met de fraudeur afgesproken om het bedrag in delen te betalen. Dikwijls werd dit door de fraudeurs zelf voorgesteld, naar verwachting om hun doelwit over de streep te trekken om over te gaan tot koop. Ondanks deze afspraak hebben zes van deze benadeelden alsnog het gehele bedrag overgemaakt naar de fraudeurs, twee benadeelden ongeveer de helft en één benadeelde een kwart. Van drie benadeelden is onbekend hoeveel geld uiteindelijk is overgemaakt.

De online betalingen naar het buitenland zijn op verschillende manieren uitgevoerd. Bij het maken van een melding bij het LMIO hebben benadeelden de keuze uit een bankoverschrijving (met IBAN), een buitenlandse overschrijving (zonder IBAN), iDEAL (niet verder gespecificeerd) en iDEAL met IBAN. Een bankoverschrijving is het verplaatsen van een bedrag naar een andere rekening door directe opdracht van de verzender. Betaling via iDEAL wordt veelal toegepast in webwinkels om te betalen via de bank van de klant; na het inloggen bij de eigen bank hoeft alleen de betaling nog bevestigd te worden. IBAN wordt gebruikt om internationale transacties beter te laten verlopen tussen rekeningen en banken uit verschillende landen. De meeste benadeelden hebben gebruikgemaakt van een bankoverschrijving met IBAN (71,3%). Een kleinere groep heeft gebruikgemaakt van een buitenlandse overschrijving zonder IBAN (8,7%). Van de geanalyseerde aangiften heeft 13,3% betaald via iDEAL (met IBAN) en 6,7% via iDEAL (niet verder gespecificeerd).

Aanvullend hebben we gekeken naar het contact ná de betaling. Hierbij viel op dat benadeelden nog een tijd aan het lijntje werden gehouden (46,0%). Een voorbeeld hiervan zijn de valse luierbox-webshops. Mogelijk is daardoor een grotere groep slachtoffer geworden. Ook zagen we dat het contact met de benadeelde direct door de fraudeur werd verbroken (42,0%). In dit geval verbreekt de fraudeur het contact relatief snel nadat de betaling is ontvangen. In 12,0% van de gevallen hebben we hier geen aanvullende informatie over kunnen vinden.
Tot slot hebben we gekeken in hoeverre er op basis van de meldingen aanwijzingen waren voor aanliggende vormen van criminaliteit. In zeventien gevallen is er een indicatie van mogelijk identiteitsmisbruik. In acht gevallen is misbruik gemaakt van een persoonlijke identiteit en in zeven gevallen is misbruik gemaakt van een zakelijke identiteit. De overige meldingen zijn niet toereikend om een uitspraak te doen over identiteitsmisbruik.

4.3 Gedetailleerde werkwijze fraudeurs

Van de meeste categorieën van aankoopfraude hebben we slachtoffers kunnen spreken. De uitzondering hierop was pamperfraude. Door middel van slachtofferinterviews is het fraudeproces van twintig aankoopfraudezaken gereconstrueerd. De bevindingen daarvan zijn hier gepresenteerd en zijn onderverdeeld in de volgende categorieën: (1) auto's, (2) elektronica, (3) tickets, (4) vakantiewoningen, (5), huurwoningen, (6) sociale media, (7), webshop, (8) gezocht-advertenties, en (9) hacken. Let op dat het niet elkaar uitsluitende categorieën zijn. Zo gaat het in een van de 'sociale media'- en 'gezocht'-gevallen om de aankoop van tickets en gaat het in beide 'hacken'-gevallen om de aanschaf van elektronische apparaten. In onderstaande beschrijvingen van werkwijzen wordt de fraudeur of oplichter aangeduid met de term 'verkoper' of 'verhuurder'.
De interviews leverden rijke data op. Details die interessant zijn, maar niet essentieel voor het verhaal zijn gekaderd. Dit betreft het perspectief van de klant op (onderdelen van) het incident en valt derhalve buiten de aanvalsstrategie. Deze kaders kunnen dus, om de snelheid van het lezen te bevorderen, worden overgeslagen. Per categorie is één casus uitgewerkt. De resterende elf casussen zijn ondergebracht in bijlage VI. Wat tot slot nog interessant is om te vermelden, is dat negen kandidaten aangaven eerder slachtoffer te zijn geweest van een dergelijke fraude-incident of dat ze later nogmaals op eenzelfde wijze werden opgelicht (i.e. herhaald slachtofferschap).

Casus 1: Oplichting met auto's
We hebben drie interviews afgenomen met personen die waren opgelicht met de aanschaf van een auto. Kandidaten 7 en 10 waren allebei actief op zoek naar een auto en hun verhalen kwamen sterk overeen. Voor kandidaat 13 ging het om de aanschaf van een oldtimer. De casus van kandidaat 7 (hierna aangeduid met mevrouw) is hier uitgewerkt.
Mevrouw maakte gebruik van de website AutoScout24 om een auto te zoeken. Via de website kwam ze in contact met een verkoper die aangaf dat hij woonachtig is in Noor-

wegen – van oorsprong Noors is – en dat de auto die ze wilde daar nu ook was. De verkoper gaf aan dat het voor hem te duur zou zijn om de auto op naam te zetten in Noorwegen en bood aan om de auto op te sturen via een transportbedrijf. Eveneens vermeldde hij daarbij dat de auto, indien die niet beviel, binnen vijf dagen kosteloos retour gestuurd kon worden. Ook vroeg de verkoper om een kopie van een identiteitsbewijs voordat de verkoop kon beginnen. Mevrouw stuurde hierop een kopie van haar rijbewijs. De helft van het totaalbedrag moest worden overgemaakt om over te gaan tot verscheping van de auto. Voor de verscheping werd een transportbedrijf ingezet (AB Transport Service Ltd.) en er werd een Track&Trace-code gegeven, zodat mevrouw het transport van de auto kon volgen.
De dader heeft mevrouw viermaal om geld gevraagd, waarvan mevrouw drie keer een bepaald bedrag heeft overgemaakt. Nadat mevrouw het eerste bedrag van 3.750 euro had overgemaakt, kreeg ze bericht terug van de verkoper dat de naam van de rekening niet overeenkwam met de naam op de vervoerspapieren en vroeg daarom nogmaals het bedrag over te maken. Dit deed mevrouw niet. Vervolgens werd contact opgenomen met wederom het verzoek om te betalen, maar nu werd aangedragen dat dit moest, zodat de auto verzekerd vervoerd kon worden. Volgens de verkoper was haast geboden, want als de auto al op transport zou zijn, zou het haar nog meer geld gaan kosten. Nadat de tweede 3.750 euro betaald was, werd een derde keer contact gezocht door de verkoper. Ditmaal werd verzocht om een 'borg' te betalen bij de Duitse grens. Het ging om een bedrag van 2.300 euro. Ook dit bedrag maakte mevrouw over. Uiteindelijk vroeg de verkoper een vierde keer om geld over te maken. Daarbij gaf de verkoper aan zelf ook geld bij te leggen en dat mevrouw het restant later terug zou krijgen. Eveneens werd haar aangeraden om geld bij familie of vrienden te lenen. Dit heeft mevrouw niet gedaan.

Mevrouw heeft een week na de laatste betaling gebeld met het verzoek de aankoop te annuleren en het betaalde bedrag, minus de onkosten die daaraan verbonden zouden zijn, terug te krijgen. De verkoper gaf aan dat het wel goed zou komen – dat ze haar geld terug zou krijgen – en maande mevrouw om niet meer te bellen. Een week later belde mevrouw anoniem, maar toen werd er niet opgenomen. Wel kreeg ze een 'boze' e-mail waarin wederom werd aangegeven dat ze niet meer mocht bellen. Daarna was de advertentie offline gehaald en werkten de e-mailadressen en telefoonnummers niet meer. Daarop heeft mevrouw advies ingewonnen bij de politie. De politie gaf aan dat de auto niet op naam van de betreffende verkoper stond en adviseerde haar om aangifte te doen van identiteitsfraude.

Mevrouw maakte de eerste twee geldbedragen voor de auto over naar een Kroatisch bankrekeningnummer. Mevrouw gaf aan dat de verkoper hierbij verklaarde het geld niet direct zelf te mogen ontvangen. Het derde bedrag werd overgemaakt naar een

Engels bankrekeningnummer dat zou toebehoren aan het Britse transportbedrijf. Mevrouw gaf aan dat er in het Engels werd gecommuniceerd met de verkoper en het transportbedrijf. Naast e-mailcontact heeft mevrouw ook telefonisch contact gehad. Mevrouw gaf aan met drie verschillende mensen gesproken te hebben van het transportbedrijf, via één telefoonnummer. Na doorvragen over de verzonden kopie van het rijbewijs gaf mevrouw aan niet te hebben gemerkt dat haar identiteit is misbruikt.

Bij doorvragen kunnen benadeelden zich mogelijk aanvullende zaken herinneren die vertrouwen wekten om door te gaan met de aankoop. Een eerdere positieve ervaring met AutoScout24 gaf mevrouw een vertrouwd gevoel. Bovendien was de advertentie zichtbaar op meerdere autoverkoopsites. Mevrouw ontving gegevens van het transportbedrijf en voerde daarop verschillende controles uit die goed leken. Bovendien had mevrouw dit nog door een collega laten controleren. Het kenteken leek te kloppen, het transportbedrijf had een KvK-nummer en de verkoper was zichtbaar op de bedrijfswebsite en sociale media waar hij claimde te werken. Mevrouw gaf vervolgens aan dat de daders erg vriendelijk waren aan de telefoon en beloofden dat alles goed zou komen. Mevrouw gaf tevens aan dat naïviteit en hebberigheid hierin hebben meegespeeld. Omdat ze geld had overgemaakt ging ze ervan uit dat ze waar voor haar geld kreeg. Hier speelde ook mee dat de verkoper zelf geld zou betalen – en daarvoor zelfs een lening moest afsluiten – voor het transport. Ook wekte het ontvangen van een Track&Trace-code vertrouwen, die mevrouw kreeg nadat ze onverwacht belde. Daarnaast ondersteunde de Track&Trace-informatie dat de auto in Duitsland voor de grens stond.

Casus 2: Oplichting met elektronica

We hebben met twee mensen gesproken die waren opgelicht met de aanschaf van elektronica (kandidaten 9 en 11). De casus van kandidaat 11 (hierna aangeduid met mevrouw) is hier uitgewerkt.

Mevrouw was voor haar dochter op zoek naar een e-reader. Omdat dit 'een nogal prijzig dingetje' was zocht mevrouw naar een tweedehands exemplaar op Marktplaats. Op een gegeven moment zag mevrouw een advertentie waarin een e-reader werd aangeboden. Deze was volgens haar niet opvallend goedkoop: 'Het zou kunnen dat iemand het daarvoor wil verkopen.' De communicatie was in het Nederlands en verliep via de Marktplaats-app. De verkoper deed zich vriendelijk voor en er waren dan ook geen signalen dat het niet zou kloppen. Het enige wat mevrouw vreemd vond, was dat ze het bedrag moest overmaken naar een Engels bankrekeningnummer. De verkoper had daar echter een goed verhaal bij, namelijk dat haar Nederlandse bankrekeningnummer nog niet was geactiveerd. Mevrouw maakte het geld via een bankoverschrijving over, waarna de verkoper liet weten het bedrag te hebben ontvangen. De verkoper bedankte haar, gaf aan dat ze bij vragen die altijd kon stellen en dat mevrouw binnenkort een

Track&Trace-code zou ontvangen. Die code heeft mevrouw echter niet gekregen, evenmin als het product. Na een paar dagen wachten probeerde mevrouw nog contact te leggen met de verkoper, maar zonder succes. Ook gaf ze aan aangifte te zullen doen wanneer ze geen tegenbericht zou ontvangen. Dat leverde echter ook niets op. Later zag ze dat de advertentie was verwijderd.

Mevrouw had vooraf geen controles uitgevoerd om te kijken of de betreffende verkoper een legitieme verkoper is. Mevrouw wist dat oplichting met iPhones en dergelijke veel voorkomt, maar verwachtte niet dat er ook werd opgelicht met e-readers. Mevrouw gaf aan dat ze in het gesprek met de verkoper gehaast was, omdat ze op vakantie was. Ze gaf aan daardoor mogelijk minder goed te hebben opgelet. Achteraf vond mevrouw het opmerkelijk dat de verkoper vroeg over welke bank mevrouw beschikte. Ook vond ze het achteraf vreemd dat de verkoper haar bankrekeninggegevens verstuurde in een afbeelding met wit-gekleurd lettertype en een zwarte achtergrond. 'Ik had dat nog nooit gezien, maar dacht: ja, whatever, misschien gebruikt ze dat wel standaard.'

Casus 3: Oplichting met tickets

Van de categorie 'tickets' is met één benadeelde gesproken. Kandidaat 8 (hierna aangeduid met mevrouw) was een dag voor een festival op zoek naar twee dagkaarten. Mevrouw zag een advertentie op Marktplaats waar vijf dagkaarten werden aangeboden à 65 euro. Normaal gesproken waren de kaarten 110 euro. Mevrouw kon zien dat de particuliere verkoper zevenenhalf jaar actief was op Marktplaats en positieve recensies had.[6] Bovendien werd duidelijk dat de verkoper meerdere tickets verkocht op het account. Mevrouw probeerde contact te leggen via de telefoon, maar dat leverde geen gehoor op, waarna ze de verkoper een bericht stuurde via WhatsApp. Hierop volgde wel contact en is overeengekomen om twee tickets te kopen. Het contact verliep in het Nederlands. Mevrouw stelde voor om de betaling te verrichten via het veilige betaalsysteem van Marktplaats. De verkoper weigerde dit en gebruikte als excuus dat dit niet mogelijk was, omdat hij een Duits bankrekeningnummer had. Mevrouw overlegde met haar vriend en besloot toch het geld over te maken via een bankoverschrijving. Ze stuurde de verkoper een screenshot van de betalingsbevestiging via WhatsApp, waarbij ze belangrijke details onleesbaar had gemaakt. Daarna is mevrouw direct geblokkeerd op WhatsApp.

6 Het zou kunnen zijn dat het betreffende account was gehackt. Dit kunnen we echter niet verifiëren.

Mevrouw gaf aan vertrouwen te hebben in de aankoop, omdat het account van de verkoper al lang actief was, de recensies goed waren en de verkoper informatie over zichzelf gaf. 'Hij vertelde over zijn vier dochters, over zichzelf en zijn foto op WhatsApp leek authentiek.' Mevrouw twijfelde nog wel even aan de betrouwbaarheid toen een Duits bankrekeningnummer werd opgegeven, terwijl de verkoper aangaf in Friesland te wonen. Maar door haar enthousiasme was ze toch met de aankoop doorgegaan. Ze had geen verklaring gevraagd voor het Duitse rekeningnummer en handelde volgens eigen zeggen te snel. 'Mijn enthousiasme won het van mijn verstand.' Mevrouw gaf aan in het verleden een keer eerder op een dergelijke wijze te zijn opgelicht. Toen ging het ook om tickets, maar bleek het account van de verkoper maar één dag actief te zijn.

Casus 4: Oplichting met vakantiewoningen

In totaal zijn vier personen geïnterviewd die waren opgelicht met de huur van een vakantiewoning. In drie gevallen ging het om een accommodatie in Spanje (kandidaten 2, 14 en 18) en in één geval om een accommodatie in Nederland (kandidaat 5). De casus van kandidaat 2 (hierna aangeduid met meneer) is hier uitgewerkt.

Meneer was op zoek naar een vakantiehuis in Spanje om daar samen met zijn vrouw een paar maanden te verblijven. Via een zoekslag op Google kwam meneer uit bij de website Sunsetjavea. Via de website kwam meneer in contact met een persoon achter de website om de reservering te bevestigen. Dit gebeurde via een 'info@'-adres en de communicatie vond plaats in goed Engels. Meneer moest onder meer paspoortnummers doorsturen. Vervolgens is een huurcontract opgemaakt en werd gevraagd om een maand huur en borg over te maken, in totaal 1.000 euro. Vervolgens maakte meneer het geld over naar een Italiaans bankrekeningnummer. Ook stuurde meneer op verzoek een bevestiging van de overboeking. Daarna was er geen communicatie meer. Meneer zocht via internet het telefoonnummer op van Sunsetjavea, belde dit nummer en vroeg naar de persoon met wie hij contact had gehad. Zij gaven aan dat die persoon niet werkzaam was voor het bedrijf. Het bedrijf wist meteen dat het om oplichting ging toen meneer de betreffende naam noemde. Er waren namelijk al meerdere meldingen over ontvangen. 'Sunset zei: "ja, jullie zijn de klos; dit zijn oplichters"'. Toen besefte meneer te zijn opgelicht.

Bij doorvragen gaf meneer aan dat de website mogelijk nep was. Meneer herinnert zich echter niet meer of deze er hetzelfde uitzag als de legitieme website. De advertentie waar meneer op reageerde, stond niet op de officiële Sunset-website; dat had meneer nadien gecontroleerd. Wat achteraf wel opviel, is dat het contact verliep via het e-mailadres 'info@sunsettjavea. Het officiële adres is echter 'info@sunsetjavea', zonder extra 't'. Meneer gaf aan misschien onoplettend te zijn geweest. Meneer gaf verder aan niet te hebben

getwijfeld over de echtheid van de advertentie en de betaling. Dit kwam ten eerste door positieve ervaringen via Airbnb, waarbij meneer ook voor langere tijd vakantiewoningen huurde. Meneer gaf daarbij aan dat investeerders in vakantiewoningen wel vaker in een ander land wonen. Meneer was dus niet achterdochtig, omdat hij dacht dat de eigenaar van dit betreffende huis in Italië woonde. Ook vond meneer het gezien zijn eerdere ervaringen niet vreemd om een maand huur plus borg te betalen. De lay-out van de website en de e-mails en de documentatie die meneer ontving leken betrouwbaar; een logo was aanwezig en het zag er officieel uit. Tot slot gaf meneer aan dat er keurig werd geantwoord op vragen die hij stelde, bijvoorbeeld over de aanwezigheid van wifi en aanwezig bedlinnen.

Casus 5: Oplichting met huurwoningen

In totaal zijn drie mensen geïnterviewd die waren opgelicht met de huur van een woning (kandidaten 3, 6 en 15). De casus van kandidaat 6 (hierna aangeduid met mevrouw) is hier uitgewerkt.

Mevrouw was voor onbepaalde tijd op zoek naar een huurwoning in een grote stad in Nederland. Via een zoektocht op Google kwam ze uit op de website 'Huurexpert.nl', waar ze maandelijks een bedrag moest betalen om te reageren op advertenties. Uiteindelijk stuitte ze op een advertentie die doorverwees naar 'Garantwonen.nl'. Via die website kwam mevrouw in contact met een verhuurder die aangaf dat ze in Zwitserland woonde. De communicatie verliep via de e-mail, in het Engels. De verhuurder wilde de betaling graag regelen via 'HomeAway Services' middels een derdengeldrekening en beloofde dat als alles was betaald, ze het contract en de sleutel naar mevrouw zou sturen, zodat ze het appartement kon bekijken. Mocht het appartement haar niet bevallen, dan kon ze de sleutel terugsturen en zou ze het betaalde bedrag via HomeAway Services terugkrijgen. Mevrouw maakte 1.200 euro over via overschrijving naar een Italiaans bankrekeningnummer. Het betalingsverzoek werd door de verhuurder via een link verstuurd. Dit bedrag omvatte de eerste maand huur, de borg en contractkosten. Na een week niks gehoord te hebben, nam mevrouw contact op met HomeAway Services. Zij vertelden haar dat het betreffende reserveringsnummer niet bestond en dat deze manier van oplichting helaas vaker was voorgekomen. De dader(s) had(den) waarschijnlijk hun website nagemaakt en gebruikgemaakt van hun betalingssysteem.

Na doorvragen gaf mevrouw aan geen enkele twijfel te hebben gehad. De betaling leek goed omdat dit via een reguliere, betrouwbare website ging. Mevrouw had navraag gedaan over HomeAway Services in haar sociale netwerk en meerdere mensen in haar omgeving hadden hier positieve ervaringen mee. Mevrouw had ook nog gecontroleerd op het

slotje in de browser. Mevrouw had tevens de verhuurder gecontroleerd voordat ze overging tot betaling. Dit deed ze op LinkedIn en Facebook. Daar vond ze dat de verhuurder in Zwitserland woonde, zoals ze ook via de e-mail had verteld. Ook deden de foto's voorkomen dat het om een betrouwbare persoon ging. Die foto's werden tevens gebruikt bij het account op HomeAway. Eveneens heeft mevrouw het betreffende appartement gegoogeld. Daaruit kon ze opmaken dat het huis bij verschillende makelaars in de verhuur heeft gestaan. Dit gaf ook een gevoel van vertrouwen. Dat het bankrekening Italiaans was, wekte bij mevrouw geen wantrouwen. Ze veronderstelde dat dit klopte omdat het om een derdengeldrekening ging, vergelijkbaar met Adyen. Mevrouw had ook het gevoel dat ze met vertrouwde websites te maken had (Huurexpert en Garantwonen), omdat ze per maand een bedrag moest betalen om te reageren op de advertenties. 'Huurexpert en Garantwonen stellen de adverteerders te verifiëren.'

Casus 6: Oplichting via sociale media

In totaal zijn twee benadeelden geïnterviewd voor de categorie 'sociale media' (kandidaten 16 en 20). De casus van kandidaat 20 (hierna aangeduid met meneer) is hier uitgewerkt.

Meneer wilde heel graag naar een uitverkocht concert. Meneer had Ticketswap overwogen, maar kon op die manier geen ticket vinden. Meneer lichtte toe dat ook op de Facebook-pagina van concerten soms kaarten worden aangeboden. Meneer heeft een 'posting' op de Facebook-pagina van het concert gedaan en is op die manier in contact gekomen met een persoon uit Engeland. Die deed voorkomen dat hij niet naar het concert kon gaan en dus een kaart over had. Het contact vond plaats via de chatfunctie van Facebook en geschiedde in het Engels. Tijdens dit contact is meneer met de verkoper overeengekomen om het bedrag over te maken naar zijn Engelse bankrekeningnummer en van die overboeking een screenshot te maken en door te sturen. Daarna leek het voor meneer dat de verkoper hem geblokkeerd heeft, want de verkoper was daarna verdwenen; hij was niet meer zichtbaar voor meneer en er kon dus ook niet meer mee worden gesproken. Daarna zag hij op de betreffende Facebook-pagina dat verschillende mensen elkaar aan het waarschuwen waren dat een aantal mensen de boel oplichtten. De naam van de persoon met wie meneer zaken had gedaan stond daar ook tussen. Hij was er dus vandoor met het geld. 'Het enige dat mij heeft gered is dat het geld niet meteen op zijn bankrekening stond, maar dat het nog ergens in de cloud hing bij de bank. Toen heb ik meteen de bank verwittigd en toen hebben zij het nog weten te blokkeren.'

Na doorvragen gaf meneer aan niet te hebben getwijfeld. 'Het leek allemaal heel authentiek.' Hoewel er weinig informatie bekend is van de verkoper, kwam hij in de communicatie heel relaxed over. Het was een simpel gesprekje, waaruit weinig was af te lezen. Hij zag een account met een naam en een foto. Deze had hij vluchtig bekeken en daar was weinig verdachts aan. Een andere reden om door te gaan met de aankoop was dat hij heel graag naar dit concert wilde. 'Het was een zwaar uitverkocht concert. Dan word je wel wat fanatieker, haha, en wanhopiger.' Meneer is eenmaal eerder opgelicht met de online aanschaf van concertkaartjes.

Casus 7: Oplichting via webshops

Van de categorie 'webshop' is met één benadeelde gesproken. Kandidaat 17 (hierna aangeduid met meneer) kwam via Facebook in contact met een Engelse webshop. Een van zijn connecties had deze shop 'geliket'. Op de betreffende website stonden tien aanbiedingen van een accugereedschapsset. Acht daarvan hadden een marktconforme prijs en twee aanbiedingen een prijs die 'te mooi was om waar te zijn'. Meneer bestelde een van de aanbiedingen met de lage prijs en betaalde via iDEAL. Het betreffende bedrag werd overgemaakt naar een Belgisch bankrekeningnummer. Na de aankoop ontving meneer 'goede nazorg'. Hij kreeg een bevestigingsmail dat de bestelling was geplaatst en ontving een Track&Trace-code. Twee weken na de besteldatum e-mailde meneer met de vraag of hij was opgelicht. Daarop ontving hij een nette reactie. Wel googelde hij daarna de webshop en het bankrekeningnummer en vond dat het bankrekeningnummer eerder frauduleus was misbruikt. Op dat moment wist meneer zeker dat hij was opgelicht.

Bij doorvragen gaf meneer aan dat hij zich bewust was van een mogelijk risicovolle aankoop. De keuze om door te gaan werd ook bewust gemaakt. In overleg met een vriend, die ook aangaf dat het op oplichting leek, werd dit beslist. Mogelijk kon het toch echt zijn, omdat het apparaat werd verkocht voor gebruik met 210 volt, 'waar niemand iets mee kan'. Omdat meneer en zijn vriend handig zijn, zouden ze dat zelf kunnen aanpassen, zodat het wel gebruikt zou kunnen worden. Samen kwamen ze tot de conclusie dat als het lukte ze 'een goede deal' hadden en als het niet lukte ze maximaal 100 euro kwijt waren. Bovendien leek de betreffende webshop plausibel, omdat Facebook-connecties deze hadden geliket en de webshop ook andere producten verkocht tegen marktconforme prijzen. Ook het feit dat via iDEAL betaald kon worden, maakte het vertrouwd. Achteraf bedacht meneer dat dit laatste eigenlijk 'schijnveiligheid' is.

Casus 8: Oplichting via gezocht-advertenties

Van de categorie 'gezocht' is eveneens met één benadeelde gesproken. Kandidaat 12 (hierna aangeduid met mevrouw) was op zoek naar vier tickets voor een evenement. Via Marktplaats plaatste ze daarvoor een oproep. Op dit verzoek werd veel gereageerd, zowel via de chatfunctie van Marktplaats als rechtstreeks op haar telefoon; ze had haar telefoonnummer in de advertentie gezet. Uiteindelijk is ze met een particuliere verkoper via de chatfunctie van Marktplaats verder in contact getreden. Deze vertelde haar dat hij zes kaarten beschikbaar had en uiteindelijk besloot mevrouw alle zes kaarten te kopen. Er werd een mooie prijs afgesproken. 'Eigenlijk een die te mooi is om waar te zijn. Daar hadden misschien die eerste alarmbelletjes al moeten rinkelen.' De verkoper kwam betrouwbaar over; het gesprek verliep netjes en hij beloofde de tickets direct te e-mailen. Toen kwam de verkoper aanzetten met een Pools rekeningnummer, wat mevrouw erg argwanend maakte. Daar heeft ze verschillende keren een opmerking over gemaakt. De verkoper gaf echter aan dat dit een zakelijk account van hem was. Mevrouw verifieerde dit verhaal bij een vriend van haar die bij een Nederlandse bank werkt. Die vriend antwoordde dat het verhaal mogelijk waar kon zijn, waardoor mevrouw het al iets meer vertrouwde.

Omdat ze nog niet helemaal zeker van haar zaak was, vroeg ze of het bedrag in twee keer overgemaakt kon worden. Hoewel ze dat in eerste instantie waren overeengekomen, kwam de verkoper daarop terug nadat hij het eerste bedrag had ontvangen. Hij beargumenteerde dat hij dit te risicovol vond; dat zij straks de tickets had, en hij geen geld. Mevrouw toonde daar begrip voor en heeft 'na lang heen en weer overleg' ook het andere deel overgemaakt via een bankoverschrijving. Om een extra garantie te geven gaf de verkoper een adres op in Friesland. Mevrouw controleerde via Google Earth of daar wel echt mensen woonden. 'Maar ja, dat kan iedereen zijn natuurlijk.' Een paar dagen nadat ze het bedrag had overgemaakt, liet de verkoper weten het bedrag nog niet te hebben ontvangen. Mevrouw dacht dat dit kon kloppen, omdat ze het bedrag net voor het weekend had overgemaakt en omdat het naar een buitenlands rekeningnummer ging. Vervolgens hoorde ze niets meer. Na drie dagen niets gehoord te hebben, dacht mevrouw dat er sprake was van oplichting. Zij had nog tegen de verkoper gezegd dat wanneer ze niets zou ontvangen, ze aangifte zou doen. Ze merkte echter dat de verkoper de berichten niet meer las, omdat er geen vinkjes meer verschenen bij de berichten die via de Marktplaats-app werden verstuurd.

Bij doorvragen naar opvallendheden, gaf mevrouw aan dat de manier van communiceren steeds mee kortaf was en dat de perioden tussen vraag en antwoord steeds langer werden. 'Maar ja, hij bleef in die zin wel contact houden. En je weet nooit de reden dat iemand later reageert. Misschien heeft hij wel een ongeluk gehad. Je weet niets van die persoon.' Verder viel haar weinig op. Er werd in goed Nederlands gecommuniceerd; geen gekke spelfouten of iets dergelijks. 'Misschien had je bij gebrekkig taalgebruik een onbetrouwbaarder gevoel gehad? Hij kwam over als een keurig, nette man die zes kaartjes over

had.' Omdat mevrouw zelf de oproep had geplaatst, kon ze het profiel van de verkoper niet controleren, bijvoorbeeld hoe lang hij al actief is op Marktplaats. Mevrouw heeft vooraf wel de naam van de verkoper gegoogeld en opgezocht via Facebook. Dat leverde niets op. Uiteindelijk gaf mevrouw aan dat ze gewoon heel graag die kaartjes wilde hebben en zich daardoor heeft laten leiden. 'Het was gewoon een hele mooie deal. Ik was te happig op die kaartjes.'

Casus 9: Oplichting waarbij hacken een rol speelt

In totaal hebben we drie mensen gesproken die waren opgelicht waarbij hacken een rol speelde (kandidaten 1, 4 en 19).[7] In één van de gevallen werd de benadeelde ook zelf gehackt, mogelijk door toedoen van het incident dat hij had meegemaakt (19).[8] De casus van kandidaat 19 (hierna aangeduid met meneer) is hier uitgewerkt.

Meneer was op zoek naar een specifieke geluidsbox en zag op Marktplaats een advertentie waarin deze goedkoop werd aangeboden omdat de verpakking stuk was. Meneer controleerde het betreffende bedrijf. Dit leek te kloppen, dus zou meneer overgaan tot aanschaf. Echter, toen hij daarvoor terugkeerde naar Marktplaats zag meneer een andere advertentie (van een ander bedrijf) waarin het apparaat voor tien euro minder werd aangeboden. Daarop besliste meneer om met die verkoper in contact te treden. Meneer maakte volgens afspraak het bedrag via een bankoverschrijving over, waarbij de verkoper beloofde het product meteen te versturen. De verkoper leek uit Nederland te komen en er werd ook in het Nederlands gecommuniceerd. De verkoper had aangegeven dat meneer de volgende dag een Track&Trace-code zou ontvangen. Die kreeg hij echter niet. Meneer vond dat vreemd en stuurde daarop een bericht. De verkoper gaf aan dat het wel goed zou komen. Daarna reageerde de verkoper nergens meer op. Toen stuurde meneer nog een keer een bericht met de vraag: 'Volgens mij ben ik opgelicht, of niet?' De verkoper antwoordde met: 'Je vraag zegt al genoeg toch?' Daarna zocht meneer het telefoonnummer op van de handelsonderneming en belde het nummer dat hij vond. Aan de andere kant van de lijn werd gereageerd met: 'Ik word helemaal gek gebeld. Ik bied van alles aan, maar ik bied het niet aan. Mijn account is gehackt.'

Na doorvragen gaf meneer aan geen argwaan te hebben gehad. De communicatie verliep goed en razendsnel en ook de advertentie zag er betrouwbaar uit. Het account van de verkoper had 98,9% betrouwbaarheid en er werd bij vermeld dat de verkoper altijd snel reageerde. 'Dat klopte natuurlijk wel voor degene van wie het account daadwerkelijk was.'

7 In hoeverre er daadwerkelijk sprake is van hacken en hoe die hack eruit heeft gezien is niet te verifiëren op basis van de aan ons verstrekte informatie door de interviewkandidaten.

8 Het kan natuurlijk ook berusten op toeval dat meneers account een week na het incident is overgenomen.

Achteraf had het Duitse bankrekeningnummer wel argwaan moeten wekken. 'Stom als ik ben heb ik geen controles gedaan; meteen het geld overgemaakt. Ik heb dat klakkeloos gedaan (…) gewoon met knippen en plakken. Later zag ik pas dat het een raar Duits nummer was.' Meneer gaf aan dat het niet uitvoeren van controles niet alleen vanuit gemakzucht kwam, maar ook door zijn enthousiasme, dat hij kreeg doordat zijn vrouw het na lange tijd goed vond om dit product aan te schaffen. Tevens gaf meneer aan het achteraf vreemd te vinden dat er werd gevraagd om een screenshot te sturen van de overboeking, zodat de verkoper het product kon opsturen.

4.4 Resumé crimescripts en betrokken partijen

Op basis van de dossieranalyse en reconstructie is inzichtelijk gemaakt hoe de crimescripts van internationale aankoopfraude eruitzien en welke partijen betrokken zijn in deze crimescripts. Gezien de veelheid aan informatie, volgt hier een beknopt overzicht van zowel de crimescripts als van de betrokken partijen in deze scripts.

Crimescripts
Een crimescript is een set elkaar opvolgende acties die een crimineel uitvoert of laat uitvoeren, ter realisatie van een delict. Elk script bestaat uit minimaal enkele basisstappen, nodig om het delict te kunnen plegen. Dan onderscheiden we nog aanvullende en extra stappen. 'Aanvullende stappen' zijn acties ter ondersteuning van de basisstappen, bijvoorbeeld om de kans op succes te vergroten. 'Extra stappen' zijn acties die de crimineel zet na het voltooien van het delict, bijvoorbeeld om opsporing te bemoeilijken.
Tabel 4.2 geeft een overzicht van basisstappen en extra stappen van de vier aangetroffen crimescripts. Aanvullende acties die fraudeurs uitvoeren, bijvoorbeeld om het vertrouwen van hun slachtoffers te winnen, staan samengevat in sectie 7.1.1. De stappen in tabel 4.2 vallen onder de 'scènes' *pre*-activiteiten, activiteit, en *post*-activiteiten (zie par. 3.2). Hierbuiten vallen dus stappen die vallen onder de scène 'voorbereiding', zoals wat fraudeurs doen om hun identiteit te verhullen. Daarop hebben we in dit onderzoek geen zicht gekregen.
De laatste basisstap is steeds 'de fraudeur incasseert het bedrag'. Dat kan rechtstreeks zijn of indirect. Het geld kan immers eerst worden gestort op een bankrekening van een geldezel, waarna de fraudeur het geld op andere wijze bemachtigt, al dan niet via verschillende tussenpersonen. De essentie blijft dat de fraudeur het bedrag incasseert.

Tabel 4.2: Overzicht van crimescripts

Crimescript 1: Advertentie plaatsen Basisstappen	*Crimescript 2: Opzetten valse webshop* Basisstappen
1. De fraudeur plaatst een advertentie op een online platform 2. Het slachtoffer reageert op de advertentie 3. Het slachtoffer maakt geld over 4. De fraudeur incasseert het bedrag Mogelijke extra stappen 5. De fraudeur verwijdert de advertentie 6. De fraudeur heft het verkopersaccount op	1. De fraudeur bouwt een webshop 2. De fraudeur regelt de randzaken voor het opzetten en adverteren van een webshop[1] 3. Het slachtoffer reageert op de advertentie 4. Het slachtoffer maakt geld over 5. De fraudeur incasseert het bedrag Mogelijke extra stap 6. De fraudeur ontmantelt de webshop
Crimescript 3: Misbruiken account Basisstappen	*Crimescript 4: Reageren zoekadvertentie* Basisstappen
1. De fraudeur misbruikt iemands naam[2] 2. De fraudeur zet een advertentie online op een online platform 3. Het slachtoffer reageert op de advertentie 4. Het slachtoffer maakt geld over 5. De fraudeur incasseert het bedrag Mogelijke extra stap 6. De fraudeur verwijdert de advertentie	1. Het slachtoffer plaatst een gezocht-advertentie op een online platform 2. De fraudeur reageert op de advertentie 3. Het slachtoffer maakt geld over 4. De fraudeur incasseert het bedrag Mogelijke extra stap 5. De fraudeur heft het kopersaccount op

1 Randzaken betreffen (a) het registreren van een domeinnaam, (b) het kopen of huren van hostingruimte, (c) het online plaatsen van de webshop, en (d) het adverteren voor de webshop.

2 De fraudeur (a) hackt of koopt een verkopers-account met een goede rating of (b) maakt een verkopersaccount aan op naam van een bedrijf.

Betrokken partijen

De meeste betrokken partijen hebben een faciliterende rol in het frauduleuze proces. Andere partijen hebben een passieve rol in de zin dat de bedrijfsnaam wordt misbruikt. Vanzelfsprekend spelen ook (potentiële) slachtoffers (klanten/consumenten) en fraudeurs (en hun handlangers) een belangrijke rol. Belangrijke (categorieën van) partijen die we hebben geïdentificeerd zijn:

- handel- en veilingsites, zoals Marktplaats, eBay, Speurders, AutoScout24 en Tweedehands (nodig voor het plaatsen van advertenties);
- sociale media, zoals Facebook en Instagram (plaatsen advertenties);
- legitieme webshops/websites, zoals Tweakers en Groupon (plaatsen advertenties);
- online diensten voor de verhuur van vakantiewoningen, zoals Airbnb en HomeAway Services (plaatsen advertenties);
- Internet Service Providers (hosting van valse webshops);
- organisaties voor registratie domeinnamen (registratie van valse webshops);
- banken (overschrijven van geld);
- (Collecting) Payment Service Providers (overschrijven van geld);
- transportpartijen (waarvan de naam wordt misbruikt in relatie tot het verschepen van goederen);
- escrow-diensten (waarvan de naam worden misbruikt in relatie tot betalingen);
- Kamer van Koophandel (KvK-nummers worden misbruikt/vervalst).

5. Handelingsstrategieën tegen internationale aankoopfraude

In dit hoofdstuk komen handelingsstrategieën aan bod die kansrijk lijken om aankoopfraude vanuit het buitenland tegen te houden dan wel te verstoren. Om het overzicht te bewaren zijn deze mogelijkheden ingedeeld volgens het raamwerk voor situationele criminaliteitspreventie (naar Cornish & Clarke, 2003; Hartel e.a., 2011).[1] In tabel 5.1 is dit raamwerk reeds ingevuld voor de context van aankoopfraude. We kijken in dit raamwerk naar situationele omstandigheden waarin aankoopfraude wordt gepleegd. Niet de oorzaken van deze vorm van criminaliteit staan centraal, maar de manieren waarop deze kan worden voorkomen.

De verstoringsstrategieën zijn gebaseerd op de interviews met experts en met benadeelden.[2,3] Het gaat hier niet alleen om innovatieve verstoringsmogelijkheden, maar ook om reeds bekende. Om inzichtelijk te maken vanuit welke hoedanigheid deze strategieën naar boven zijn gekomen, zijn deze genummerd. Wat betreft de expertinterviews is het nummer gekoppeld aan de betreffende organisatie waar de expert voor werkt. Het gaat hierbij om de volgende indeling: ING (E1); SIDN (E2); Fraudehelpdesk (E3); ECC (E4); City of London Police (E5); Guardia di Finanza (E6); ICS (E7); en EIB (E8). Tevens is de input vanuit de klankbordgroep verwerkt, aangeduid met (E9). Uitspraken van benadeelden zijn voorzien van de extra toevoeging 'B'.

1 Hartel e.a. (2011) hebben een nadere classificatie aangebracht aan de vijf categorieën voor situationele criminaliteitspreventie. De eerste drie classificeren zij als economische en de laatste twee als psychologische technieken.

2 De analyse van meldingen leverde wat betreft het in kaart brengen van verstoringsmogelijkheden niet veel op. In slechts tien van de 150 gevallen is beperkte informatie te vinden over het uitvoeren van controles vóór de betaling. In de meldingen werd door een vijfde van de benadeelden (19,3%) genoemd dat ze ná de betaling de persoon of het bedrijf hebben gecontroleerd.

3 Belangrijk om te vermelden is dat een aantal strategieën die tijdens de interviews zijn besproken soms door de onderzoekers zelf zijn ingebracht, zie bijlage IV. In hoeverre deze strategieën daadwerkelijk zijn ingebracht door de onderzoekers staat vermeld in de tekst.

Tabel 5.1: 25 technieken voor de preventie van online aankoopfraude vanuit het buitenland

Economische kosten en baten			Psychologische kosten en baten	
Increase the effort	**Increase the risks**	**Reduce the rewards**	**Reduce provocations**	**Remove excuses**
1. Harden targets: - *bewustzijn verhogen,* - *cyberhygiëne*	6. Extend guardianship: - *controles uitvoeren,* - *burgerwacht,* - *melding stimuleren*	11. Conceal targets: -	16. Reduce frustrations: -	21. Set rules: - *binnen platform communiceren,* - *verkoper controleren,* - *vertrouwd betalen*
2. Control access: - *tweefactor-authenticatie*	7. Natural surveillance: - *betrouwbare controles aanbieden*	12. Remove targets: - *melding bij opzeggen domeinnaam,* - *detecteren bedrijven zonder website*	17. Avoid disputes: - *aankoop via officiële partijen,* - *informatie rechten particulier versus consument*	22. Post instructions: - *waarschuwing en voorlichting binnen online platform*
3. Screen exits: - *vertrouwd betalen,* - *geld blokkeren*	8. Reduce anonymity: *-identificatie/ verificatie (ver) kopers,* - *controlebericht bij inloggen vanaf ander IP-adres* *-weren VPN-gebruik*	13. Identify property: - *identificatie legitieme webshops/verkopers*	18. Reduce arousal: -	23. Alert conscience: - *actief waarschuwen bij geld overmaken naar buitenland,* - *IBAN-Naam Check (EU)*
4. Deflect offenders: - *identificatie en verificatie,* - *whitelisting registrars*	9. Place managers: - *vierogenprincipe*	14. Disrupt markets: - *verwijderen frauduleuze accounts, advertenties en webshops (NTD)*	19. Neutralize peer pressure: - *voorlichting (potentiële) geldezels*	24. Assist compliance: - *plug-in controle-systemen platform,* - *meldknop fraude op platform*
5. Control facilitators: - *gebruik blacklists*	10. Formal surveillance: - *detectie,* - *Europese PPS,* - *Europees meldpunt*	15. Deny benefits: - *efficiëntere internationale samenwerking tussen banken*	20. Discourage imitation: - *pakkans verhogen*	25. Control disinhibitors: - *campagnes op (basis)scholen*

In tabel 5.1 zijn de vijf strategieën en vijfentwintig technieken van situationele misdaadpreventie van Cornish en Clarke (2003) toegepast op online aankoopfraude vanuit het buitenland. Per strategie worden de geïdentificeerde verstoringsmaatregelen beschreven (par. 5.1-5.5). Bij het bespreken van verstoringsmogelijkheden wordt onderkend dat de verschillende verstoringsmogelijkheden zowel voor- als nadelen hebben; wat van invloed is op de effectiviteit en haalbaarheid ervan. Deze beperkingen worden hier besproken. We hebben eveneens – waar mogelijk – aandacht voor welke partijen een rol kunnen of zouden moeten spelen in relatie tot de verstoringsmogelijkheden.

5.1 Strategie 1: Inspanningen vergroten om criminaliteit te plegen

De eerste strategie 'increase the effort' is het moeilijker maken voor criminelen om criminaliteit te plegen. Binnen deze strategie hebben Cornish en Clarke (2003) vijf

technieken ontwikkeld die de inspanningen vergroten om criminaliteit te plegen (1-5). Deze zijn uitgewerkt voor de context van aankoopfraude.

Techniek 1: Harden targets. De eerste techniek betreft het versterken van doelwitten (i.e. digitale weerbaarheid). Het **bewustzijn vergroten** van aankoopfraude bij consumenten is een verstoringsmogelijkheid die door de meeste experts spontaan werd genoemd, bijvoorbeeld door middel van waarschuwingen en voorlichtingscampagnes (E1, E3, E4, E5, E6, E7, E8, E9).[4] Dergelijke awareness-campagnes kunnen in samenwerking met partners worden opgepakt, bijvoorbeeld met banken, het LMIO, het OM en ministeries. De veronderstelling is dat wanneer meerdere partners dezelfde punten onderschrijven en met dezelfde boodschap naar buiten treden, de voorlichting effectiever is. Potentiële gevaren schuilen in gebrekkige coördinatie en de eigen belangen van organisaties die mogelijk niet geheel overeenkomen (E9). Waarschuwingen kunnen tevens worden geplaatst op de websites en worden genoemd in andere communicatie-uitingen van de betrokken actoren, bijvoorbeeld op sociale media.
Volgens een van de experts is de effectiviteit van campagnes waarschijnlijk laag en is dat dan ook niet dé oplossing: 'Al geruime tijd worden bewustzijnscampagnes gevoerd, maar fraude en oplichting vinden nog steeds plaats' (E1). Ook andere experts zien beperkingen in de effectiviteit ervan (E3, E4, E5, E7). Experts van de City of London Police gaven als voorbeeld dat zij waarschuwen voor veelvoorkomende trucs die worden gebruikt door criminelen bij de verkoop van auto's.[5] Toch trappen veel mensen erin, omdat ze een goede deal denken te hebben en het advies pas zien wanneer het te laat is. Experts van het ECC gaven aan dat zij wel eens tips vermelden in een nieuwsbericht op hun website om online zo veilig mogelijk aankopen te kunnen doen, maar verwachten daarbij niet dat het grote aantallen mensen zal bereiken. Experts van de EIB en het ICS onderstrepen het geven van specifiek advies. Daarbij kan gedacht worden aan het zelf intypen van een URL in de adresbalk. Volgens experts van de EIB is het belangrijk om aan mensen duidelijk te maken dat iedereen vatbaar is voor online fraude; nu denkt men 'dat zij daar nooit in zouden trappen'.[6] Daarnaast werd de AVG genoemd als beperkende factor wat betreft het geven van voorlichting, zie tekstkader.[7]

4 Denk bijvoorbeeld aan de adviezen van ConsuWijzer en de ACM-campagne over nepshops op sociale media rondom 'Black Friday'. Bron: ACM (2018). 'ACM waarschuwt met Nepshop voor aankopen via social media'. Via: https://www.acm.nl/nl/publicaties/acm-waarschuwt-met-nepshop-voor-aankopen-social-media.

5 Het gaat hierbij om het vermelden dat de auto in bezit is van een vrouw die tevens eerste eigenaar is. In deze 'truc' wordt de gemeenschappelijke perceptie misbruikt dat een vrouw een meer voorzichtige bestuurder is en de auto beter zou laten onderhouden, waardoor de deal aantrekkelijker klinkt. Wanneer kopers contact opnemen over deze auto, vertellen de fraudeurs dat de auto al wordt bekeken en mogelijk wordt verkocht voordat het slachtoffer de kans heeft om het te bekijken. Slachtoffers worden vervolgens gevraagd om een aanbetaling te doen om zodoende te kunnen garanderen dat zij de auto kunnen kopen.

6 Ter illustratie, de EIB heeft een webshop nagebootst en consumenten producten laten kopen. Op het moment van betaling hebben ze hen een boodschap gegeven met een waarschuwing voor online oplichting. Dat heeft volgens hen meer effect gehad dan de algemene campagnes.

7 AVG staat voor Algemene Verordening Gegevensbescherming. Zie bijvoorbeeld: https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/avg-europese-privacywetgeving/algemene-informatie-avg.

Wat betreft het verstoren van aankoopfraude zet de Fraudehelpdesk vooral in op waarschuwen, bewustwording. De Fraudehelpdesk was voorheen meer actief op dit gebied, maar momenteel ligt dat lastiger. Expliciet waarschuwen voor valse webshops, door namen te noemen, is moeizamer geworden naar aanleiding van de AVG. Daarnaast kan waarschuwen op basis van een melding een delicate aangelegenheid zijn, bijvoorbeeld als het gaat om bestaande bedrijven. Het kan zijn dat bedrijven, of eventueel de leveranciers van bedrijven, in zwaar weer zitten en niet op tijd leveren, in plaats van dat ze frauduleus handelen. Ook bij een wisseling van bestuurder, die de zaken anders wil aanpakken, kan het zijn dat er vertraging in de levering ontstaat. Dan kun je niet bij de eerste melding direct actie ondernemen en zeggen dat het niet te vertrouwen is. (E3)
Daarnaast is publiek-private samenwerking moeilijk vanwege de AVG. De AVG belet de Fraudehelpdesk bijvoorbeeld om gegevens door te geven aan de politie en samen met hen op te trekken. Informatie delen is volgens hen nuttig, omdat een melding die bij de Fraudehelpdesk wordt gedaan, mogelijk nog niet bij de politie terecht is gekomen. Er hoeft bijvoorbeeld nog geen geld kwijt te zijn, wil iemand melding doen bij de Fraudehelpdesk. Denk aan iemand die kleding van een bepaald merk wil kopen en een potentieel frauduleuze website signaleert. Pas als er echt geld kwijt is, gaat men over tot eventueel doen van aangifte bij de politie. De politie heeft op haar website een lijst met malafide handelspraktijken; de check verkopergegevens. Deze lijst is nu alleen gebaseerd op politiedata uit aangiften. Dat is volgens de experts van de Fraudehelpdesk een gemis, omdat zij naar eigen zeggen vaak eerder informatie krijgen dan de politie.
Ook experts van ICS zien dat mogelijkheden om fraude te bestrijden worden beperkt. Zij stellen dat idealiter privacywetgeving erop is gericht dat gegevens niet worden gedeeld, mits er aan een aantal voorwaarden is voldaan. Fraudebestrijding zou onder die voorwaarden moeten vallen. Dit kan bijvoorbeeld het gemak waarmee criminelen nu kunnen 'bankhoppen' lastiger maken.

Een belangrijke opmerking wanneer het gaat om voorlichting is dat de betreffende informatie op de juiste plek en tijd getoond moet worden aan de juiste mensen (E5, E8, E9). Als voorbeeld werd genoemd om een boodschap te tonen wanneer men overweegt een transactie te doen. Een concrete uitwerking hiervan is de site Tweedehands.be die actief waarschuwt als klanten tickets (een risicovol product) willen kopen (E8). Een andere optie is dat Google, eventueel in samenwerking met overheidsdiensten, dergelijke waarschuwende informatie plaatst tussen de advertenties die zij tonen, bijvoorbeeld wanneer wordt gezocht met specifieke zoektermen (E8). Ook hierbij gelden beperkingen. Als het gaat om online aankopen, maar ook om betalingsverkeer, is er een belang om het zo gemakkelijk mogelijk te houden; als het hinderlijk is klikken mensen aanvullende c.q. waarschuwende informatie gelijk weg (E1, E9). De City of London Police stuurt bijvoorbeeld 'goed getimede' alerts uit waarbij gebruik wordt gemaakt van een 'fraudekalender'. Met de fraudekalender kan men voorspellen wanneer bepaalde soorten fraude waar-

schijnlijker zijn en kan daarmee worden vooruitgelopen op potentiële trends. Hierbij kan gedacht worden aan alerts tussen juli en september wanneer studenten op zoek zijn naar een kamer of in de decembermaanden rond 'Black Friday', 'Cyber Monday' en kerst. Dergelijke alerts worden kort voor en tijdens deze evenementen verstuurd. Daarbij gaven de experts aan dat ze lang genoeg moeten duren om mensen te bereiken, maar kort genoeg zodat mensen niet de interesse verliezen.
Ook kan bij deze eerste techniek om aankoopfraude te verstoren worden gedacht aan de verantwoordelijkheid van consumenten zelf (E4, E9). Vanuit het ECC werd hierover het volgende gezegd: 'Als je mensen achteraf aanspreekt of het niet te mooi was om waar te zijn hoor je ook: "Tja, het zag er zo goed uit." Ja, natuurlijk ligt er bij hen ook een verantwoordelijkheid, maar dat neemt niet weg dat zo'n online platform daar ook iets tegen zou kunnen doen. Het is niets nieuws.' Bij online aankopen via een webshop geldt hetzelfde. Mensen moeten worden opgevoed welke aspecten van een aankoop verdacht kunnen zijn. De vergelijking wordt getrokken met een louche-uitziende winkel in een donker steegje waarvoor je ook bedachtzaam moet zijn. Eigen verantwoordelijkheid werd eveneens benoemd in de slachtofferinterviews, zie onderstaand tekstkader.

Twaalf benadeelden gaven expliciet aan dat een belangrijke of de belangrijkste verantwoordelijkheid om slachtofferschap te voorkomen bij henzelf ligt. Eén gaf aan: 'Ik had verstandiger moeten zijn' (B7). Een andere benadeelde gaf aan: 'Natuurlijk is men verantwoordelijk voor zijn eigen daden; niet dat ze slachtoffer worden, maar wel dat ze zelf opletten' (B9). Twee benadeelden gaven aan dat bescherming tegen aankoopfraude wel lastig is, bijvoorbeeld omdat oplichters zo gehaaid te werk gaan. 'Wanneer is iets nep?' (B10). Een ander gaf aan dat het moeilijk is om goed op te letten in een snel veranderende wereld. 'Kun je wel van mensen verwachten dat ze goed opletten? En wat is dat dan?' (B9).

Basis cyberhygiëne is een vereiste voor veilig online aankopen. We zagen in een aantal gevallen dat hacken als basisdelict werd gebruikt voor aankoopfraude. Hoewel deze maatregel niet expliciet is benoemd in de interviews, is het voor zowel online kopers als verkopers belangrijk om de basisveiligheid op orde te hebben. Hierbij kan worden gedacht aan up-to-date software en een goed wachtwoordbeleid.

Techniek 2: Control access. De tweede techniek betreft toegangscontrole. Hierbij lijkt één mogelijkheid van toepassing die kan worden toegepast door online platformen, namelijk het aanbieden van **tweefactor-authenticatie** (2FA). Dit is een authenticatiemethode waarbij twee stappen succesvol doorlopen moeten worden om toegang te krijgen. Een voorbeeld van 2FA is het invullen van een wachtwoord op een website waarop een corresponderende code via sms of e-mail wordt toegezonden. Slechts bij

het invullen van het wachtwoord én een aanvullende code wordt toegang gegeven tot het account. Deze verificatiemethode maakt het moeilijker voor fraudeurs om misbruik te maken van accounts (E9).[8] Een mogelijk probleem is dat fraudeurs deze beveiligingsmaatregel omzeilen, bijvoorbeeld door middel van een simwissel. Hierop kan worden geanticipeerd door ook telefoonmaatschappijen mee te nemen in de ontwikkeling van preventiemaatregelen.

Techniek 3: Screen exits. De derde techniek vertalen wij voor dit onderzoek als het 'cashen' van het geld dat slachtoffers hebben overgemaakt. Door benadeelden werden suggesties gedaan voor verstoringsmogelijkheden rondom de manier van betalen. Negen benadeelden gaven aan in de toekomst wellicht van betaalmogelijkheden gebruik te maken waarbij men voor een groot deel verzekerd is als consument of men meer vertrouwen geniet, zoals creditcard, PayPal of betaling via een escrow-dienst. Bij gebruikmaking van een escrow-dienst kan een koper het afgesproken bedrag overmaken naar een derdengeldrekening, die het tegoed beheert totdat het product of de dienst ontvangen is; vervolgens wordt het bedrag doorgestuurd naar de verkoper. Een voorbeeld hiervan is betalen volgens het 'gelijk oversteken'-principe van Marktplaats. Door gebruik te maken van deze vertrouwde manier van betalen wordt geen geld overgemaakt zolang geen product of dienst geleverd wordt, wat het cashen van geld moeilijker maakt voor fraudeurs. **Vertrouwd betalen** kwam ook in de expertinterviews terug als belangrijke maatregel om fraude te verstoren (E5, E6, E7, E8, E9). In geval van aankopen via creditcard helpt het mee dat VISA en Mastercard hun 'merchants' screenen, wat moet leiden tot meer veiligheid (E7). Een kritische noot die hierbij werd genoemd is dat klanten door deze manier van bescherming mogelijk risicovoller gedrag gaan vertonen (E5).
In de klankbordgroep werd erover gediscussieerd in hoeverre het gebruik van een escrow-dienst verplicht gesteld kan worden, omdat vrijblijvend gebruik ervan waarschijnlijk niet effectief is. 'Het helpt een goedgelovig persoon niet die wordt verleid om er geen gebruik van te maken. (…) Dat roept de vraag op in hoeverre mensen daarop zitten te wachten; wil de consument deze bemoeienis? (…) Er is ook nog zoiets als vrijheid van handelen' (E9). Dit heeft mogelijk ook betrekking op de zorgplicht van betrokken partijen. Deze kan lager komen te liggen wanneer dergelijke maatregelen worden bestempeld als ongewenst of bemoeienis. Een mogelijke oplossing die kan werken is het verplicht gebruik te laten maken van een interne derdengeldrekening bij aankopen boven een X-bedrag of voor risicovolle producten, zoals tickets en auto's. Het dwingend opleggen van een bepaalde handelsmethode en de effecten daarvan behoeft echter nader onderzoek. Gebruik van een externe escrow-dienst wordt afgeraden, omdat daarvan de naam misbruikt kan worden. Een potentieel gevaar schuilt echter ook in het gebruik van interne escrow-diensten, omdat deze eenvoudig gespooft kunnen worden (middels *phishing kits*).

8 Sinds afgelopen zomer brengt Marktplaats de mogelijkheid voor tweefactor-verificatie onder de aandacht. Bron: Marktplaats.nl (z.d.). *Bescherm je account met de SMS-beveiligingscontrole*. Via: https://help.marktplaats.nl/help/account_mijn_marktplaats/marktplaats_nl/i/bescherm-je-account-met-de-sms-beveiligingscontrole.

Daarnaast is nog een tweede maatregel geïdentificeerd. In 2019 wordt overgestapt naar een interbancaire infrastructuur die 'instant payments' mogelijk moet maken in de EU. Deze ontwikkeling maakt detectie moeilijker. Hoewel de snelheid van geld overmaken mogelijk niet vertraagd kan worden, gezien deze ontwikkeling, zou een verstoringsmogelijkheid kunnen zijn om het **geld tijdelijk** te **blokkeren** voor opname (E9). Het geld staat dan wel meteen bijgeschreven, maar is bijvoorbeeld voor een periode van drie of vijf dagen niet opneembaar. Dit zou als (betaalde) dienst moeten worden aangeboden, omdat het anders de ontwikkeling in de kern aantast. Met deze dienst wordt aan banken meer tijd verschaft om eventuele frauduleuze overboekingen terug te halen. De kanttekening die hierbij werd genoemd is op welke titel een bank het geld moet terughalen, omdat dergelijke betalingen nu onherroepelijk zijn, zie ook tekstkader.

Vanuit het perspectief van banken is er in principe alleen een rol weggelegd in geval van fraude, omdat de bank dan meestal ook zelf verlies lijdt (E1). In geval van oplichting, zoals de bank aankoopfraude interpreteert, is die rol van de bank minder aanwezig, omdat het slachtoffer zelf het geld heeft overgemaakt. In dat geval ondervindt de bank geen schade. Bovendien kan een bank frauduleus geld in principe niet terugboeken.

Bij oplichting heeft de klant zelf het bedrag overgemaakt en kan er sprake zijn van een geschil tussen de partijen. Een transactie is in principe onherroepelijk en de bank mag niet ingrijpen in dit proces. Zelfs als er meldingen van het LMIO binnen zijn gekomen, mag er vaak geen geld worden teruggestort. Dit is wel mogelijk met een vrijwaring, maar daar moeten juridische stappen voor ondernomen worden en 'dat houdt juridisch ook niet altijd stand'. Hoe kan een bank immers vaststellen dat een product niet is geleverd, en al helemaal uit het buitenland?

Indien geld van een Nederlandse rekening naar het buitenland is overgemaakt kunnen banken een zogenaamd SWIFT-bericht sturen.[9] *Het succes van een SWIFT-bericht is afhankelijk van (a) de tijd (periode tussen de melding en de overboeking) en (b) het land (of het land medewerking wil geven). Rechtstreeks contact tussen de banken is lastiger dan het lijkt, door diverse wettelijke regels inzake privacy. In principe wordt alleen het SWIFT-bericht gebruikt in de communicatie met buitenlandse banken.*

Ook opsporing is moeilijk vanwege buitenlandse opsporingsverzoeken en privacywetgeving. Via het IRC (Internationaal Rechtshulp Centrum) kan een buitenlandse opsporingsdienst wel een EOB (Europees opsporingsbevel) indienen en op die manier gegevens vorderen bij een buitenlandse bank. Dergelijke verzoeken vertragen de opsporing, en dat is weer positief voor de daders.[10]

9 Dit is voor banken het enige officiële kanaal waarmee zij een buitenlandse bank kunnen verzoeken een bedrag te bevriezen en eventueel terug te boeken.

10 Er is nieuwe EU-wetgeving voorgesteld die het mogelijk maakt om in strafonderzoeken digitale informatie in een ander EU-land op te vragen zonder tussenkomst van justitie. Bron: NRC (2018). *Nederland ligt dwars bij EU-wet over criminaliteit*. Via: https://www.nrc.nl/nieuws/2018/12/04/eu-justitie-wordt-politiek-wapen-a3051178.

Techniek 4: Deflect offenders. De vierde techniek kan worden vertaald als het afbuigen van daders. In de huidige tijdsgeest gaan zaken steeds sneller; zie ook de 'instant payments'-ontwikkeling hiervoor. Snelheid staat ook hoog in het vaandel bij financiële instellingen wanneer het gaat om het openen van bankrekeningen. Dit kan gemakkelijk online en soms met 'afgeleide identificatie'.[11] Middels afgeleide identificatie kan iemand met een bankrekeningnummer ongeveer negen andere rekeningnummers openen. Een expert noemt afgeleide identificatie als faciliterende factor voor fraude (E1). Het zou beter zijn (lees: om frauduleus gebruik van bankrekeningen minder makkelijk te maken) wanneer men daarvoor met een identiteitsbewijs op het bankkantoor moet langskomen, zie tekstkader.

'Het openen van een bankrekening kan tegenwoordig ook met een foto van een identificatiebewijs of een foto van het gezicht. Dit is dus makkelijk voor een fraudeur om rekeningnummers te gebruiken en zo de interbancaire blacklist te omzeilen. In een ideale wereld zou iedereen naar het bankkantoor moeten komen om zich te legitimeren, maar dat is niet de situatie. Steeds meer banken bieden deze mogelijkheid aan en daar gaat de bankwereld steeds meer naartoe. Alle handelingen moeten zo veel mogelijk online kunnen.' (E1)

Betere **identificatie en verificatie** aan de voorkant lijkt dus een effectieve, maar mogelijk lastig haalbare verstoringsmogelijkheid. Een soortgelijke trend is waarneembaar bij het aanmaken van domeinen, waarbij betere registratie en controle daarvan kan helpen frauduleus handelende webshops aan te pakken. Wanneer we aankoopfraude specifiek betrekken op valse webshops kan een belangrijke verstoringsmaatregel zijn dat registrars de identiteit van de houder van domeinnamen (beter) gaan controleren (E2, E5, E8).[12] Dit zijn de registrars voor .nl-domeinnamen overigens wettelijk al verplicht, omdat het in de algemene voorwaarden van het SIDN staat.

Het manueel controleren van alle houders is niet haalbaar; tijdrovend en arbeidsintensief. Vroeger moesten de domeinhouders zich wel identificeren door bijvoorbeeld een KvK-uittreksel op te sturen, maar daar is van afgestapt. Nu wil men zo snel mogelijk een domeinnaam registreren. Daarom is het ook moeilijk om deze vorm van verificatie weer in te

11 Afgeleide identificatie is het valideren van iemands identiteit door middel van een bankoverschrijving van minimaal 1 eurocent van een bankrekeningnummer met dezelfde tenaamstelling als de gegeven identiteit.

12 Een registrar is een bedrijf dat domeinnaamdiensten aanbiedt en rechtstreeks toegang heeft tot het registratiesysteem van SIDN. Voorbeelden van registrars zijn internetservice-, hosting- of accessproviders, maar ook webdesign-, merken- en reclamebureaus. Zie: https://www.sidn.nl/a/nl-domeinnaam/registrar-zoeken.

voeren. Daar komt bij dat er waarschijnlijk registrars (extensies) zijn die de identiteit niet zullen controleren en dat daders naar deze registrars toe zullen gaan of dat daders naar een ander domein dan .nl gaan. Een e-identificatie (zoals DigiD) zou meer haalbaar zijn. Idealiter worden wereldwijd alle domeinhouders gecontroleerd middels e-identificatie, maar dat is lastig omdat elk land andere wetgeving heeft. Alleen in gezamenlijk overleg is het verplichten van registrars tot controle op identiteit met e-identificatie haalbaar. (E2) Ook hier spelen zaken die het kunnen bemoeilijken om effectieve controles uit te voeren. In sommige phishing-zaken zorgen fraudeurs er namelijk voor dat ze met een transactie van het rekeningnummer van hun slachtoffer een nieuwe website kunnen hosten. De website lijkt vervolgens legitiem en zo kunnen fraudeurs verder gaan met mensen oplichten (E1). Mogelijk kan gebruik worden gemaakt van ***whitelisting*** *voor* ***registrars*** *(een soort keurmerk) die wel (uitgebreide) controles doen naar de identiteit van domeinnaamhouders (E6, E9).*

Techniek 5: Control facilitators. De vijfde techniek behelst controle door facilitators. Hoewel bij techniek 3 werd gesteld dat banken een beperkte rol spelen, omdat slachtoffer zelf het geld overmaken, is er wel een mogelijke rol weggelegd wanneer de begunstigde en/of het slachtoffer klant is van de betreffende bank. Een maatregel van banken tegen potentieel begunstigden is het blokkeren van hun bankrekening (E1, E8)[13] en een vooraankondiging sturen dat de bank voornemens is om de relatie op te zeggen en de potentieel begunstigde 'IVR (intern verwijzingsregister) te plaatsen' (E1).[14] Hoewel ernaar wordt gekeken om aankoopfraude in de toekomst mogelijk onder EVR (extern verwijzingsregister) te scharen, bijvoorbeeld om bankhoppen te voorkomen, is een beperking dat het alleen om Nederlandse bankrekeningnummers gaat.[15] Aankoopfraude 'vanuit het buitenland' valt daar dan buiten. EVR plaatsen is overigens niet waterdicht, omdat deze daders wel bankrekeningen kunnen openen bij banken die niet zijn aangesloten bij de Nederlandse Vereniging van Banken (NVB).
Nederlandse banken hanteren een **blacklist** voor hun detectiesystemen.[16] In een blacklist zijn (binnen- en buitenlandse) rekeningnummers opgenomen die eerder frauduleus zijn gebruikt en deze wordt eveneens gevoed met signalen vanuit het Electronic

13 Niet alleen bankrekeningnummers kunnen worden geblokkeerd, ook het blokkeren van telefoonnummers die in verband worden gebracht met fraude kan een effectieve verstoringsmogelijkheid zijn (E8).
14 Bij aankoopfraude wordt enkel IVR geplaatst. Indien een begunstigde IVR geplaatst wordt, dan mag hij/zij acht jaar lang niet meer bankieren bij de ING (vier jaar indien de begunstigde minderjarig is).
15 Als een begunstigde EVR geplaatst wordt, dan mag hij/zij acht jaar niet meer bankieren bij alle banken die aangesloten zijn bij de NVB. De begunstigde mag dan enkel een convenantenrekening openen bij de bank die hem/haar EVR heeft geplaatst. Een convenantenrekening is een bankrekening met beperkte mogelijkheden en extra toezicht. Of dit het gewenste effect heeft, behoeft echter nader onderzoek.
16 Een blacklist van valse webshops kan ook gehanteerd worden. We bespreken bij techniek 13 echter een whitelist van legitieme webshops, waardoor we hier niet verder op ingaan.

Crime Task Force (ECTF).[17] Een verstoringsmogelijkheid is het herkennen van de transactie in de detectiesystemen. Dat is wel afhankelijk van het bedrag, de frequentie van het crimescript en of het binnen de regels van detectie opvalt.[18] Na detectie van fraude kan het betreffende IBAN op de blacklist. Dit betekent dus dat het minimaal één keer mis is gegaan. Zodra geld wordt overgemaakt naar een rekeningnummer (nationaal of internationaal) dat op de blacklist voorkomt, wordt de transactie automatisch tegengehouden.[19] Hoewel een bankrekening hiervoor misbruikt moet zijn, en het fraude dus niet op voorhand verstoort, kan het wel verder misbruik tegengaan. Deze blacklist wordt overigens niet gedeeld met andere banken.
Een interbancaire blacklist voor potentiële en/of bevestigde frauduleuze rekeningnummers kan een sterkere verstoringsmogelijkheid zijn. Echter, zowel de haalbaarheid als de effectiviteit ervan zijn mogelijk laag volgens een van de experts (E1). De haalbaarheid is vermoedelijk laag omdat gegevens delen tussen banken nationaal en internationaal moeilijk is. Elk land is gebonden aan eigen privacywetgeving en dit maakt internationale uitwisseling van frauduleuze rekeningnummers (of andere persoonsgegevens) moeilijk. Men kan wel een buitenlandse bank notificeren van frauduleuze activiteit op een buitenlands rekeningnummer, maar dan is het aan de buitenlandse bank om daar actie op te ondernemen. De effectiviteit is vermoedelijk ook laag, omdat daders door kunnen gaan met oplichting als ze een ander rekeningnummer gebruiken; een gedeelde beperking door experts van de EIB.[20]

5.2 Strategie 2: Risico's vergroten om criminaliteit te plegen

De tweede strategie 'increase the risks' is het vergroten van het risico om criminaliteit te plegen. Binnen deze strategie hebben Cornish en Clarke (2003) vijf technieken ontwikkeld die dit risico kunnen vergroten (6-10). Deze zijn uitgewerkt voor de context van aankoopfraude.

Techniek 6: Extend guardianship. De zesde maatregel is het uitbreiden van beveiligingsmaatregelen en/of bewaking door anderen. Een maatregel die verstorend werkt is wan-

17 In het ECTF werken banken en politie samen om internetcriminaliteit aan te pakken.
18 In de detectiesystemen wordt niet alleen gekeken naar de hoogte van het bedrag. Ook het zogenoemde 'smurfen' wordt meegewogen. Dit zijn veel transacties van lage bedragen die als doel hebben om niet op te vallen in de detectiesystemen.
19 Blacklisten is niet altijd mogelijk. Als de betaling via een Payment Service Provider (PSP) plaatsvindt, dan ziet de bank niet rechtstreeks de transactie en is blacklisten dus niet mogelijk. Een PSP zou hier wellicht controles op kunnen uitvoeren en zelf frauduleuze rekeningnummers kunnen blacklisten. Opnieuw is deze maatregel achteraf en moeten eerst meerdere slachtoffers gemaakt worden voordat het rekeningnummer geblacklist wordt. Als de transacties zichtbaar zijn voor EquensWorldline (zie: https://equensworldline.com/), heeft deze partij misschien een mogelijkheid om te verstoren.
20 Er werd doorgevraagd over mogelijkheden tot blacklisten op basis van NAW-gegevens in plaats van een enkel rekeningnummer. Op deze wijze worden banken ook gewaarschuwd op basis van de persoon zelf en kan het openen van meerdere bankrekeningen verstoord worden. Volgens de expert van de ING is dat echter niet mogelijk. Dan gaat het bijna om EVR, waarvoor het vereist is dat er aangifte is gedaan. Bij een melding van het LMIO is dit vrij zeker, maar begunstigden van aankoopfraude worden zoals eerder aangegeven voorlopig alleen IVR geplaatst.

neer gebruikers vooraf aan een aankoop meer **controles uitvoeren** (E6, E7, E8, E9). Dit werd ook onderkend door de benadeelden, die aangaven dat controles moeten worden gedaan op de verkoper, het product en de betreffende website. Experts gaven aanvullende tips om te controleren naar welk land geld wordt overgeboekt (E6) en om naar beoordelingen te kijken voordat wordt overgegaan tot een transactie (E6, E7). 'Ook wanneer er geen reviews worden gegeven moet dit voor vraagtekens zorgen bij klanten' (E7). Een specifiek voorbeeld is de 'handelservaringen' van Marktplaats. Hiermee kunnen kopers en verkopers reviews geven aan elkaar waardoor zij meer inzicht krijgen in de persoon met wie zij handelen (E9). Er lijkt met name veel te winnen wanneer controles worden gedaan c.q. men erop wordt gewezen dit te doen bij de aanschaf van risicovolle producten. In het tekstkader zijn enkele voorbeelden beschreven wat voor controles men kan doen en wat deze controles kunnen opleveren.

Een verbetermogelijkheid die werd gesuggereerd door twee benadeelden en een expert (E6) is om vooraf de website (beter) te controleren. In één geval bestond de website nog geen maand en was die in een vreemd land gehost. 'Die simpele checks hadden het [incident] kunnen voorkomen' (B10). Ook de experts van de EIB gaven aan dat het belangrijk is voor klanten om dergelijke checks uit te voeren. In het andere geval hadden Google-resultaten kunnen laten zien dat de website onbetrouwbaar was of had controle van het KvK-nummer uitkomst kunnen bieden. Een van de benadeelden opperde dat Google misschien een rol kan spelen in het voorkomen van fraude; een week na de oplichting bezocht mevrouw de website opnieuw en Google gaf toen aan dat het een onveilig domein is. 'Google heeft dit kunnen opsporen, dus het zou mooi zijn als ze dit eerder kunnen doen' (B6). In overeenstemming met deze benadeelde gaven experts van de EIB aan dat Google een grotere rol kan spelen in het weren van mogelijk valse domeinnamen in de zoekresultaten. 'Google weet namelijk zelf ook het verschil tussen hostingbedrijven die benaderbaar zijn of vooral anonieme domeinhouders hebben.'

Een expert gaf aan dat in Italië kopers contact kunnen opnemen met de Guardia di Finanza op het moment dat zij twijfelen of een aanbetaalde auto daadwerkelijk aan een grens staat (E6). Hiermee is de initiële betaling niet tegengehouden, maar het voorkomt wel dat verdere betalingen worden verricht.

Andere verbetermogelijkheden die door benadeelden werden genoemd zijn het kijken naar beoordelingen of reviews van de verkoper (n = 7; hoewel het kan gaan om een gehackt account), het rekeningnummer beter controleren (n = 3; 'Want als ik goed had gezien dat het een Duits account was, dan had ik wel genoeg geweten. Dan kun je je in ieder geval afvragen: waarom heb je een Duits account?' (B19)), het vragen naar een foto aan de verkoper met een specifiek item (zoals mes en vork of een pak melk) met of naast het product (n = 2), en het beter controleren van e-mailadressen ('want bij een letter verschil kan het dus al mis zijn' (B2)).

Klanten kunnen hier zelf ook een rol in spelen door van (potentieel) frauduleuze advertenties een melding te maken (E6). Het **stimuleren** van het **maken** van (proactieve) **meldingen** kan bijdragen aan de verstoring van aankoopfraude.
Tot slot vertelde een van de benadeelden dat hij op een veilingsite een extra account had aangemaakt onder de naam 'ik ben een oplichter'. Bij verdenkingen van een frauduleuze advertentie biedt meneer onder dit account een bedrag van 99.999 euro op het betreffende artikel. Met een dergelijk bedrag komt meneer bovenaan te staan in de lijst met biedingen en hij hoopt op die manier anderen te waarschuwen. Hij gaf aan dat andere gebruikers dit ook doen. Dit kan zich vertalen in een soort **burgerwacht** als mogelijke manier om online aankoopfraude te verstoren.[21] Hierbij merken andere gebruikers van bepaalde platformen advertenties aan als (potentieel) frauduleus of waarschuwen ze elkaar daarvoor.[22]

Techniek 7: Natural surveillance. De zevende techniek is natuurlijk toezicht. Bij deze techniek kwam allereerst het **aanbieden** van **betrouwbare controles** naar voren. Er zijn inmiddels al een aantal controlesystemen, zoals het LMIO-controlesysteem, waar gecontroleerd kan worden of een rekeningnummer als verdacht staat gemeld. Een ander voorbeeld is het RDW-controlesysteem waarbij gecontroleerd kan worden of een auto als gestolen staat geregistreerd. De betrouwbaarheid van deze checks kan vermoedelijk worden vergroot wanneer databases met informatie uit meerdere bronnen worden gevoed.
Mogelijk kunnen nieuwe controlesystemen worden ontwikkeld. Bijvoorbeeld in het geval er door een fraudeur documentatie over een product wordt aangeleverd, dat te controleren is in hoeverre die documentatie echt is. Hetzelfde geldt voor identificatiedocumenten, bijvoorbeeld of die gestolen zijn dan wel ongeldig zijn verklaard (E3). Het punt bij dit laatste voorbeeld is dat de effectiviteit mogelijk niet hoog zal zijn. Mensen die een kopie van hun identiteitsbewijs opsturen zijn mogelijk niet op de hoogte van (eventueel) misbruik. Hetzelfde kan gedacht worden bij de toepassing van KvK-nummers. Ten eerste zou er een echtheidskenmerk kunnen worden toegepast. Vervolgens zou er een checkfunctie kunnen komen waar consumenten deze kunnen controleren (E9). In verband met de verhuur van woningen zou Airbnb bijvoorbeeld kunnen vragen naar vergunningen, maar ook verifiëren met wie zaken worden gedaan, of de villa bestaat en op de juiste naam staat (E4). '(…) webwinkels moeten aan heel veel regels voldoen, hotels moeten aan heel veel regels voldoen, waarom zouden platformen daarmee weg kunnen komen door alleen maar te zeggen: ik ben maar een platform?' (E4). Het gebruik van keurmerken werd ook nog genoemd als optie, maar tegelijkertijd wordt de effectiviteit laag ingeschat, omdat het relatief eenvoudig te vervalsen is (E4).

21 Voorheen was er het forum opgeletopinternet.nl dat ook als een soort burgerwacht functioneerde. Dit is echter per 1 juli 2017 gestopt. Zie ook: http://www.opgeletopinternet.nl/index.php/topic,40098.0.html.

22 Dergelijke maatregelen kunnen ook worden opgesteld vanuit het perspectief van opsporing en vervolging. Denk bijvoorbeeld aan het strafrechtelijk vervolgen van daders en het uitvoeren van civiele procedures bij geldezels (Leukfeldt, 2016). Dit valt echter buiten de scope van dit onderzoek.

Een andere nieuwe mogelijkheid is het controleren van Track&Trace-codes. Een lijst met transportbedrijven waar wordt aangegeven of deze wel/niet betrouwbaar zijn, zou kunnen bijdragen aan het tegengaan van de crimescripts waarin deze bedrijven voorkomen. De overheid zou een website kunnen maken met alle transportbedrijven, met daarbij een rechtstreekse link naar de websites. Op deze websites zou men dan de Track&Trace-code moeten kunnen controleren. Door een website met alle transportbedrijven te gebruiken wordt voorkomen dat consumenten belanden op een website die gespooft is. In het geval dat een fraudeur de naam van een transportbedrijf misbruikt zou de klant dit middels de check op de track&Trace-code kunnen identificeren en kunnen fraudeurs mogelijk sneller worden opgespoord. Een benadeelde gaf in de context van nieuwe controlesystemen een ander voorbeeld, zie tekstkader.

Op Europees niveau zou er een website moeten zijn waarop men gemakkelijk kan zien of partijen te vertrouwen zijn. Dit moet op basis van bedrijfsnaam, KvK-nummer, adres, en dergelijke eenvoudig en gratis opgezocht kunnen worden. 'Staat de partij erop, dan moet je erop kunnen vertrouwen dat het goed gaat. Staat een partij er niet op, dan weet je niet zeker of het wel of geen vertrouwde partij is, maar dan heb je minder kans op een frauduleuze betaling' (B9). Veilingsites, webshops, en dergelijke zouden daar ook naar toe moeten linken. 'Dit geldt in ieder geval voor bedrijven. Voor particulieren voert dit waarschijnlijk te ver door' (B9).

Een andere optie waar online handelsplaatsen op kunnen inzetten is om veiligheidsinformatie prominent en continu in beeld te zetten (E3). Bijvoorbeeld dat het aan te bevelen is om controles uit te voeren voordat men overgaat tot betaling. Nu moet vaak naar een aparte veiligheidspagina worden genavigeerd. Zelf actief op zoek gaan naar dergelijke informatie doen consumenten veelal niet, net zoals veel mensen de voorwaarden niet lezen (E4). Ook werd het waarschuwen van klanten of informeren over veiligheidsinformatie via pop-ups genoemd (E5). Een nadeel hiervan kan echter zijn dat men software gebruikt die dergelijke pop-ups blokkeert. Een ander mogelijk probleem hierbij wordt door een expert (E9) 'banner-blindheid' genoemd. Gebruikers zien de informatie in dat geval niet meer staan en daarmee is dit niet meer effectief.

Techniek 8: Reduce anonimity. De achtste maatregel betreft het verminderen van anonimiteit. Om de anonimiteit te verminderen is een rol weggelegd voor de online handelsplatformen die ervoor kunnen zorgen dat de verkopers, maar ook kopers die bij hen zaken doen, beter worden geïdentificeerd. Een vijftal benadeelden en meerdere experts (E1, E3, E5, E7, E8, E9) benoemden spontaan dat de platformen meer moeten doen om **verkopers** en/of **verhuurders** te **identificeren en verifiëren**, bijvoorbeeld bij het aanmaken van een account. 'Gezien zij de daders faciliteren om hun advertenties te plaat-

sen is het hun verantwoordelijkheid' (B13). Een andere optie is het laten verlopen van accounts die een bepaalde tijd niet meer zijn gebruikt. Dit kan het misbruik ervan door criminelen voorkomen.

In twee expertinterviews werden kanttekeningen geplaatst bij de effectiviteit en haalbaarheid ervan (E7, E8). Experts van ICS veronderstellen dat wetgeving nodig is om zodoende deze platformen daaraan te laten conformeren. Dit kan echter worden opgelost wanneer platformen betrouwbaar worden middels KYC ('know your customer'), door daarvan bijvoorbeeld een 'unique selling point' te maken. 'Uit concurrentieoverwegingen kunnen ze daarmee een betrouwbare dienst aanbieden.' Dit kunnen ze bijvoorbeeld doen bij een verhoogd risico, zoals betalingen boven 1.000 euro naar het buitenland. Mogelijk kunnen de platformen ook worden aangesproken op maatschappelijk verantwoord ondernemen of kunnen brancheorganisaties een rol vervullen om het digitale verkeer op deze platformen meer betrouwbaar te laten worden. Experts van de EIB zijn bezorgd dat deze maatregel leidt tot schijnveiligheid. Dit is bijvoorbeeld het geval wanneer een 'betrouwbaar' account wordt gehackt.

Een andere mogelijkheid om te werken aan betere identificatie is het gebruik van een digitaal identiteitsbewijs. Een digitale identiteit zorgt ervoor dat de anonimiteit afneemt en men zeker weet met wie men zaken doet. Een benadeelde opperde om hiervoor DigiD te gebruiken. Dit werd ook genoemd door experts (E9). Mogelijk dat recente ontwikkelingen in eHerkenning, zoals eIDAS (Electronic Identities And Trust Services), daarbij kunnen faciliteren. Tot slot werd door een expert aangegeven dat in het aanmeldproces voor betaalverzoeken op Marktplaats reeds een identificatieplicht zit. Dit wordt samengebracht in het profiel van een gebruiker (E9). Als alternatief kunnen online handelsplatformen dit bijvoorbeeld vormgeven middels gedragscodes.[23]

Identiteitsmisbruik, met daaraan gepaard anonimiteit voor de fraudeur, kan mogelijk ook verstoord worden door het invoeren van een **controlebericht**, bijvoorbeeld via sms of WhatsApp, zodra wordt ingelogd op een account van een online handelsplatform vanaf een ander IP-adres**.** Op deze manier wordt de eigenaar van het account genotificeerd van mogelijk afwijkend gebruik. De eigenaar kan hierdoor sneller handelen bij misbruik van het account en samen met het online handelsplatform passende acties ondernemen tegen identiteitsmisbruik en/of fraude en zo de fraudeur tegenwerken.

Tot slot kan de anonimiteit van daders worden tegengehouden door gebruikers te **weren** die gebruikmaken van een **VPN-verbinding**.[24] Dit wordt bijvoorbeeld toegepast door Netflix (een aanbieder van streamingdiensten) om het buitenlandse aanbod van films en series te blokkeren voor Nederlandse gebruikers.

---

23 Gedragscodes worden ingezet bij de tien grootste sekssites van Nederland om prostitutie-advertenties te verifiëren. Dit is voortgevloeid uit een convenant met de politie, het OM en kinky.nl. Bron: NRC (2018). *Sekssites beloven meer te doen tegen mensenhandel*. Via: https://www.nrc.nl/nieuws/2018/12/06/sekssites-beloven-meer-te-doen-tegen-mensenhandel-a3059802.

24 VPN staat voor Virtual Private Network.

Techniek 9: Place managers. De negende techniek wordt vertaald als plaatsbeheerders. Voor deze techniek is een maatregel boven komen drijven, namelijk het **vierogenprincipe**. Een van de benadeelden gaf aan dat wanneer hij iets boekt hij aan zijn vrouw vraagt om de overboeking te verifiëren. Ook in de klankbordgroep werd de suggestie gedaan dat de sociale omgeving belangrijk is, waarmee men kan overleggen voor het overgaan tot aankoop. De kopers kunnen hun vrienden, familie en/of collega's vragen of de aankoop betrouwbaar geacht wordt. De omgeving kan als spiegel dienen en eventueel corrigeren (E9).

Techniek 10: Formal surveillance. De tiende maatregel is formeel toezicht. Een verstoringsmaatregel die in deze categorie valt is **detectie**. Detectie is belangrijk om uit te voeren door financiële instellingen met als doel om frauduleuze transacties te onderscheppen. Denk hierbij aan het monitoren, analyseren en stoppen van verdachte transacties.[25] Ook online handelsplatformen moeten inzetten op detectie, bijvoorbeeld om frauduleuze accounts en advertenties op te sporen. Hetzelfde geldt voor partijen die zorgdragen voor de registratie van domeinnamen. Dit betekent dat de betrokken partijen blijven investeren in de ontwikkeling van hun detectiesystemen. Hieronder zijn enkele voorbeelden uitgewerkt van detectie zoals uit de interviews naar voren is gekomen.
Betere controles op (het plaatsen van) advertenties door online platformen werken als potentiële verstoringsmogelijkheid alsook het verwijderen van valse advertenties (E3, E4, E5).[26] Daar ligt een verantwoordelijkheid voor de online platformen om dit mogelijk te maken. 'Het kost tijd, geld en investeringen om het te kunnen monitoren en de rotte appels eruit te halen, maar het is niet nieuw. Men zou hier meer aandacht aan moeten besteden om dit tegen te gaan, het gaat al zo lang door' (E4). Er worden echter wel vraagtekens gezet bij de uitwerking ervan (E3, E4).

'Het is natuurlijk ook een plicht voor zo'n platform, als ze weten dat er sprake is geweest van oplichting om daar iets mee te doen. Plus, om die advertentie weg te halen, maar dat neemt niet weg dat dezelfde persoon onder een andere alias of wat dan ook hetzelfde verhaal net in een andere vorm giet en dan weer online zet. (…) En waarschijnlijk doen Marktplaats en Speurders en AutoTrack (…) daar ook wat aan, maar is dat voldoende als het nog steeds voorkomt? Ik vraag het me af' (E4).

Negen benadeelden gaven ook aan dat de betreffende online platformen een verantwoordelijkheid hebben hierin, met name omdat het lijkt alsof deze platformen daders

25 Deze uitwerking past dus ook binnen technieken 5 en 15.
26 Het kan hierbij ook gaan om valse commerciële advertenties; waarvoor handelssites geld ontvangen.

faciliteren bij hun oplichtingspraktijken. Een benadeelde gaf aan het kwalijk te vinden van Marktplaats dat de mogelijkheid wordt geboden om de gegevens van een account te wijzigen; 'hierdoor is misbruik mogelijk' (B4). Een andere benadeelde gaf aan dat, hoewel het betreffende platform waar zij is opgelicht wel verhuurders verifieert, ze meer kunnen doen, bijvoorbeeld om het doorlinken (naar valse websites) in advertenties te voorkomen.

Hostingpartijen kunnen middels detectie het 'valse webshops'-crimescript verstoren. Fraudeurs knippen en plakken namelijk bestaande webshops en de algemene voorwaarden. Een hostingpartij kan deze webshops en/of de gekopieerde algemene voorwaarden mogelijk herkennen (E1). Zo heeft de ING bijvoorbeeld een contract met hostingpartijen om te scannen op valse websites die zich voordoen als de ING. Experts van de Fraudehelpdesk noemden in dit verband een piepjessysteem dat afgaat wanneer domeinen worden geregistreerd die heel erg op andere domeinen lijken. Experts van ICS gaven aan dat er veel overeenkomsten zijn tussen de verschillende valse webshops. Dit zou een partij als SIDN in staat moeten stellen om aan de hand van 'scripts' valse websites te detecteren. Daarbij valt te denken aan veelgebruikte afbeeldingen, slecht vertaalde algemene voorwaarden en dergelijke. Experts van het ECC gaven ook aan dat SIDN hierin een rol kan hebben, bijvoorbeeld wanneer zij alerts ontvangen als dergelijke websites in de lucht zijn. De expert van SIDN gaf aan hierin al een rol te vervullen.

'Er is nu ook al een belangrijke rol weggelegd wat betreft detectie bij SIDN. Dit wordt recentelijk op proactieve basis gedaan, terwijl dat voorheen veelal reactief was. Zo wordt nauw gelet op verdachte websites door bijvoorbeeld valse registratiegegevens te controleren. Uiteindelijk moet dit op basis van verder ontwikkelde algoritmes dagelijks gaan plaatsvinden.' (E2)

'In hoeverre een frauduleuze aankoop daadwerkelijk plaatsvindt, wordt niet gezien door SIDN. Daarnaast is het voor SIDN onduidelijk of de valse webshops nationaal of internationaal zijn. Op basis van de registratiegegevens die SIDN kan inzien, kan de houder zich in Nederland bevinden maar ook in het buitenland. De content op de website geeft ook geen indicatie, omdat deze zowel in het Nederlands als Engels is. Er zijn wel vermoedens dat er meer valse webshops komen uit China en Oost-Europa.' (E2)

Ook andere experts gaven aan dat domeinnamen worden overgenomen en in Chinese handen terechtkomen. Het gaat dan veelal om websites met een onlogische URL. Als voorbeeld werd een URL van een kerk, slager of voetbalvereniging genoemd waar men schoenen kan kopen (E3, E4, E7). Experts van ICS gaven aan dat de aankoopfraudes waarmee zij te maken hebben veelal transacties betreffen van klanten die producten bestellen bij Chinese webshops. Tevens worden zij geconfronteerd met valse websites die zijn ontworpen om creditcardgegevens te stelen.

Een van de experts riep ertoe op dat de politie meer moet samenwerken met de industrie (en eigenlijk met alle betrokken partijen, zie tekstkader) om fraude te voorkomen (E5). Zo zijn experts van de City of London Police bijvoorbeeld in gesprek met advertentieplatformen en advertentieregelgevers. Door samen te werken moet het volgens hen mogelijk zijn om een advertentie van een frauduleus product of dienst vanaf het begin te identificeren aan de hand van de manier waarop ze worden gepresenteerd (o.a. onrealistisch hoge rendementen en overdreven aantrekkelijke prijzen) voordat schade wordt aangericht. 'The key is working together. We have to cooperate with each other' (E5).

Hoewel er in de door ons geanalyseerde zaken alleen door benadeelden werd betaald via het digitale betalingsverkeer, kwam in het interview met de City of London Police naar voren dat in een bepaald crimescript slachtoffers moesten betalen door middel van iTunes-kaarten.[27] *Door als politie in gesprek te gaan met retailers die deze kaarten verkopen, stelden de verkopers in het vervolg vragen aan kopers die grote hoeveelheden wilden afnemen, waarmee deze vorm van oplichting kon worden teruggebracht. Voor aankoopfraude geldt dat er ook moet worden samengewerkt met internationale politiediensten, wat overigens al wordt gedaan.*

Er zijn reeds diverse publiek-private samenwerkingsverbanden of overlegvormen waarin stakeholders (online) fraudeproblematiek met elkaar bespreken en bekijken hoe dit het beste is aan te pakken. Hierbij kan bijvoorbeeld worden gedacht aan het EPIO-overleg waarin het LMIO, de NVB, banken en andere stakeholders actief zijn en andere interbancaire overleggen (E1).[28] In die overleggen wordt onder andere aandacht besteed aan verstoringsmogelijkheden van criminaliteit. 'We doen wat we kunnen, maar we zien niet alles. En we kunnen het niet helemaal voorkomen.' Een ander voorbeeld is de EIB die samenwerkt met Tweedehands.be in de aanpak van fraude (E8). Concrete maatregelen die zijn voortgevloeid uit deze samenwerking zijn dat, na analyse van crimescripts, geen betalingen meer verricht kunnen worden via anonieme betaalmogelijkheden, zoals 'giftcards' en 'paycards', en dat er geen contact meer kan plaatsvinden op het platform met klanten middels 'scripts' of 'robots'.
In groter verband kan worden gedacht aan het Electronic Crime Task Force (E1), een samenwerkingsverband tussen de banken, politie en het Openbaar Ministerie (OM). Het gaat daarbij voornamelijk om high-impactzaken, die vaak ook een internationale component kennen. Als een bank inzicht heeft in een (netwerk van) begunstigde(n) dan wordt daar spoedig op geacteerd en waar nodig worden gegevens verstrekt aan de

27 Een benadeelde zette haar vraagtekens bij het faciliteren van prepaid betaalkaarten (i.e. betaalkaarten waar geen bankrekeningnummer achter zit) door banken. Dit maakt het volgens deze benadeelde gemakkelijker voor fraudeurs om geld op te nemen.

28 EPIO staat voor expertpoule internetoplichting.

politie. Hier kan echter ook een preventieve werking van uitgaan. Als vanuit detectie of bijvangst van een ander onderzoek (potentiële) slachtoffers en/of begunstigden aan het licht komen, kunnen daar preventieve maatregelen op worden genomen. Als wordt gekeken naar aankoopfraude, is er ook samenwerking tussen banken en het LMIO. Concreet houdt deze samenwerking in dat wanneer er drie meldingen binnenkomen van hetzelfde bankrekeningnummer bij het LMIO, er maatregelen worden genomen bij de bank. Ook wordt andere nuttige informatie gedeeld met het LMIO, zoals patronen en signalen. Dergelijke zaken worden eveneens gedeeld met andere partijen, zoals Marktplaats. Tevens wordt informatie over malafide webshops gedeeld tussen LMIO, OM en niet-bancaire betaaldienstverleners.[29] Het delen van informatie draagt bij aan de verstoring van fraude en oplichting (E1).[30]

Al brainstormend met een van de experts kwam het idee bovendrijven voor een 'low impact crime' of 'high volume crime' task force (E1). Dit is mogelijk haalbaar, maar iemand moet zich daar dan wel hard voor maken, en alle partijen (banken en politie) moeten daarmee akkoord gaan. Dan blijft de vraag wat het belang voor de bank is, want de bank blijft een commercieel bedrijf. Immers, het betreft geen prioritaire aangelegenheid voor de bank; er is geen verlies.

Volgens twee experts zit de ideale oplossing waarschijnlijk in **Europese publiek-private samenwerking** (PPS) (E1, E6). In deze samenwerking kunnen gegevens over frauduleuze werkwijzen, persoonsgegevens van fraudeurs, bankrekeningnummers en andere relevante informatie gedeeld worden. Door het delen van deze gegevens wordt het makkelijker voor de aangesloten partijen om preventief in te zetten op deze aanvalsstrategieën en/of fraudeurs. Daarnaast wordt hiermee de pakkans vergroot. Deze Europese PPS kan ervoor zorgen dat fraudeurs meer moeite moeten doen om de fraude te laten slagen, bijvoorbeeld doordat zij meer geldezels moeten werven. Geldezels of katvangers zijn nodig om geld te cashen en naar verwachting worden met een dergelijke PPS geldezels eerder geïdentificeerd. Een van de experts gaf aan dat het gevoel hem echter beklemt dat dit wordt gehinderd door de privacywetgeving. 'Het internet kent geen grenzen. Wij wel, helaas' (E1).
De andere expert zei het volgende in relatie tot Europese PPS (E6): 'The dream would be to have a European collaboration. At the moment, the European collaboration is good and effective in the physical world. But we are trying to solve online cases by using traditional methods. In the future, 100% of the cases will be online and transna-

29 Currence.nl (2017). *LMIO, OM en Currence iDEAL pakken malafide webshops aan*. Via: https://www.currence.nl/nieuws/lmio-om-en-currence-ideal-pakken-malafide-webshops-aan/.
30 Bij het delen van informatie kan ook worden gedacht aan het verstrekken van camerabeelden en het uitleveren van juridische gegevens.

tional. Therefore, it would be easier to report transnationally. Europe should implement a collaboration of public and police forces, to have an immediate collaboration instead of taking more time to build cases. This could take form in a website portal where all customers in Europe can report online cases [**een Europees meldpunt**]. This portal can be used by European parties like OLAF and other relevant parties who have a direct communication with police forces.'

Een benadeelde ziet in dit verband een rol weggelegd voor internetgiganten zoals Google en Facebook. De overheid zou volgens deze benadeelde met betreffende partijen EU-breed moeten samenwerken. 'Als ik zie waar Google toe in staat is om in no time een precies profiel van mij te kunnen maken, dan moeten ze dat ook wel met criminelen kunnen doen.' En als dergelijke partijen niet willen samenwerken, dan moet dat volgens deze benadeelde afgedwongen kunnen worden. 'Google en Facebook en dergelijke hoeven hun bedrijfsgegevens niet publiekelijk weg te geven, maar de hele privacy lijkt er veel meer op gericht om criminelen te helpen beschermen.' (B18)

Een andere expert opperde ook om één grote database of register te maken waar meldingen van valse webshops gedaan worden; het liefst op Europees of wereldwijd niveau (E2). Nu is dat volgens hem te versnipperd en niet up-to-date. Meldingen worden nu bijvoorbeeld gedaan bij SIDN, LMIO en Radar. In het verlengde van de Europese PPS kunnen via dit meldpunt alle aangiftes met bijbehorende relevante informatie verzameld worden. Burgers van alle aangesloten landen kunnen hier melding maken en daardoor wordt het overzichtelijker welke zaak bij welk(e) land(en) hoort, voor eventuele opsporing. In de huidige situatie zijn de mogelijkheden tot melding maken per land verschillend en worden verschillende definities van fraude gebruikt. Een Europees meldpunt kan bijdragen aan een eenduidige Europese meetmethode en door het delen van kennis het fraudebewustzijn verhogen.[31]

5.3 Strategie 3: Beloningen voor criminaliteit beperken

De derde strategie 'reduce the rewards' is het beperken van de beloningen van criminaliteit. Binnen deze strategie hebben Cornish en Clarke (2003) vijf technieken ontwikkeld die deze beloningen kunnen verlagen (11-15). Deze zijn hier uitgewerkt voor de context van aankoopfraude.

Techniek 11: Conceal targets. De elfde techniek is het verbergen van doelen. Voor deze techniek hebben we geen verstoringsmogelijkheden kunnen identificeren. Dit komt

31 Dit wordt ook onderschreven in NFA (2011).

vermoedelijk doordat slachtofferschap van aankoopfraude een random gebeurtenis lijkt te zijn. In het geval van het 'reageren zoekadvertentie'-crimescript kan gedacht worden aan het verbergen van 'gevraagd'-advertenties, maar erg realistisch lijkt deze verstoringsstrategie niet.

Techniek 12: Remove targets. De twaalfde techniek is het verwijderen van doelen. Hieronder wordt het onbereikbaar maken van potentiële slachtoffers verstaan. De experts van de Fraudehelpdesk noemden in dit verband een specifiek aandachtspunt voor ondernemers die een website of webshop hebben. Zij gaven aan dat ondernemers die een **domeinnaam** willen **opzeggen** hiervan **melding** kunnen **maken** bij SIDN. Dit voorkomt dat derden misbruik van dat betreffende account kunnen maken. Op die manier wordt het moeilijker gemaakt om potentiële slachtoffers te bereiken en fraude te plegen. Deze maatregel wordt onderkend door experts van ICS. Zij gaven daarbij aan dat SIDN mogelijk ook een proactieve rol daarin kan aannemen. Een andere mogelijkheid om fraudeurs tegen te werken is om **bedrijven zonder website te detecteren**. Volgens geïnterviewde experts maken fraudeurs ook valse webshops aan op de naam van bedrijven die geen website hebben. Door deze bedrijven te detecteren en te waarschuwen kan dit verstorend werken voor bepaalde aankoopfraudes.

Techniek 13: Identify property. De dertiende techniek betreft identificatie van eigendom. Het **identificeren van legitieme webshops en verkopers** werpt een drempel op bij fraudeurs. De eerste verstoringsmogelijkheid is een whitelist van webshops. Dit is een lijst met webshops die geverifieerd zijn en als betrouwbaar zijn aangemerkt. In onderstaand tekstkader is een suggestie van een benadeelde gepresenteerd.

Een van de benadeelden ziet het identificeren van legitieme webshops meer in het hanteren van betere rating-systemen. De rating zou niet gegeven moeten worden op basis van de informatie die op een website staat, maar op basis van statistieken; hoeveel bezoekers heeft de website, hoeveel transacties zijn er afgehandeld, et cetera. 'Als ik daar had gezien dat er maar twaalf of vijftien transacties hebben plaatsgevonden, dan had ik nooit op die site geboekt. Met Google kun je tegenwoordig alles vinden, dus waarom heb je dan niet ergens een knop zitten als je op een site zit waarmee je de betrouwbaarheid van die website kan valideren of verifiëren. Als je dan naar een site gaat met weinig rating, dan zoek je zelf het risico op.' Meneer trekt hierbij de vergelijking met keurmerken. (B18)

Een alternatieve strategie is om specifieke domeinnamen te introduceren voor specifieke producten en diensten (E5). Op deze specifieke domeinen dient daadwerkelijk controle plaats te vinden wanneer zij worden aangevraagd, waardoor ze als 'vertrouwd' bestempeld kunnen worden. Zo maakt de Britse politie gebruik van .police.uk. Dit

maakt het duidelijk dat men van doen heeft met de politieorganisatie. Belangrijker is dat niemand anders een dergelijk domein kan kopen. Nu kan er relatief eenvoudig een domein worden aangevraagd en is controle minimaal. Bovendien zijn op dit moment alle verschillende domeinen te koop, inclusief .nl, .uk en .eu, wat de indruk wekt dat het bedrijf/individu zich in Nederland, het Verenigd Koninkrijk of de EU bevindt, terwijl dit misschien niet het geval is. Met deze maatregel kunnen webshops een toevoeging bij hun domeinnaam krijgen zodra ze geverifieerd zijn aan de hand van hun licentie. Alle geverifieerde webshops die tickets verkopen eindigen bijvoorbeeld op .tickets.nl. Op die manier weet de consument zeker dat de licentie van de webshop is gecontroleerd en tegelijkertijd werpt dit een drempel op voor fraudeurs omdat het lastig kan worden gemaakt om een dergelijke dedicated domeinnaam te bemachtigen. Hierbij moet er wel rekening mee worden gehouden dat de kosten laag moeten zijn; een MKB-ondernemer moet hier ook gebruik van kunnen maken.

Techniek 14: Disrupt markets. De veertiende maatregel is het verstoren van markten. De verstoring van markten kan op online handelsplatformen en social media (advertenties) of via webshops. Op online handelsplatformen kan dit door het actief blokkeren of **verwijderen** van **frauduleuze accounts** en **advertenties**. Door deze accounts en advertenties te verwijderen wordt de kans op slachtofferschap kleiner. Mogelijk kunnen gegevens worden verstrekt aan de politie (E1, E2).[32] Dat geldt vanzelfsprekend ook voor sociale media. Daarbij wordt tegelijkertijd aangegeven dat online platformen al verschillende maatregelen treffen. Zij zien IP-adressen en zouden advertenties, gegevens, locaties, et cetera van de fraudeur mogelijk bloot kunnen leggen. Dit is echter maar in beperkte mate effectief, want de fraudeur kan een ander account aanmaken, een ander adres opgeven en een ander IBAN gebruiken.[33]
Frauduleuze webshops kunnen, wanneer als zodanig geïdentificeerd, via een **notice-and-take-down** (NTD)-verzoek onbereikbaar worden gemaakt (E1, E2, E3, E4, E6, E7, E8, E9). Dit is het melden van een valse webshop aan de partij die de website host.[34] Ook hiermee kan het aantal (potentiële) slachtoffers worden teruggebracht. Een NTD-verzoek kan iedereen indienen, maar heeft als potentieel nadeel dat het hostingbedrijf niet snel reageert of zelfs betrokken is bij de criminele activiteiten. Hoewel een NTD daarnaast een ingrijpende procedure is, kunnen volgens experts van het ECC partijen als de ACM en de Fraudehelpdesk hierin een actieve rol nemen om websites af te laten sluiten. Diverse experts veronderstellen dat SIDN hierin, bijvoorbeeld vanuit een zorgplichtgedachte, een grotere rol kan spelen in het proactief platleggen van valse websites (E7, E9). In onderstaand tekstkader wordt duidelijk dat dit geen sinecure is.

32 Op dit moment is het echter zo dat de politie niet op proactieve wijze gegevens ontvangt, maar ontvangt zij alleen gegevens aan de hand van een vordering (E9).

33 Het IBAN en het verdere betalingsverkeer ziet een platform in principe niet, tenzij de koper en verkoper via een eigen escrow-dienst de betaling afhandelen.

34 Een voorbeeld van deze procedure is te vinden op de website van SIDN, zie: https://www.sidn.nl/downloads/procedures/Notice_and_Take_Down_procedure_voor_nl_domeinnamen.pdf.

Als een NTD bij SIDN wordt ingediend dan moet SIDN kunnen beoordelen dat het onmiskenbaar strafbaar of onrechtmatig is wat de website doet. Verzoeken tot een NTD komen vooral binnen voor websites met een schending van intellectueel eigendomsrecht en over smaad/laster. Voor valse webshops gaat het om ongeveer 30 NTD's per jaar. Daarnaast is het moeilijk om te beoordelen dat valse webshops strafbaar/onrechtmatig handelen. (E2)

Daarnaast is de NTD-procedure omslachtig, omdat het verzoek aan meerdere partijen wordt voorgelegd. Wat SIDN wel kan doen is het controleren van registratiegegevens, omdat deze negen van de tien keer vals zijn (E2). In de algemene voorwaarden staat dat de registratiegegevens correct moeten zijn en dat op basis van incorrecte registratie een registratie beëindigd mag worden door SIDN. Er wordt dus alleen een registratie verwijderd als de registratiegegevens vals zijn. SIDN wil namelijk niet zelf op de stoel van de rechter gaan zitten om te bepalen welke website wel of niet geregistreerd mag zijn.

SIDN vraagt eerst de registrar om de registratiegegevens te controleren. Met sommige registrars is goed contact en die verwijderen malafide websites. Maar contact met sommige andere registrars is moeilijker en die zijn ook vaak in het buitenland gevestigd. Indien een registrar de gegevens niet geeft, wordt de registratie van de verdachte website beëindigd door het SIDN. Daar gaat momenteel een lange tijd overheen, namelijk 35 dagen. SIDN is bezig om de ***tijd*** *die het kost om een* ***website offline*** *te* ***halen*** *te* ***verkorten****, wat bijdraagt aan het verstoren van deze vorm van criminaliteit. De verwachting is namelijk dat valse webshops dan minder slachtoffers maken. Bovendien kost het criminelen geld en moeite om een nieuwe domeinnaam te registreren.*

Het initiatief tot een NTD hoeft niet bij de politie te liggen, maar kan ook door private partijen worden opgepakt. Experts van de City of London Police gaven aan dat het offline halen van een domein waarop valse producten worden verkocht – waarvoor flink geadverteerd wordt – en daarbij een melding publiceren waarin staat dat het bedrijf frauduleus is, een grote kostenpost is voor fraudeurs, omdat ze het 'bedrijfsimago' moeten aanpassen. Als kanttekening vermelden zij hierbij dat dergelijke verstoringstechnieken een dreiging niet per se elimineren. De daders kunnen zich eenvoudigweg verplaatsen naar een ander platform of opereren onder een nieuwe naam, zie ook tekstkader.

'When you use the word disruption, often it's just displacement. Fraudsters will often find another way. However, we are slowing them down and displacing them bit by bit; we disrupt them in the end as it costs them more money. (…) Do we always disrupt them? Arguably we don't, but do we make it harder for them? Yes we do.'

Techniek 15: Deny benefits. De vijftiende techniek betreft het ontzeggen van voordelen. Dit kan worden gerealiseerd door middel van een **efficiëntere internationale samenwerking tussen banken.** In de huidige situatie worden SWIFT-berichten gebruikt om geldstromen tegen te houden en terug te halen. Indien banken efficiënter samenwerken en de geldstromen sneller tegengehouden worden en/of kunnen worden teruggehaald, dan wordt de fraudeurs hun geld ontzegd. Uit expertinterviews blijk echter dat internationale samenwerking betreffende het tegenhouden van geldstromen beperkt is gezien verschillende internationale regelgeving. Samenwerking kan daarom beter worden ingezet op het uitwisselen van verdachte zaken, crimescripts, et cetera.

5.4 Strategie 4: Provocaties verminderen die uitnodigen tot criminaliteit

De vierde strategie 'reduce provocations' is het verminderen van provocaties die uitnodigen tot criminaliteit. Binnen deze strategie hebben Cornish en Clarke (2003) vijf technieken ontwikkeld die deze provocaties kunnen verminderen (16-20). Deze zijn uitgewerkt voor de context van aankoopfraude.

Techniek 16: Reduce frustrations. De zestiende techniek gaat over het verminderen van frustraties bij de dader. Deze maatregel is van toepassing bij een misdaad met emotionele motieven, maar aankoopfraude lijkt op basis van onze data een misdaad die vooral bewust wordt gepleegd voor economisch gewin. Derhalve was het voor deze criminaliteitsvorm lastig om verstoringsmogelijkheden te identificeren binnen deze techniek.

Techniek 17: Avoid disputes. De zeventiende maatregel heeft betrekking op het vermijden van geschillen. Geschillen, waaronder aankoopfraude, kunnen worden voorkomen door **aankopen** te doen **via officiële partijen** of via het eigen sociale netwerk. In de regel zorgen officiële partijen voor een gedegen levering van het product of dienst en kunnen geschillen worden voorkomen. Deze mogelijkheid voor verstoren werd door negen benadeelden genoemd. In het geval van het kopen van tickets werd door drie benadeelden gewezen op het platform Ticketswap.[35] In een van de expertinterviews werd de mogelijkheid geopperd om te werken met 'whitelists', waar mensen kunnen controleren of een website veilig is (E7).

35 Een andere mogelijkheid om ongewenste handel met tickets te voorkomen is om deze te personaliseren. Zie bijvoorbeeld: https://help.ticketmaster.nl/hc/nl/articles/360006690253--Waarom-worden-tickets-op-naam-gepersonaliseerd-verkocht-.

Experts van het ECC noemden een specifiek aandachtspunt dat betrekking heeft op de mate waarin men als koper beschermd is. Koopt men van een particulier, dan is er heel weinig bescherming en heeft men nergens recht op. Koopt men van een handelaar, dan is er veel betere bescherming door het consumentenrecht (zie ook hoofdstuk 6). Geschillen kunnen mogelijk vermeden worden door particulieren **informatie** te geven over de verschillende **rechten** die zij hebben op basis van welke rol zij aannemen in het doen van online aankopen; **particulier versus consument.** Platformen kunnen daarin een rol spelen om aan hun klanten duidelijker te maken met wie ze te maken hebben. Dat betekent dan wel dat deze partijen meer moeten doen aan verificatie. Het werpt een drempel op voor fraudeurs, maar ook voor de platformen. 'Ja, en drempels willen ze dus allemaal niet, want het moet zo simpel en veel mogelijk, want ze willen daarbij winst behalen en hoe meer transacties, hoe meer winst, maar dat mag geen reden zijn' (E4).

Techniek 18: Reduce arousal. De achttiende strategie is vertaald als het verminderen van opwinding. Voor deze meer emotioneel gedreven maatregel hebben we in het onderzoek geen aanwijzing gevonden dat dit kan helpen in het verstoren van deze criminaliteitsvorm.

Techniek 19: Neutralize peer pressure. De negentiende techniek gaat over het neutraliseren van groepsdruk. Groepsdruk wordt in dit onderzoek gelinkt aan geldezels. Hoewel de inzet van geldezels in de door ons geanalyseerde crimescripts niet naar voren kwam, werd dit wel vaak benoemd in de expertinterviews. Geldezels worden geronseld om hun bankrekening ter beschikking te stellen om frauduleus verkregen geld te cashen.
Voorlichting hoeft niet alleen betrekking te hebben op consumenten, maar kan ook betrekking hebben op de actoren die zich bezighouden met criminaliteit, zoals **geldezels**. Een concreet voorbeeld hiervan is het EMMA-project dat wordt gecoördineerd vanuit Interpol.[36,37] In dit project werden begin 2016 81 geldezels (van bijvoorbeeld phishing en oplichting) door de politie gearresteerd. Dit initiatief, samen met de campagne 'Word geen money mule', heeft volgens een expert zeker effect (E1). Zo weten (potentiële) geldezels dat ook achter hen wordt aangezeten, zowel door de bank als de politie. Door voorlichting te geven over de gevolgen van medeplichtigheid aan fraude kan mogelijk een drempel worden opgeworpen.
Een andere verstoringsmogelijkheid gericht op geldezels zijn zogenoemde 'knock-and-talk'-acties (E1), ook wel 'stopgesprekken' genoemd.[38] Hierbij kan gedacht worden aan een wijkagent die met een 'first offender' geldezel in zijn/haar thuissituatie de kwestie bespreekt, eventueel samen met de ouders erbij. Tijdens dit gesprek kan een waarschuwing worden gegeven dat bij een volgende keer of bij het niet teruggeven van het buitgemaakte geld er een strafrechtelijk traject zal volgen en/of schulden bij de bank kunnen ontstaan. Een alternatieve waarschuwing kan zijn, wanneer een geldezel een uitkering ontvangt, om deze activiteiten door te spelen aan uitkeringsinstanties

36 EMMA staat voor European Money Mule Action.
37 Europol (2016). *Europe-wide action targets money mule schemes.* Via: https://www.europol.europa.eu/ newsroom/news/europe-wide-action-targets-money-mule-schemes.
38 Projectleider LMIO (persoonlijke communicatie, 8 november, 2018).

(E9). Voor internationale aankoopfraude zou voor een dergelijke strategie samenwerking gezocht moeten worden met de buitenlandse diensten en/of instanties. Vervolgonderzoek kan uitwijzen in hoeverre een en ander vanuit een civiel perspectief mogelijk is, bijvoorbeeld via deurwaarders of rechtsbijstandsverzekeraars.

Techniek 20: Discourage imitation. De twintigste techniek betreft het ontmoedigen van imitatie. In de huidige situatie is de pakkans voor aankoopfraude vanuit het buitenland laag. Dit lucratieve verdienmodel nodigt uit tot imitatie. Door de **pakkans te verhogen** kan imitatie van aankoopfraude worden ontmoedigd. Hier ligt niet alleen een rol voor de politie in relatie tot opsporing en vervolging, maar vooral een rol voor private partijen met een preventief karakter. Denk bijvoorbeeld aan het aanspreken c.q. waarschuwen van geldezels door banken; zie techniek 19. Mogelijk kan de politiek, of de overheid in bredere zin, afdwingen dat hierin een slag wordt gemaakt.

5.5 Strategie 5: Excuses wegnemen voor het plegen van criminaliteit

De vijfde, en daarmee laatste strategie 'remove excuses' is het wegnemen van excuses voor het plegen van criminaliteit. Binnen deze strategie hebben Cornish en Clarke (2003) vijf technieken ontwikkeld die excuses kunnen wegnemen (21-25). Deze zijn uitgewerkt voor de context van aankoopfraude.

Techniek 21: Set rules. De eenentwintigste techniek is het stellen van regels. Door regels vast te stellen over de communicatie en de betalingswijze kunnen excuses worden weggenomen. Bij een aankoop kan een individu rekening houden met de volgende drie regels. De eerste regel is: blijf **communiceren op het online handelsplatform**. Dit biedt meer bescherming dan communiceren buiten het platform. De tweede regel is: **controleer de verkoper**. Recensies en persoonlijke gegevens kunnen gecontroleerd worden op internet, alsook websitegegevens.[39] De derde regel is: **maak gebruik van vertrouwd betalen**. Regel één wordt hieronder toegelicht. Regels twee en drie zijn reeds uitgewerkt (zie technieken 3 en 6).
Een tip die door meerdere experts werd genoemd is om te blijven communiceren in de omgeving van het betreffende online platform (E3, E4, E5, E6, E8), bijvoorbeeld in de aangeboden chatomgeving. Dit wordt gezien als veiliger dan communiceren via een onafhankelijk platform, zoals WhatsApp en privé-e-mail. Hier ligt tevens een taak voor online platformen om klanten daarover te informeren. Ter illustratie, Airbnb heeft volgens experts van de EIB duidelijk op de website vermeld hoe oplichting voorkomen kan worden, en als men op de website blijft dat men beschermd is door de verschillende mogelijkheden die ze bieden. Een mogelijke reden voor consumenten om buiten het platform te opereren is dat ze goedkoper het product of de dienst kunnen afnemen. In dat geval 'lijkt het alsof ze een berekend risico nemen'.

39 Hierbij kan gedacht worden aan https://who.is/ voor de controle van .com-domeinnamen en https://www.sidn.nl/ voor de controle van .nl-domeinnamen.

Communiceren binnen de omgeving van een platform is echter niet een waterdichte oplossing, want accounts kunnen bijvoorbeeld gehackt worden. Een mogelijkheid om dit op te lossen is door een melding te geven van de 'interne' communicatie op een ander kanaal, zoals e-mail of sms. Dit zorgt ervoor dat een gebruiker mogelijk kan detecteren dat zijn/haar account is gehackt; hoewel een e-mailbox natuurlijk ook gehackt kan worden en dergelijke communicatie kan worden afgevangen.

Techniek 22: Post instructions. De tweeëntwintigste techniek betreft het geven van instructies. De voorgenoemde regels (zie techniek 21) worden niet gevolgd als ze niet bekend zijn bij het publiek. Een verstoringsmaatregel is om **waarschuwingen en voorlichting** te geven op het **online handelsplatform**. Dit is bijvoorbeeld handig wanneer kopers op zoek zijn naar een risicovol product, zoals tickets. Een concreet voorbeeld uit de praktijk is dat 2dehands.be haar gebruikers via e-mail waarschuwt zodra ze op zoek gaan naar tickets.

Techniek 23: Alert conscience. De drieëntwintigste techniek betreft het aanspreken of waarschuwen van het geweten. Een aantal geïnterviewde experts benoemen dat algemene bewustzijnscampagnes minder effect hebben in vergelijking tot specifiek gerichte bewustzijnscampagnes. Een waarschuwing is daarbij het meest effectief op het moment en de plaats waar online fraude plaatsvindt. Dit kan dus het online handelsplatform zijn of het moment van betalen. Een concrete verstoringsmaatregel is het **actief waarschuwen zodra geld wordt overgemaakt naar het buitenland** (E7, E9), hoewel fraudeurs vaak een goed verhaal hebben waarom dat dan zou moeten. De bank of de Payment Service Provider kan een waarschuwing geven zodra geld naar het buitenland wordt overgemaakt, eventueel met checks om een betrouwbare aankoop te verzekeren. Bij banken is er overigens al wel vaak een detectie op een eerste transactie naar het buitenland. Wellicht zou dat uitgebreid moeten worden wanneer er meerdere betalingen in korte tijd naar hetzelfde nummer worden overgemaakt. Denk bijvoorbeeld aan het crimescript waarbij voor de aankoop van een auto vaak meerdere betalingen worden gedaan.
In het verlengde van bovengenoemde kan een buitenlands rekeningnummer gecontroleerd worden door middel van een **IBAN-Naam Check op Europees niveau** (E3, E7). In de overige expertinterviews werd deze mogelijkheid niet door experts zelf aangedragen, maar is ernaar gevraagd door de onderzoekers. Bij de overboeking ziet de gebruiker of het rekeningnummer op de gegeven naam geregistreerd staat. Als er geen match is tussen de naam en het rekeningnummer wordt een waarschuwing aan de gebruiker gegeven. Op deze wijze kan de gebruiker extra gewaarschuwd worden. Een dergelijke check maakt het misbruiken van gestolen identiteitsbewijzen ook lastiger (E1). Een van de benadeelden benoemde dat in ieder geval álle banken in Nederland een IBAN-Naam Check moeten invoeren (B2). De klankbordgroep opperde om het eerst in de Benelux uit te proberen (E9). Tevens zitten er een aantal kanttekeningen aan deze verstoringsvorm, zie onderstaand tekstkader.

Een dergelijke check lost niet alles op. Vanuit de AVG wordt namelijk vrij beperkte informatie gegeven, bijvoorbeeld 'bedoelt u naam X?'. Vroeger kon je bij een 1 cent-transactie zien wie de andere rekeninghouder was, maar nu kan dit niet meer getoond worden. Daarnaast hebben mensen de mogelijkheid om de transactie ondanks een afwijking door te zetten. Als de fraudeurs gebruikmaken van social engineering 'de rekening staat op naam van X, want …', is deze verstoring te omzeilen. Een andere mogelijkheid zou zijn om een harde blokkade in te voeren als het rekeningnummer niet overeenkomt met de opgegeven naam. De bank zou dan een extra controle uit kunnen voeren bij deze gevallen. Op grote schaal is dit echter niet realistisch en vertraagt het het betalingsverkeer (E1). Ook moeten mensen zich bewust zijn van wat een (uitgebreide) IBAN-Naam Check doet (E2).

Daarnaast speelt het effectiviteitsvraagstuk op andere wijze een rol. Experts gaven aan dat bankrekeningen veelal toebehoren aan geldezels (E3, E5). Experts van de Fraudehelpdesk gaven tevens aan dat hiermee aankoopfraude bij Chinese webwinkels niet wordt tegengehouden. Experts van ICS vroegen zich af hoe betrouwbaar een dergelijk systeem is. In Nederland kan namelijk al met afgeleide identificatie een rekening worden geopend, wat potentieel onveilig is. De vraag is hoe dat is geregeld in het buitenland en welke regels daar gelden. Daartegenover stellen experts van de EIB dat als het in Nederland geregeld kan worden, dat ook binnen Europa moet kunnen lukken; en het liefst overal. Andere experts gaven aan dat het belangrijk is om te leren van praktijken uit andere landen (E5). Daarbij werd een voorbeeld genoemd van de praktijk in Georgië. Voor een fraudeur is het daar moeilijk om geld te ontvangen, omdat ze daar een kopie van de factuur moeten overleggen met aanvullend een verklaring wanneer ze geld ontvangen van een nieuwe betaler.

Techniek 24: Assist compliance. De vierentwintigste techniek is hulp bieden bij naleving. Het controleren van gegevens kost moeite, waardoor men kan nalaten dit te doen. In eerdere verstoringsmaatregelen werd geadviseerd om de verkoper te controleren (zie technieken 6 en 21). De betrouwbaarheid van het rekeningnummer van een verkoper kan gecontroleerd worden op de website van het LMIO. Op de website van de RDW is er de mogelijkheid om een kenteken te controleren en wordt aangegeven of een auto niet verzekerd is of als gestolen/vermist is opgegeven. Een van de benadeelden noemde deze optie als mogelijke verstoringsmogelijkheid; de experts noemden dit niet spontaan. Deze checks staan dus online, maar zijn niet zichtbaar op het moment van de zoektocht en/of aankoop van het product. Men moet nu (a) weten dat deze checks bestaan en (b) er apart naartoe surfen. Een manier om hulp te bieden bij het uitvoeren van controles kan door gebruik te maken van een **plug-in** op bijvoorbeeld **online handelsplatformen**, waarbij deze zaken direct gecontroleerd kunnen worden. Volgens een van de experts kan het aangeven op welke data deze checks zijn gebaseerd extra gewicht meegeven voor consumenten (E2).

Dergelijke checks moeten simpel uit te voeren zijn en mogelijk alleen een ja of nee communiceren, aangezien het om gevoelige informatie gaat. De AVG kan een beperkende rol spelen, omdat er al gauw sprake is van verwerking van gegevens (E9). Wellicht is deze beperking te ondervangen als gebruikers van deze controlesystemen alleen een 'groen lampje' te zien krijgen, of kan langs de AVG worden gewerkt door aan verkopers expliciet toestemming te vragen of ze gecontroleerd mogen worden. Daarnaast moet het ook niet zo zijn dat het criminelen gaat helpen (E3). Experts van ICS betwijfelen de effectiviteit hiervan. Volgens hen biedt dit schijnveiligheid, doordat criminelen er gemakkelijk langs kunnen werken. In het geval van auto's kunnen criminelen gemakkelijk een auto op straat fotograferen en deze online te koop aanbieden. 'Op die manier lijkt een "goede" auto te worden verkocht, ook volgens het RDW-systeem' (E7). Een alternatief kan zijn dat deze controle automatisch door het handelsplatform wordt gedaan; dat wanneer een advertentie voor een auto wordt geplaatst, het kenteken wordt aangemeld bij de RDW. De RDW zou aan de tenaamgestelde een bericht kunnen sturen ter verificatie dat de auto te koop staat.
Een andere verstoringsmaatregel is een duidelijke **meldknop op online handelsplatformen**. Uit de slachtofferinterviews is meermaals naar voren gekomen dat de platformen geen duidelijk meldsysteem hadden en/of geen actie ondernamen zodra een advertentie of account als frauduleus werd gemeld. Een dergelijke maatregel kan dus hulp bieden bij het melden van (potentiële) fraude.

Techniek 25: Control disinhibitors. De vijfentwintigste techniek betreft controle van impulsief gedrag. Het lijkt verstandig om hiermee te beginnen op basisscholen. **Campagnes op scholen** moeten gericht zijn op toekomstig slachtofferschap en moeten daderschap voorkomen. Door kinderen op een vroege leeftijd cyberhygiëne aan te leren, verkleint dit de kans op slachtofferschap van aankoopfraude. Daarnaast is de campagne erop gericht om een subcultuur te voorkomen waarin het normaal is om cybercriminaliteit te plegen. Daarbij moet duidelijk worden gemaakt dat cybercriminaliteit echte misdaad is, met echte slachtoffers. Hoewel dit niet expliciet naar voren kwam in de interviews, lijkt dit wel van belang. Dit geldt niet uitsluitend voor aankoopfraude, maar in bredere context.

5.6 Strategieën zijn niet het eindpunt

De hierboven geïdentificeerde maatregelen markeren niet het einde in de strijd tegen internationale aankoopfraude. Maatregelen zijn immers zelden perfect en ze kunnen zelfs nadelen hebben. Daarnaast kunnen fraudeurs wanneer zij eenmaal de maatregelen kennen, hun werkwijzen daarop aanpassen om er zodoende omheen te werken. Het is dan ook lastig om op deze plaats vast te stellen wat de korte- en langetermijneffecten van de maatregelen zullen zijn. Vervolgonderzoek is dan ook nodig om de verstoringsmaatregelen te evalueren op uitvoerbaarheid en vooral effectiviteit. Een goed startpunt kan zijn om te onderzoeken welke interventies in andere landen reeds zijn toegepast en welke (positieve en negatieve) effecten die interventies teweegbrachten. Een andere manier om de effectiviteit te toetsen is door experimenteel onderzoek hiernaar te verrichten.

6. Zorgplicht

Iemand kan een goed of dienst kopen als consument of particulier. 'Als consument' betekent dat die persoon zaken doet met een bedrijf; 'als particulier' betekent dat die persoon zaken doet met een andere particulier. In dit hoofdstuk geven we een overzicht van de wettelijke bepalingen inzake zorgplicht die van toepassing zijn op het moment dat iemand als consument of particulier te maken krijgt met fraude nadat hij via internet goederen of diensten heeft aangekocht. De vraag is dan of de tussenpersoon, in de zin van Internet Service Provider (ISP), bank, of Payment Service Provider, aansprakelijk gesteld kan worden voor de schade die de koper/afnemer van de dienst lijdt door de fraude van de tegenpartij. Het gaat hier om een internationale context, waarbij met name EU-recht en de uitleg ervan door het Hof van Justitie van de Europese Unie bepalend is. Daarbij kan op voorhand worden geconcludeerd dat de positie van de consument sterker is dan die van de particuliere koper. In geval van online fraude geniet de ISP een sterke bescherming tegen aansprakelijkheidsclaims van consumenten of particulieren. Bij banken lijkt er een tendens te zijn dat consumenten een sterkere positie hebben gekregen en dat banken een actief fraudebeleid dienen te hebben, willen ze vrijgesteld kunnen worden van aansprakelijkheid.
In dit hoofdstuk wordt gestart met het presenteren van de juridische basis voor de totstandkoming van een overeenkomst (par. 6.1) en hoe een overeenkomst tot stand komt langs elektronische weg (par. 6.2). Daarna wordt ingegaan op de aansprakelijkheid van de ISP bij online fraude (par. 6.3) en die van banken, iDEAL en PSPs (par. 6.4). Tot slot staat de aansprakelijkheidstelling bij een rechter of geschillencommissie centraal (par. 6.5).

6.1 De juridische basis voor de totstandkoming van een overeenkomst

De juridische basis voor het aangaan van overeenkomsten via internet, zoals koop en verkoop of het aangaan van een dienst, is in Nederland geregeld in Boek 3 en Boek 6 van het Burgerlijk Wetboek (BW). Is er sprake van consumentenkoop, dan is Boek 7.1 BW eveneens van toepassing.
Volgens art. 6:217 lid 1 BW komt een overeenkomst tussen partijen tot stand door een aanbod van de ene partij en de aanvaarding daarvan door de wederpartij. Dit heet wilsovereenstemming. Aanbod en aanvaarding zijn rechtshandelingen, omdat beide partijen een rechtsgevolg in het leven willen roepen, zoals de overdracht van eigendom van een artikel door de verkoper en de betaling ervan door de koper. Van belang hierbij is dat partijen in alle vrijheid de overeenkomst zijn aangegaan en dat er sprake is van

een wil en een daarmee overeenstemmende verklaring om de overeenkomst aan te gaan. Die verklaring moet duidelijk zijn gedaan en geen twijfel oproepen.
Het artikel moet de eigenschappen bezitten die de koper wil en waarover hij een verklaring heeft afgelegd (art. 3:33 BW). De verkoper geeft aan dat het artikel deze eigenschappen heeft. De verkoper heeft een mededelingsplicht en de koper een informatieplicht. Alvorens de overeenkomst tot stand komt en verbintenissen over en weer ontstaan, dienen de eigenschappen van het artikel door uitvoering van de informatie- en mededelingsplicht duidelijk kenbaar te zijn gemaakt, alsook de wil van beide partijen om een overeenkomst aan te gaan. Beide plichten maken onderdeel uit van de precontractuele fase, die gekenmerkt wordt door de goede trouw. In de precontractuele fase dienen partijen zich naar elkaar toe redelijk en billijk te gedragen (art. 3:11, 6:2 en 6:248 BW). Indien dit niet gebeurt en er ontstaat schade, dan kan sprake zijn van een onrechtmatige daad ingevolge art. 6:162 BW.
Mocht er sprake zijn van een discrepantie tussen wil en verklaring, omdat er sprake is van bijvoorbeeld een vergissing, dan wordt de wederpartij beschermd als er bij hem sprake is van een gerechtvaardigd vertrouwen (art. 3:35 BW) dat wil en verklaring overeenstemmen. Er komt dan toch een overeenkomst tot stand. Als een aanbod te mooi is om waar te zijn, dan dient doorgevraagd te worden of de verklaring wel overeenstemt met de wil en kan een beroep op art. 3:35 BW niet zonder meer worden aangenomen als het overduidelijk is dat er sprake is van een vergissing.[1]
Uitgangspunten bij het aangaan van een koopovereenkomst zijn dus een duidelijke wil en verklaring, maar ook gerechtvaardigd vertrouwen. Andere, algemene, uitgangspunten van het contractenrecht zijn (Timmer & Paffen, 2008):

- Contractvrijheid: partijen zijn vrij om overeen te komen wat ze willen zolang het niet in strijd is met de wet, goede zeden en openbare orde (art. 3:40 BW).
- Pacta sunt servanda: belofte maakt schuld: overeenkomsten moeten worden nagekomen. Dit principe hangt samen met de vrije wil van partijen. Als in alle vrijheid een overeenkomst tot stand komt, moet deze worden uitgevoerd.
- Vormvrijheid: de vorm waarin een overeenkomst wordt gegoten is eveneens vrij, tenzij anders is bepaald (art. 3:37 BW). Een overeenkomst mag mondeling, op papier, elektronisch of anderszins, tenzij de wetgever anders heeft bepaald. Dit is bijvoorbeeld het geval met de koop van een registergoed, waarvoor vormvereisten gelden.
- Redelijkheid en billijkheid: art. 6:2 BW bepaalt dat partijen verplicht zijn zich naar elkaar redelijk en billijk te gedragen. Binnen het verbintenissenrecht spelen beide begrippen een essentiële rol bij het aangaan van de overeenkomst, maar ook bij uitvoering ervan alsmede de uitleg van de overeenkomst indien partijen deze verschillend interpreteren.

1 Rechtbank Breda (vrz.) 31 januari 2007, ECLI:NL:RBBRE:2007:AZ7368. Zie ook: Blei Weissmann (2018).

6.2 De totstandkoming van een overeenkomst langs elektronische weg

Een belangrijk kenmerk van overeenkomsten die langs elektronische weg tot stand komen, is dat er sprake is van koop op afstand door middel van een elektronisch middel. De handel verloopt altijd via een derde partij, te weten een ISP, een platform dat toegang geeft tot het internet en dat daarmee elektronische handel mogelijk maakt. ISP's kunnen overal ter wereld hun diensten aanbieden. Dat maakt dat de handel op internet al vrij snel internationaal is. Dit is onderkend in de wetgeving en de Verenigde Naties en de Europese Unie hebben dan ook regels gesteld voor de handel via internet, die door de meeste landen, in ieder geval alle EU-lidstaten, zijn geïmplementeerd in hun nationale wetgeving.[2]
Indien we ons beperken tot internethandel in de landen van de Europese Unie, dan is hiervoor de basis Richtlijn 2000/31/EG.[3] Dat is de Europese Richtlijn inzake elektronische handel of kortweg de Richtlijn e-commerce. Deze richtlijn coördineert en harmoniseert voor alle lidstaten regels over de vrije vestiging van ondernemingen, de informatieplicht, commerciële communicatie, het sluiten van overeenkomsten langs elektronische weg, de aansprakelijkheid van dienstverleners die als tussenpersoon optreden en gerechtelijke en alternatieve geschillenbeslechting.[4]
De rode lijn hierin is de versterkte informatieplicht van de verkoper aan de koper. Door het op afstand kopen is het uitermate belangrijk dat de informatie van de verkoper zodanig (gedetailleerd) is, dat de koper zich een goed beeld kan vormen van het product. Deze informatie moet volledig en duidelijk zijn en niet tot zoektochten van de consument hoeven leiden. De wetgever heeft bepaald dat de informatie gemakkelijk, rechtstreeks en permanent kenbaar moet zijn op websites.[5] Dit betekent dat de informatie transparant moet zijn en dat de bezoeker van de website niet uitgebreid moet hoeven zoeken naar deze informatie. Volgens de memorie van toelichting (MvT) mag de dienstverlener geen obstakels plaatsen die rechtstreekse toegang verhinderen of de informatieverstrekking minder transparant maken. Dit kan het geval zijn als de toegang tot gegevens gebeurt langs opeenvolgende doorverwijzingen, de vereiste gegevens onoverzichtelijk worden gepresenteerd of een tegenprestatie wordt gevraagd voor het toegankelijk maken van de gegevens.[6] Een bekende zaak hierover is die van Ryanair

2 UNCITRAL Model Law on Electronic Commerce with Guide to Enactment 1996 with additional article 5bis as adopted in 1998, New York: United Nations 1999. Zie ook: *Kamerstukken II* 2001/02, 28 197, nr. 3, p. 3 en Van Esch (2004). Voor de EU is van toepassing Richtlijn 2000/31/EG, geïmplementeerd in de Aanpassingswet richtlijn inzake elektronische handel van 13 mei 2004. Voor consumenten is Boek 7 BW aangepast aan Richtlijn 97/7/EG bij wet van 21 december 2000 tot aanpassing van Boek 7 van het Burgerlijk Wetboek (Stb. 2000, 617), aangepast op 13 juni 2014 met de Implementatiewet richtlijn consumentenrechten (Stb. 2014, 140).
3 Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt, *PbEG*, L 178.
4 Art. 1 Richtlijn 2000/31/EG, Doel en toepassingsgebied. Zie ook: *Kamerstukken II* 2001/02, 28 197, nr. 3, p. 2-3.
5 Art. 3:15d lid 1 BW.
6 *Kamerstukken II* 2001/02, 28 197, nr. 3, Artikelen, p. 37.

die van het College van Beroep voor het bedrijfsleven (CBb) een boete kreeg voor het niet duidelijk vermelden van de prijsopbouw van de vliegtickets.[7]
Mochten koper en verkoper op het internet tot een koopovereenkomst komen, waarbij ook in deze elektronische omgeving wil en verklaring en het gerechtvaardigd vertrouwen de basis vormen, dan kan sprake zijn van fraude indien de zaak of de dienst niet wordt geleverd. Vaak is de verkoper in die gevallen, vooral in internationale handel, niet meer te traceren. De vraag is dan of de benadeelde partij uiteindelijk de ISP aansprakelijk kan stellen, omdat die toegang heeft gegeven tot het frauduleus handelen. De richtlijn heeft hierover regels gesteld, die geïmplementeerd zijn in art. 6:196c BW.

6.3 Aansprakelijkheid van de ISP bij online fraude

De tussenpersoon die een dienst van de informatiemaatschappij verleent, wordt in de wet min of meer beschouwd als een (passief) doorgeefluik dat het mogelijk maakt dat er kan worden gecommuniceerd en gehandeld langs elektronische weg. In de richtlijn wordt de rol van de verlener van de dienst van de informatiemaatschappij, en daarmee tussenpersoon, onderverdeeld in drie varianten, namelijk als 'mere conduit' (doorgeefluik = access provider), als 'cache' (tussentijdse en tijdelijke opslag van informatie = access provider) en als 'host' (opslag van informatie = hosting provider). In de richtlijn en het BW wordt de tussenpersoon (aangegeven als 'de verlener van een dienst van de informatiemaatschappij') gevrijwaard van aansprakelijkheid mits voldaan wordt aan bepaalde voorwaarden. Stol en Strikwerda (2017, p. 130) schrijven hierover: 'De mate van "onschendbaarheid" van providers in civielrechtelijke zin is afhankelijk van het soort dienst dat deze verleent (…).' In de richtlijn en in jurisprudentie is nadrukkelijk bepaald dat in principe van de tussenpersoon geen toezichthoudende taak wordt verlangd.[8]
De rode lijn in de jurisprudentie van art. 6:196c BW is dat hoe passiever en technischer de rol van de ISP is, hoe sneller hij een beroep kan doen op de vrijwaring van aansprakelijkheid. Art. 6:196c lid 4 BW bepaalt wanneer sprake kan zijn van aansprakelijkheid. Dat is niet het geval indien hij niet weet van een activiteit of informatie met een onrechtmatig karakter en, in geval van een schadevergoedingsvordering, niet redelijkerwijs ervan behoort te weten. Zodra de ISP echter achter de onrechtmatigheid van de activiteit of informatie komt, dient hij, om aansprakelijkheid te ontlopen, deze informatie prompt te verwijderen of de toegang ertoe onmogelijk te maken. Met name de ISP in zijn hoedanigheid van hosting provider laat zien dat stilzitten kan leiden tot aansprakelijkheid.
Volgens de wetgever kan de Service Provider gehouden zijn om maatregelen te treffen als hij ervan in kennis wordt gesteld dat een van de gebruikers van zijn computersysteem door middel van diens server onrechtmatig handelt.

7 CBb 10 mei 2016, 15/338, ECLI:NL:CBB:2016:103.
8 Art. 15 Richtlijn 2000/31/EG; HvJ 16 februari 2012, C-360/10 (SABAM/Netlog), ECLI:EU:C:2012:85.

'Van de Service Provider mag een zekere mate van zorg worden verwacht ten aanzien van het voorkomen van verdere inbreuk. Mede gelet op de omstandigheid dat de Service Providers bedrijfsmatig handelen, de mogelijkheid die hun ten dienste staat de toegang tot de home page af te sluiten en de schade die van verdere inbreuken het gevolg zou kunnen zijn, moet worden geoordeeld dat de Service Provider die ervan in kennis wordt gesteld dat een gebruiker van zijn diensten op diens home page auteursrechtinbreuk pleegt of anderszins onrechtmatig handelt, terwijl aan de juistheid van die kennisgeving in redelijkheid niet valt te twijfelen, zelf onrechtmatig handelt indien hij alsdan niet ingrijpt. Van de Service Provider mag dan worden verwacht dat hij de inbreukmakende documenten uit zijn computersysteem verwijdert en tevens dat hij aan de rechthebbende op diens verzoek de naam en het adres van de desbetreffende gebruiker bekend maakt.'[9]

Ofschoon het uitgangspunt dat een ISP in zijn algemeenheid slechts een technisch doorgeefluik is in het arrest van Hof Amsterdam wordt bevestigd, wordt internetprovider XS4ALL toch aansprakelijk gesteld voor de schade van de tegenpartij (Deutsche Bahn) omdat deze als 'host' had moeten begrijpen dat de betreffende informatie, waarnaar de tegenpartij verwijst en zegt er schade van te ondervinden, actief had moeten onderzoeken en uiteindelijk had moeten verwijderen. Door dat na te laten heeft hij in strijd met de hem betamende zorgvuldigheid en derhalve onrechtmatig jegens Deutsche Bahn gehandeld. Het ging hier om een publicatie van een gedetailleerde handleiding op websites over hoe treinverkeer op de Duitse spoorwegen kon worden gesaboteerd.[10]

In de zaak Stokke-Marktplaats eist Stokke dat Marktplaats voorafgaand aan de plaatsing van (particuliere) advertenties voor de verkoop van Tripp-Trapp kinderstoelen, deze controleert op inbreuk van het merkenrecht van Stokke. Hof Amsterdam bepaalt dat Marktplaats als hosting provider dit niet hoeft te doen. Geconstateerd wordt dat Marktplaats geen actieve, maar een neutrale rol speelt naar haar klanten-verkopers en potentiële kopers toe. Het hof constateert vervolgens dat Marktplaats een beroep kan doen op de vrijwaring van de aansprakelijkheid omdat Marktplaats prompt heeft gehandeld om inbreukmakende Stokke-advertenties te verwijderen, zodra zij daarvan kennis heeft gekregen of had behoren te krijgen.[11]

Het hof verwijst in deze zaak naar het arrest van het Hof van Justitie van de Europese Unie (HvJ) in de L'Oréal-eBay-zaak, waarin, kort gezegd, eveneens is bepaald dat een beroep op vrijwaring van de aansprakelijkheid niet opgaat wanneer de beheerder van de elektronische marktplaats, eBay in dit geval, had moeten weten van de onwettigheid van bepaalde verkoopaanbiedingen en niet prompt heeft gehandeld door de content te verwijderen.[12] Het hof past hiermee art. 6:196c lid 4 onder b BW toe.

---

9 Rechtbank Den Haag 4 juli 2001, ECLI:RBSGR:1999:AA1039. Zie ook *Kamerstukken II* 2001/02, 28 197, nr. 3, p. 49.

10 Hof Amsterdam 7 november 2002, ECLI:NL:GHAMS:2002:AF0091 (XS4ALL tegen Deutsche Bahn).

11 Hof Leeuwarden 22 mei 2012, ECLI:NL:GHLEE:2012:BW6296 (Stokke-Marktplaats).

12 HvJ 12 juli 2011, C-324/09 (L'Oréal e.a. tegen eBay), ECLI:EU:C:2011:474.

6.4 Aansprakelijkheid van banken, iDEAL en Payment Service Providers

De wetgever heeft in Boek 7 afdeling 3 BW de aansprakelijkheid van banken als tussenpersoon geregeld bij transacties tussen koper en verkoper.[13] Er geldt een zorgplicht, die afhangt van de omstandigheden van het geval, waarbij uit de jurisprudentie kan worden herleid dat een bijzondere zorgplicht aanwezig is als de bank op basis van bijzondere omstandigheden moet beseffen dat er sprake is van ongebruikelijke activiteiten en/of transacties en/of deze activiteiten strijdig zijn met de financieeltoezichtwetten. Als dan de bank niet voldoende onderzoek hiernaar heeft gedaan, is zij aansprakelijk voor de geleden schade. De bijzondere aansprakelijkheid ligt hiermee vooral in een onderzoeks- en waarschuwingsplicht.[14]
Alle banken hebben inmiddels beleid waarbij de klant redelijk wordt beschermd tegen cybercriminelen. Klanten krijgen via nieuwsbrieven ook regelmatig informatie over het beschermen van hun gegevens, bankrekeningen en hoe cybercriminelen te herkennen. Daarmee hanteren banken een actief informatiebeleid naar de klanten toe (expertinterview 1). Aansprakelijkstelling van banken door klanten die slachtoffer zijn geworden van buitenlandse online fraude kan via de geschillencommissie van het Klachteninstituut Financiële Dienstverlening (Kifid). Ook kan de bank via de burgerlijke rechter gedagvaard worden. Uitspraken van het Kifid tonen in zijn algemeenheid aan dat van banken een grote mate van alertheid en ondersteuning naar hun klanten toe mag worden verwacht. De informatieplicht drukt hierbij zwaar op banken. Het lijkt erop dat de klant, bij toepassing van de zorgplicht, bij banken een grotere bescherming krijgt dan in het algemene contractenrecht (Janssen, 2014).
Voor transacties die via iDEAL lopen, geldt eenzelfde lijn. iDEAL is in dit geval een zogenoemde Collecting Payment Service Provider. Daarnaast zijn er Payment Service Providers (PSP's). PSP's zijn bedrijven die online betaaloplossingen als iDEAL aanbieden; denk bijvoorbeeld aan Adyen.[15] Deze partijen vallen, als ze een vergunning hebben op grond van de Wet op het financieel toezicht (Wft), onder het toezicht van De Nederlandsche Bank en daarmee onder de (zorgvuldigheids)eisen van de Wft. Wat nieuw is, zijn de zogenoemde C2C (customer-to-customer)-betalingen die iDEAL recent heeft opengesteld, waarbij klanten via iDEAL kunnen betalen aan klanten. Voor C2B (customer-to-business)-betalingen via iDEAL – dus tussen bedrijven en klanten – zijn extra veiligheidswaarborgen toegepast. Bedrijven die gebruik willen maken van bijvoorbeeld iDEAL, worden vrij uitgebreid gescreend door iDEAL of de andere contractspartijen, wat de kans op fraude niet uitsluit maar wel vermindert.[16]
Voor C2C-betalingen lijkt dit lastig, waardoor fraude gemakkelijker gepleegd lijkt te kunnen worden. Ook hier zijn echter buffers tegen fraude ingebouwd door bijvoor-

13 Art. 7:542 t/m 7:548 BW.
14 Conclusie van 9 januari 1998, ECLI:NL:PHR:2015:1975 (MeesPierson/Ten Bos) en HR 23 december 2005, ECLI:NL:HR:2005:AU3713 (Safe Haven).
15 overOnlineBetalen (z.d.). *Payment Service Providers* Via: https://overonlinebetalen.nl/payment-service-providers/.
16 Zie: https://www.ideal.nl/ en https://www.internetkassa.nu/.

beeld te regelen dat geld alleen via een IBAN kan worden overgemaakt en/of door te betalen via de eigen bank waarbij gebruik wordt gemaakt van een https-omgeving, zijnde een versleutelde online omgeving. De C2C-betalingen lopen dan ook hoofdzakelijk via een derde partij (die gecertifieerd moet zijn, zoals Tikkie.me en iDEAL) en via banken, waardoor het beschermingsregime voor particulieren langs deze weg weer van kracht wordt. Ook bij C2C lopen betalingen via banken, waarbij een vrij sterke authenticatie is vereist.[17]

6.5 Aansprakelijkheidstelling bij de rechter of een geschillencommissie

In het burgerlijk recht dient de benadeelde partij zelf actie te ondernemen om haar rechten veilig te stellen. Dat kan bij de privaatrechtelijke rechter of via het indienen van een klacht bij een geschillencommissie. Wel is naar aanleiding van Richtlijn 2000/31/EG de Autoriteit Consument en Markt (ACM) opgericht met als doel ervoor zorg te dragen dat de algemene transparantie- en informatieverplichtingen uit art. 3:15d en 3:15e BW door het bedrijfsleven nageleefd worden. De ACM houdt, tezamen met toezichthouders van de Belastingdienst/FIOD-ECD, toezicht op de naleving van de bepalingen, hetgeen is geregeld in art. 3:15f BW en aanverwante wetgeving (Wet handhaving consumentenbescherming, Wet op de economische delicten).[18] Consumenten en particulieren kunnen bij de ACM met het indienen van een klacht ervoor zorgen dat er aandacht wordt gevraagd voor hun probleem.
Voor transacties waarbij banken als tussenpersoon fungeren, kan de consument terecht bij het Kifid voor problemen met financiële producten. Voorts is in art. 1 onder 4° Wet op de economische delicten overtreding van art. 3:15d en 3:15e BW strafbaar gesteld en kan dus aangifte worden gedaan bij de politie.
Voor alle vormen van aansprakelijkheid geldt dat ze worden beoordeeld aan de hand van het algemene leerstuk van de onrechtmatige daad op grond van art. 6:162 BW. Indien als gevolg van handelingen op het internet een partij schade ondervindt, kan hij de verlener van de dienst van de informatiemaatschappij verzoeken om hiertegen op te treden. Als dit niet of in onvoldoende mate wordt gedaan, kan de benadeelde partij naar de rechter stappen en via art. 6:162 BW zijn schade proberen aan te tonen en een maatregel verlangen, zoals blokkade van de site of verwijdering van de informatie. De benadeelde partij dient hierbij te bewijzen dat zijn belang is geschaad door de internetprovider, die jegens hem onrechtmatig handelt door in strijd te handelen met art. 6:196c lid 1, 2, 3 of 4 BW. Als de onrechtmatigheid wordt aangenomen kan de rechter toepassing geven aan de gevraagde maatregel zoals blokkering van de site of verwijdering van de informatie, al dan niet vergezeld gaande van een schadevergoeding. In art. 6:196c lid 4 onder b BW vindt deze zogenoemde notice-and-take-down (NTD)-procedure haar grond (zie ook par. 5.3).

17 Zie: https://www.consumentenbond.nl/.
18 De Fiscale Inlichtingen- en Opsporingsdienst (FIOD) en de Economische Controledienst (ECD) vormen samen de opsporingsdienst van de Belastingdienst.

Indien aangifte is gedaan bij de politie kan strafrechtelijk gezien het OM eisen dat gegevens ontoegankelijk worden gemaakt voor zover dit noodzakelijk is ter beëindiging van een strafbaar feit of ter voorkoming van nieuwe strafbare feiten. Een en ander is geregeld in art. 54a en 125o Sr (Wetboek van Strafrecht).[19]

Het juridische afwegingskader van de rechter bij een handhavingsverzoek of een dagvaarding bestaat uit de grondrechten van vrijheid van meningsuiting en informatie (art. 11 Handvest EU), recht op privacy (art. 7 Handvest EU), de vrijheid van ondernemning (art. 16 Handvest EU) en de bescherming van lichamelijke en geestelijke integriteit (art. 17 lid 2 Handvest EU). Er is geen rangorde binnen deze grondrechten, waardoor de rechter per geval zal moeten beoordelen welk grondrecht binnen de omstandigheden van het geval prevaleert (Van der Sloot, 2011).

In de conclusie van de advocaat-generaal (A-G) bij cassatiezaak van Stichting Brein jegens Ziggo, is in rechtsoverweging 7.20 te lezen, dat niet goed te voorspellen is hoe de afweging van de grondrechten in concreto zal uitpakken. Dit zal in belangrijke mate afhangen van de omstandigheden van het geval en hetgeen over en weer is gesteld. Hij vervolgt met te stellen dat de vrijheden hun grens vinden in hetgeen juridisch toelaatbaar is. In het geval van Stichting Brein/Ziggo, waarin de eerstgenoemde blokkering van de site van The Pirate Bay door Ziggo vordert, stelt de A-G dat de gevorderde blokkade moet worden afgewogen tegen de belangen van de vrijheid van ondernemerschap en vrijheid van informatie. De gevorderde blokkade mag deze rechten in de kern niet aantasten. Wanneer dat echter het geval is, is afhankelijk van de omstandigheden van het geval.[20]

Per geval zal dus moeten worden bekeken welk grondrecht prevaleert en in welke mate het grondrecht dient te worden beperkt. Daarbij gelden de algemene eisen van proportionaliteit en in geval van inbreuk van auteursrechten de overige eisen van art. 3 Handhavingsrichtlijn auteursrechten.[21] Zo heeft het HvJ in zijn prejudiciële uitspraak in de zaak UPC/Telekabel Wien bepaald dat een blokkade van een website mag, mits voldaan wordt aan drie eisen:

- De dienstverrichter tot wie het verbod is gericht, moet de technische middelen kunnen kiezen die worden gebruik om aan het verbod te voldoen. Hij mag aan het verbod ontkomen als hij kan aantonen dat hij hiertoe alle redelijke maatregelen heeft genomen. Deze eis komt tegemoet aan de vrijheid van ondernemerschap.
- De blokkeringsmaatregelen mogen geen nadelige gevolgen hebben voor gebruikers die rechtmatig toegang willen hebben tot de informatie van de website. Deze eis komt tegemoet aan de vrijheid van informatie.
- De blokkeringsmaatregel moet tot doel hebben de inbreuk op (in dit geval) auteursrechten te beëindigen en te voorkomen en moet redelijk doeltreffend zijn om dat doel na te streven.[22]

19 *Kamerstukken II* 2001/02, 28 197, nr. 3, par. 16, p. 27.
20 Conclusie van 16 maart 2018, ECLI:NL:PHR:2018:202, r.o. 7.20.
21 Richtlijn 2004/48/EG van 29 april 2004 betreffende de handhaving van intellectuele eigendomsrechten.
22 HvJ 27 maart 2014, C-314/12 (UPC tegen Telekabel Wien), ECLI:EU:C:2014:192; Conclusie van 16 maart 2018, ECLI:NL:PHR:2018:202, r.o. 7.7-7.9.

Een uitspraak waarin het zoeken naar de balans tussen alle betrokken grondrechten duidelijk wordt gemaakt, is de zaak SABAM/Netlog. Daarin bepaalt het HvJ in een prejudiciële uitspraak dat lidstaten een exploitant van een sociale netwerksite niet de plicht op mogen leggen om voor zijn gebruikers een filtersysteem te installeren, om daarmee te voorkomen dat auteursrechtelijke werken onrechtmatig worden gebruikt. Met een dergelijke verplichting wordt als het ware een toezichtverplichting geïntroduceerd, die in strijd is met de richtlijn.[23]

23 HvJ 16 februari 2012, C-360/10 (SABAM), ECLI:EU:C:2012:85.

7. Conclusie, discussie, beperkingen

In dit hoofdstuk staan we allereerst stil bij de conclusies (par. 7.1). De belangrijkste resultaten worden bediscussieerd en tegen het licht gehouden van reeds beschikbare kennis. Daarna worden de beperkingen van het onderzoek besproken (par. 7.2). Verspreid over dit hoofdstuk worden eveneens aanbevelingen gedaan voor vervolgonderzoek. Ten slotte worden enkele slotopmerkingen toegelicht in paragraaf 7.3.

7.1 Conclusies en discussie

In deze paragraaf worden de onderzoeksvragen beantwoord. Als eerste hebben we aandacht voor de stappen in de crimescripts voor aankoopfraude. Daarna geven we een overzicht van partijen die een rol spelen in deze crimescripts. Vervolgens volgt op hoofdlijnen een overzicht van verstoringsmogelijkheden. Daarna trekken we conclusies op basis van de juridische zorgplicht. Tot slot geven we antwoord op de hoofdvraag van het onderzoek.

7.1.1 *Uit welke stappen bestaan de crimescripts voor internationale aankoopfraude?*

In deze sectie geven we antwoord op de deelvraag uit welke stappen de crimescripts bestaan. Een essentiële stap in het welslagen van aankoopfraude is dat een slachtoffer en een fraudeur bijeenkomen. Meestal betekent dit dat een slachtoffer vanuit een bepaalde behoefte op zoek gaat naar een dienst of product en daarbij in contact treedt met een fraudeur. In dat geval heeft de fraudeur het initiatief genomen om een product of dienst aan te bieden op een online platform en reageert het slachtoffer daarop. Op basis van de dossierstudie vindt dit type crimescript in meer dan de helft van de gevallen plaats (55%). In de tweede meest voorkomende vorm van aankoopfraude (23%), hebben fraudeurs een valse webshop opgezet waarin zij bepaalde producten of diensten aanbieden. De derde meest voorkomende crimescript-categorie die we hebben gedestilleerd uit de dossieranalyse is dat een fraudeur de goede naam misbruikt van een particulier of zakelijke verkoper (13%). In mindere mate neemt een fraudeur contact op met het slachtoffer wanneer deze laatste het initiatief neemt door een gezocht-advertentie te plaatsen (4%).
Hierna worden per crimescript de basale stappen gepresenteerd. Het gaat hierbij om stappen die in drie van de vier, door Tompson en Chainey (2011) beschreven, 'scènes' van een crimescript plaatsvinden: *pre*-activiteiten, activiteit, en *post*-activiteiten. Ver-

volgens staan we stil bij aanvullende, meer gedetailleerde, stappen die genomen moeten worden om een fraudeaanval te laten slagen. Deze stappen behoren veelal tot de scène 'activiteit'. Op de eerste scène die Tompson en Chainey identificeren – voorbereiding – gaan we niet dieper in, omdat we daarover geen aanvullende informatie hebben bemachtigd. Een voorbereidingshandeling kan bijvoorbeeld zijn dat een fraudeur actie onderneemt om zijn of haar identiteit te verhullen. Daders maken dankbaar gebruik van de relatieve anonimiteit van het internet (Oerlemans, 2017). We hebben wel aandacht hiervoor als het gaat om handelingsstrategieën tegen aankoopfraude.

Crimescript 1: Advertentie plaatsen

Op de meest basale manier kan worden gesteld dat een beperkt aantal stappen nodig is om aankoopfraude te plegen. Voor de categorie 'advertentie plaatsen' gaat dit als volgt, zie tabel 7.1.

Tabel 7.1: Crimescript 'advertentie plaatsen'

Scène	Stap	Actie
Pre-activiteit	1.	De fraudeur plaatst een advertentie op een online platform
Activiteit	2.	Het slachtoffer reageert op de advertentie
	3.	Het slachtoffer maakt geld over
Post-activiteit	4.	De fraudeur incasseert het bedrag[1] *Mogelijke extra stappen*[2]
	5.	De fraudeur verwijdert de advertentie
	6.	De fraudeur heft het verkopersaccount op

1 Hoewel we hier, alsook bij de andere crimescripts, stellen dat 'de fraudeur' het geld rechtstreeks incasseert, is dat niet te bewijzen. Het kan namelijk zijn dat het geld wordt gestort op een bankrekening van een geldezel en dat de echte fraudeur het geld op andere wijze bemachtigt, al dan niet via verschillende tussenpersonen. Het kan voor de geldezel gunstig zijn om het geld zo snel mogelijk van de rekening te halen, voordat het wordt ontdekt en geblokkeerd. Echter, het slachtoffer staat te allen tijde met lege handen, omdat volgens de Nederlandse wet banken het geld niet mogen terugstorten en slachtoffers het bedrag niet kunnen storneren. Het geld kan alleen terug worden gestort in opdracht van de fraudeur zelf.

2 Indien het handelsplatform fraude constateert, dan is het veelal degene die de advertentie weghaalt en eventueel het account opheft.

Crimescript 2: Opzetten valse webshop

De tweede crimescript-categorie is complexer, omdat er een valse webshop is opgezet waarin fraudeurs bepaalde producten of diensten aanbieden, zie tabel 7.2. Dit betekent dat voor deze categorie meer stappen nodig zijn dan voor de eerste.

Tabel 7.2: Crimescript 'valse webshop'

Scène	Stap	Actie
Pre-activiteit	1.	De fraudeur bouwt een webshop
	2.	De fraudeur regelt de randzaken voor het opzetten en adverteren van een webshop
		a) De fraudeur registreert een domeinnaam
		b) De fraudeur koopt of huurt hostingruimte
		c) De fraudeur plaatst de webshop online
		d) De fraudeur adverteert voor de webshop[1]
Activiteit	3.	Het slachtoffer reageert op de advertentie
	4.	Het slachtoffer maakt geld over
Post-activiteit	5.	De fraudeur incasseert het bedrag *Mogelijke extra stap*[2]
	6.	De fraudeur ontmantelt de webshop (bijvoorbeeld om sporen te wissen)

1 Dit kan bijvoorbeeld door slimme zoekmachinemarketing toe te passen of een link naar de webshop te plaatsen op socialemediaplatformen (zoals Facebook) en advertentiewebsites (zoals Groupon).
2 Uiteraard kan de ontmanteling van de webshop ook geschieden buiten de macht van fraudeurs om, bijvoorbeeld middels een notice-and-take-down (NTD).

Crimescript 3: Misbruiken account

Voor het 'misbruiken account'-crimescript is ook complexer ten opzichte van het 'advertentie plaatsen'-crimescript. Fraudeurs maken hier misbruik van de naam van particulieren of bedrijven om zodoende op ogenschijnlijk betrouwbare wijze producten of diensten aan te bieden. Dit kan op twee manieren plaatsvinden, zie tabel 7.3.

Tabel 7.3: Crimescript 'misbruiken account'

Scène	Stap	Actie
Pre-activiteit	1.	De fraudeur misbruikt de naam van iemand anders
		a) De fraudeur hackt of koopt een verkopers-account met een goede rating[1]
		b) De fraudeur maakt een verkopersaccount aan op naam van een bedrijf[2]
	2.	De fraudeur zet een advertentie online op een online platform
Activiteit	3.	Het slachtoffer reageert op de advertentie
	4.	Het slachtoffer maakt geld over
Post-activiteit	5.	De fraudeur incasseert het bedrag *Mogelijke extra stap*[3]
	6.	De fraudeur verwijdert de advertentie

1 De wijze waarop dergelijke accounts gehackt zijn is niet naar voren gekomen uit onze data. Een mogelijkheid is dat inloggegevens afhandig zijn gemaakt (via social engineering) of zijn geraden. Een andere mogelijkheid is dat het e-mailaccount van een benadeelde is gehackt op technische wijze of dat het wachtwoord online is aangekocht. In een dergelijk geval kan iemand het verkopersaccount overnemen door via de betreffende omgeving het wachtwoord te resetten om het zodoende te kunnen aanpassen.
2 Dit is vooral het geval wanneer bedrijven zelf geen verkopersaccount dan wel een eigen website hebben.
3 Indien het handelsplatform (eventueel via de legitieme eigenaar van het account) fraude constateert, dan is het veelal degene die de advertentie weghaalt en mogelijk het account opheft.

Crimescript 4: Reageren zoekadvertentie

In het geval van 'reageren zoekadvertentie' zijn de stappen in het crimescript als volgt, zie tabel 7.4.

Tabel 7.4: Crimescript 'reageren zoekadvertentie'

Scène	Stap	Actie
Pre-activiteit	1.	Het slachtoffer plaatst een advertentie op een online platform
Activiteit	2.	Het fraudeur reageert op de advertentie
	3.	Het slachtoffer maakt geld over
Post-activiteit	4.	De fraudeur incasseert het bedrag *Mogelijke extra stap*[1]
	5.	De fraudeur heft het kopersaccount op

1 Indien het handelsplatform fraude constateert, dan is het veelal degene die het account opheft.

Aanvullende stappen om de aanval te laten slagen

De stappen die hierboven zijn beschreven, geven de hoofdlijnen weer. Omdat er veelal sprake is van contact tussen mensen, moesten fraudeurs soms aanvullende acties verrichten om het vertrouwen van hun (potentiële) slachtoffers te winnen of om foutieve beslissingen te forceren. Dit is ook bekend uit eerder onderzoek (o.a. Jansen, 2018; Van Wilsem, 2011). In andere gevallen verrichten fraudeurs aanvullende acties om slachtoffers aan het lijntje te houden, bijvoorbeeld om niet te snel betrapt te worden of om meer geld af te troggelen. Aanvullende acties zijn vooral nodig in de fase waar potentiële slachtoffers een advertentie zien en beoordelen, en in het contact met de fraudeur. Deze vallen dus binnen de scène 'activiteit'. Geld overmaken zonder enig contact met de fraudeur is logisch wanneer het valse webshops betreft, maar niet als het gaat om aankopen via bijvoorbeeld veilingsites. Deze aanvullende acties worden hierna besproken.

Vertrouwen winnen en foutieve beslissingen forceren. In sommige zaken viel het op dat benadeelden tegen beter weten in handelden, waarbij ze hun niet-pluis-gevoel negeerden. Om vertrouwen te winnen of de kans op het maken van foutieve beslissingen bij potentiële slachtoffers te vergroten, zetten fraudeurs beïnvloedingstechnieken in (Cialdini, 2009). Voorbeelden die naar voren zijn gekomen zijn: het wekken van urgentie of het inspelen op schaarste (bijvoorbeeld door aan te geven dat meer mensen geïnteresseerd zijn in een geadverteerde auto), het aanwenden van autoriteit (bijvoorbeeld documentatie overleggen die lijkt te komen van een overheidsinstantie) en het gebruik van het wederkerigheidsprincipe (het bieden van korting wanneer het te betalen bedrag in één keer wordt voldaan). Bij fraude door misbruik van de naam van legitieme partijen zagen we dat fraudeurs veelal de huisstijl en logo's kopiëren in de communicatie die plaatsvindt met het slachtoffer. Op dergelijke wijze is het moeilijker te beoordelen dat het een frauduleuze overeenkomst betreft. Ook werd soms een geldig KvK-nummer vermeld, dat vertrouwen wekte wanneer dit werd gecontroleerd. Een vals KvK-nummer kan ook vertrouwen wekken, omdat niet iedereen het KvK-nummer controleert op de website van de Kamer van Koophandel.

Ook was in één geval sprake van een 'framing-effect', waarbij fraudeurs slim misbruik maken van cognitieve 'biases' (in het menselijk denken). In dit geval werd de keuze om niet door te gaan met betalingen voor een auto gepresenteerd vanuit een 'loss frame'; 'als je dit niet doet, dan verlies je…'. Vanuit de psychologische literatuur weten we dat mensen de neiging hebben om risico's te nemen wanneer ze met potentiële verliezen worden geconfronteerd (Kahneman, 2011). Dit hangt samen met het beïnvloedingsprincipe commitment en consistentie (Cialdini, 2009). Als men eenmaal het eerste bedrag heeft overgemaakt, bijvoorbeeld voor de aanschaf van een auto, dan is het erg lastig om uit dat proces te komen, en gemakkelijk om ermee door te gaan.

Daarnaast wonnen fraudeurs veelal het vertrouwen van benadeelden door correcte communicatie. Fraudeurs kwamen vriendelijk en professioneel over en wisten vaak veel te vertellen over de betreffende producten die werden aangeboden. Fraudeurs probeerden soms ook proactief mee te denken met benadeelden, wat vertrouwd overkwam. Ook werd na een bestelling vaak een bevestiging gestuurd, en in sommige gevallen ter aanvulling een Track&Trace-code. Tevens werd veelal snel en adequaat gereageerd op vragen die benadeelden stelden. De communicatie vond op verschillende manieren plaats. Het viel op dat in een aantal zaken het contact tussen slachtoffer en dader zich buiten het platform begaf waar het initiële contact werd gelegd. Hierbij kan worden gedacht aan contact dat verliep via een gehackt Airbnb-account naar e-mail en contact via de chat van Marktplaats naar WhatsApp. Het is dan lastig voor dergelijke partijen om achteraf op te treden, omdat het contact buiten hun zicht is verlopen. Ook hadden fraudeurs soms contact met hun slachtoffers via een zelf gecreëerde chatmogelijkheid.

Aanvullend kwam in de fraudezaken met auto's naar voren dat fraudeurs sympathie probeerden te winnen door aan te geven zelf kosten te moeten maken. Hierbij wordt tevens ingespeeld op het wederkerigheidsprincipe, dat van invloed is op menselijk handelen (Cialdini, 2009). Ook werd aangedragen dat het versturen van een kopie van een identiteitsbewijs en het noemen van namen van contactpersonen door de 'verkoper' vertrouwen wekte.

Tevens werd vertrouwen gewonnen bij de wijze van betaling. Een belangrijke truc is om zogenaamd de betaling te laten verlopen via een escrow-dienst; een tussenpartij die de belangen van koper en verkoper behartigt, want wanneer een product of dienst niet bevalt, zal het geld netjes worden teruggestort. Een ander voorbeeld is het meegeven van referentienummers die in de beschrijving van de overschrijving gezet moeten worden. Het verrichten van betalingen via iDEAL kon ook rekenen op verhoogde betrouwbaarheid bij benadeelden.

Tot slot gaven enkele benadeelden aan dat er sprake was van vertrouwen in de aankoop, omdat een product of dienst op meerdere websites werd aangeboden. Tevens kwam het voor dat men geen wantrouwen had, omdat men niet verwachtte dat er fraude werd gepleegd met bepaalde producten, zoals e-readers en gitaren.

Aan het lijntje houden. Een tactiek van de fraudeur is om slachtoffers 'aan het lijntje te houden' of 'tijd te rekken', om zo minder snel betrapt te worden en meer geld te kunnen incasseren. Bij fraude met de aankoop van auto's werd bijvoorbeeld een verhaal opge-

houden dat de aanbetaling niet voldoende bleek en dat ook de rest van het bedrag voldaan moest worden. Fraudeurs verzochten dit bedrag over te maken met als argument om de auto verzekerd te laten vervoeren of om het vervoer door te laten gaan bij een grens.
Bij fraude via valse webshops zagen we dat de fraudeurs vertrouwen wonnen door een of enkele keren het product toe te sturen, en vervolgens niet meer. Dit ging om webshops waar men een abonnement kon afsluiten om periodiek luiers te ontvangen. Ook namen de 'pamperfraudeurs' moeite om gedupeerden uit te leggen waarom er geen of foutieve luiers waren geleverd, vermoedelijk om benadeelden aan het lijntje te houden en zodoende langer de website actief te houden, om meer consumenten te kunnen benadelen.

Andere opvallendheden. In het geval van fraude met auto's werden kopers verzocht om een kopie te versturen van een identiteitsbewijs, zoals paspoort en rijbewijs. Hoewel er sprake lijkt van identiteitsdiefstal, hebben we geen identiteitsmisbruik kunnen ontdekken in de verhalen van de benadeelden. Echter, sommige benadeelden ontvingen een paspoortkopie van een fraudeur, wat kan duiden op identiteitsmisbruik. Ook lijkt het erop dat persoonlijke omstandigheden of de context waarin het slachtoffer zich begaf verhoogd risico op slachtofferschap met zich meebrengen. Zo gaven sommige benadeelden aan te zijn overgegaan tot aankoop terwijl zij haast hadden. Daardoor waren zij vermoedelijk niet in staat om de aankoop goed te controleren. Tijdsdruk wordt dus niet alleen opgevoerd door fraudeurs (urgentie), maar is er soms ook door omstandigheden bij de benadeelden zelf. Tevens werd moeheid een keer genoemd, waarbij iemand een aankoop deed terwijl hij net een lange reis achter de rug had. Dergelijke contextuele factoren worden ook in ander onderzoek genoemd als mogelijke verklaringen voor slachtofferschap van online fraude (Jansen, 2018). Daarnaast zagen we dat mensen niet rationeel nadenken bij de aanschaf van producten die ze heel graag willen hebben (i.e. enthousiasme, hebberigheid, naïviteit). Tot slot zijn er mensen die bewust een risico willen lopen voor de kans op een mooie deal.

7.1.2 *Welke partijen zijn betrokken bij de crimescripts en welke rol vervullen zij bij de totstandkoming van het delict?*

In deze sectie besteden we aandacht aan de partijen die een rol spelen in de crimescripts. Overeenkomstig eerder onderzoek (Bloem & Harteveld, 2012), zagen we dat de meest voorkomende productcategorieën waarmee wordt opgelicht elektronica en auto's zijn. Hoewel verschillende actoren een rol spelen bij de verschillende productcategorieën, spelen sommige actoren altijd of in veel gevallen een rol. We beschrijven hier eerst welke actoren dat zijn. Daarnaast hebben we aandacht voor actoren die in mindere mate aan bod komen bij aankoopfraude vanuit het buitenland en staan we eveneens kort stil bij slachtoffers en daders.
Een essentiële actor in aankoopfraude is het (potentiële) **slachtoffer**. We weten, ook uit eerder onderzoek, dat slachtoffers met name in de midden en hoge opleidingscatego-

rieën zitten. Daarnaast zien we in onze data terug, hoewel deze niet per se representatief zijn, dat slachtoffers van alle leeftijden zijn en er geen onderscheid wordt gemaakt in sekse. Het lijkt er vooralsnog niet op dat fraudeurs zich expliciet richten op specifieke (kenmerken van) internetgebruikers. Dit suggereert dat iedereen tot op zekere hoogte gevoelig is voor slachtofferschap van aankoopfraude; een conclusie die overeenkomt met eerder onderzoek naar andere typen online fraude (o.a. Jansen & Leukfeldt, 2016). Mogelijk dat vervolgonderzoek aan de hand van andere kenmerken verklaringen kan vinden voor slachtofferschap. Om beleid te maken voor preventiedoeleinden is inzicht in welke groepen een hoger risico lopen om slachtoffer te worden belangrijk (Modic & Lea, 2011). Gerichte communicatie, door groepen specifieker te maken, zal voorlichting vermoedelijk relevanter maken dan ongerichte communicatie. Verschillende doelgroepen hebben verschillende voorkeuren aangaande hoe en waar informatie te ontvangen en manieren waarop ze informatie verwerken. Als echter blijkt dat slachtofferschap puur afhankelijk is van het frauduleuze aanbod dat een persoon net op een betreffend moment zoekt, dan is de vraag wat verder onderzoek naar slachtofferkenmerken nog kan opleveren. Het is dan wellicht interessanter om (de psychologie van) het keuzegedrag van slachtoffers nader te bekijken; waar en waarom neemt men de verkeerde afslag en hoe kunnen we die routes doorbreken? Voorlichting op het juiste moment (i.e. bij het nemen van beslissende acties) zou daarbij kunnen helpen. Daarnaast kan het interessant zijn om de mentale modellen van mensen in relatie tot online aankopen te bestuderen en te analyseren hoe die zich verhouden tot het nemen van voorzorgsmaatregelen (zie bijvoorbeeld Wash (2010)). Op die manier krijgen we beter zicht op bijvoorbeeld de capaciteit en motivatie van mensen; factoren die van invloed zijn op gedrag (Michie, Van Stralen & West, 2011).

Een tweede essentiële actor is de **dader**. Aannemelijk is dat het geld dat slachtoffers overmaken niet rechtstreeks naar de fraudeur gaat, maar naar een tussenrekening van een geldezel. In die zin kunnen aanbieders van tussenrekeningen (**geldezels**) en eventueel de **rekruteurs** daarvan ook worden aangemerkt als actoren in aankoopfraude.

Met name de plaats waar dader en slachtoffer elkaar online ontmoeten is belangrijk. De derde essentiële actor is het **online platform** dat de fraudeur gebruikt. Op basis van de dossierstudie concluderen we dat de meeste online oplichting die centraal staat in dit onderzoek wordt gepleegd via **online handels- en veilingsites**. Het gaat dan bijvoorbeeld om Marktplaats, eBay, Speurders en AutoScout24. Dit komt overeen met de routine-activiteitenbenadering: fraudeurs richten hun aanvallen op populaire online plaatsen. Daarbij geldt hoe meer bezoekers een handels- of veilingsite heeft, hoe groter het aantal potentiële slachtoffers. Dat de meeste slachtoffers worden gemaakt via Marktplaats, zegt in essentie dus niets over de (on)veiligheid van dat betreffende platform, maar meer over het gebruik ervan.

Daarnaast zagen we dat fraudeurs **legitieme websites** (via online fora) en **legitieme webshops** misbruiken om mensen op te lichten. Maar fraudeurs zetten ook zelf valse webshops op die worden gebruikt om internetgebruikers geld afhandig te maken. Voor vervolgonderzoek is het interessant om te kijken hoe valse webshops die geen producten leveren zich verhouden tot valse webshops die nepproducten verkopen. Daar is in

dit onderzoek geen aandacht aan besteed. Bij valse webshops spelen **hostingbedrijven** en **Internet Service Providers** een faciliterende rol om de website in de lucht te houden, evenals **organisaties voor de registratie van domeinnamen**. In het verlengde hiervan spelen tevens **online aanbieders van verhuur- en vakantiewoningen** een rol. Een vrij recente ontwikkeling is dat fraudeurs zich wenden tot sociale media om slachtoffers te maken (o.a. Facebook en Instagram). Dus ook **sociale media** spelen een rol in aankoopfraude.
Een volgende essentiële actor is de **bank**. In alle gevallen die we hebben bestudeerd is een belangrijk motief voor de fraudeur het geldelijk gewin, wat overeenkomt met eerder onderzoek (Conradt, 2012). Dit betekent dat het slachtoffer geld moet betalen. Onze data tonen dat dit altijd via het elektronisch betalingsverkeer plaatsvindt. In de meeste gevallen is dat via overschrijving gegaan, wat maakt dat banken belangrijke actoren zijn.[1] In enkele gevallen spraken benadeelden van overboekingen via iDEAL. Dat betekent dat ook **(Collecting) Payment Service Providers** actoren zijn in aankoopfraude. In het verlengde daarvan kwam in een van de slachtofferinterviews naar voren dat een benadeelde deels schadeloos is gesteld door zijn rechtsbijstandsverzekeraar. Interessant hier is om te kijken of schadeloosstelling voortvloeit uit een rechterlijke uitspraak of dat er is geschikt tussen partijen. Vervolgonderzoek kan ook uitwijzen of daders van aankoopfraude vanuit andere motieven handelen dan financiële.
Wanneer we het hebben over oplichting met auto's, hoorden we in de verhalen van benadeelden dat fraudeurs een transportbedrijf inzetten om de auto's te vervoeren. Deze bedrijven kunnen zijn verzonnen, maar het kan ook zijn dat de naam van een bestaand bedrijf wordt misbruikt. Dus transportbedrijven of, meer algemeen, **bezorgingspartijen** wiens naam wordt misbruikt zijn actoren in aankoopfraude. Voornamelijk bij het transport van auto's, maar ook bij het versturen van andere producten, werd soms gebruikgemaakt van een **Track&Trace-code**, waarvan sommige leken te werken. De **softwareontwikkelaars** hiervan spelen (onbedoeld) een rol in het fraudeproces.
Niet alleen de naam van bezorgingspartijen wordt misbruikt in aankoopfraude zaken. Dit geldt ook voor **escrow-diensten** in relatie tot betalingen. Tot slot speelt de **Kamer van Koophandel** onbedoeld een rol, omdat KvK-nummers van bestaande of recent failliete bedrijven worden misbruikt of valse KvK-nummers worden gebruikt.

7.1.3 *Welke handelingsstrategieën tegen internationale aankoopfraude kunnen worden geïdentificeerd, anders dan opsporing?*

In deze sectie worden drie categorieën van handelingsstrategieën tegen internationale aankoopfraude gepresenteerd. We beschrijven deze op hoofdlijnen om herhaling zo veel mogelijk te voorkomen. Aan het einde van deze sectie vatten we de belangrijkste

1 Indien bij aankoopfraude is betaald met de creditcard wordt het bedrag vergoed door de creditcardmaatschappij. Dit is mogelijk een reden om geen aangifte te doen en dat kan verklaren waarom in de dossieranalyse alleen aangiften gevonden zijn met overschrijvingen.

kanttekeningen samen en presenteren we mogelijkheden hoe deze getackeld kunnen worden.
Voordat we ingaan op de handelingsstrategieën, willen we nog even in herinnering brengen dat de in hoofdstuk 5 geïdentificeerde maatregelen niet het eindpunt zijn in de aanpak van internationale aankoopfraude (zie par. 5.6). Ze volgen uit ons onderzoek als de volgende stappen die kunnen worden gezet in het beheersen van deze criminaliteitsvorm.

Categorie 1. De eerste categorie handelingsstrategieën is gericht op klanten/consumenten, ofwel de potentiële slachtoffers. Criminelen maken gebruik van psychologische trucs om mensen over de streep te trekken in een fraudepoging. Bij het doen van online aankopen kunnen kopers maatregelen nemen om slachtofferschap te voorkomen. Door online weerbaar te zijn kunnen kopers zichzelf zo veel mogelijk beschermen. Specifiek bij het doen van online aankopen wordt aangeraden om aankopen te doen via officiële partijen. Indien een aankoop wordt gedaan met een onbekende verkoper of webshop kunnen kopers zichzelf beschermen door vóór de aanschaf controles uit te voeren, bijvoorbeeld op de verkopende partij. Indien de koper overgaat tot aanschaf, wordt geadviseerd om gebruik te maken van vertrouwd betalen, waardoor het geldbedrag pas wordt overgemaakt zodra het product of de dienst is geleverd.
Om ervoor te zorgen dat mensen online weerbaar zijn (en blijven), moeten ze zich bewust zijn van de risico's bij online aankopen en deze kunnen herkennen. Juist handelen op het juiste moment is daarbij essentieel. Digitale weerbaarheid gaat niet om het elimineren van risico's, maar om het managen daarvan (Jansen, 2018). Om aankoopfraude te verstoren is het dan ook belangrijk om het fraudebewustzijn te vergroten: kopers moeten zich bewust zijn van risico's bij online aankopen en weten welke beschermingsmaatregelingen zij kunnen nemen. Het vergroten van fraudebewustzijn kan door middel van bewustzijnscampagnes en weerbaarheidsprogramma's, bijvoorbeeld door online handelsplatformen en de overheid. Bijna alle experts benoemen bewustzijnscampagnes als verstoringsmaatregel, maar benoemen tegelijkertijd dat de effectiviteit hiervan momenteel laag is. Mensen reageren niet op de voorlichting of worden hier niet tijdig aan blootgesteld, waardoor ze pas op de hoogte zijn van fraudepraktijken na hun slachtofferschap. Hier kan rekening mee worden gehouden door de betreffende voorlichting op de juiste plek en tijd te tonen aan de juiste mensen. Vervolgonderzoek is nodig om inzichtelijk te maken hoe dergelijke online bewustzijnscampagnes en weerbaarheidsprogramma's het beste ingericht kunnen worden. Daarnaast lijkt het belangrijk om onderzoek te doen naar preventie van herhaald slachtofferschap. Herhaald slachtofferschap kwam onder bijna de helft van de interviewkandidaten naar voren. Mogelijk geldt dit voor meer slachtoffers van aankoopfraude. De vraag is hoe deze doelgroep het beste kan worden bediend om herhaald slachtofferschap te voorkomen.
Zojuist hadden we het over klanten/consumenten met het oog op hun eigen weerbaarheid. Klanten/consumenten kunnen langs nog een andere weg in actie komen tegen aankoopfraude: ze kunnen wanneer zij mogelijk frauduleuze praktijken waarnemen

een beroep doen op de zorgplicht van andere partijen zoals ISP's, online handelsplaatsen en financiële instellingen. Die hebben namelijk een zorgplicht (zie hoofdstuk 6) wanneer zij kennis dragen van malafide praktijken die worden gepleegd met behulp van hun voorzieningen. Wanneer klanten/consumenten situaties melden die fraude met behulp van die voorzieningen doen vermoeden, stimuleren zij de betreffende partijen om daartegen in actie te komen, want wanneer zij eenmaal weten van de malafide praktijk, hebben zij ook een verantwoordelijkheid daarvoor. Ook organisaties die de belangen van consumenten vertegenwoordigen kunnen in deze zin een rol spelen.

Categorie 2. De tweede categorie handelingsstrategieën is gericht op betrokken partijen en brancheorganisaties. Aankoopfraude kan worden verstoord indien criminelen en potentiële slachtoffers geen mogelijkheid hebben om online bijeen te komen (een essentiële stap in de werkwijze van fraudeurs). Om de toenadering tussen de crimineel en het potentiële slachtoffer moeilijk te maken, kunnen betrokken partijen eraan bijdragen dat: (1) geen nieuwe frauduleuze accounts, advertenties en webshops worden aangemaakt, (2) bestaande frauduleuze accounts, advertenties en webshops worden verwijderd en (3) misbruik van legitieme accounts, advertenties en webshops wordt voorkomen en gestopt.
De betrokken partijen kunnen bijdragen aan deze verstoring door (betere) identificatie en verificatie. Online handelsplatformen kunnen (ver)kopers identificeren en verifiëren om het voor criminelen moeilijk te maken om (langdurig) misbruik te maken van accounts/advertenties en fraude te plegen. Organisaties die domeinnamen registreren kunnen de identiteit van hun domeinhouders identificeren en verifiëren om valse webshops of misbruik van reeds legitieme webshops tegen te gaan. Financiële instellingen kunnen hun gebruikers beter identificeren en verifiëren om misbruik van rekeningnummers tegen te gaan. Door betere identificatie van accounts, advertenties en webshops is het moeilijker voor criminelen om anoniem te handelen en daardoor moeilijker om door te gaan met frauduleuze praktijken.
Betrokken partijen kunnen ook bijdragen aan verstoring door frauduleuze accounts, advertenties en webshops te detecteren. Frauduleuze accounts en advertenties op online handelsplatformen kunnen gedetecteerd worden door het stimuleren van meldingen door gebruikers van verdachte of frauduleuze activiteiten. Deze stimulatie kan vorm krijgen middels een meldknop voor fraude (of verdachte zaken) op online handelsplatformen. Een ander hulpmiddel is het beschermen van bestaande accounts, die aantrekkelijk zijn voor criminelen om te misbruiken. Dit kan door middel van tweefactor-authenticatie bij het inloggen op een online handelsplatform. De anonimiteit van criminelen kan verstoord worden door gebruikers van VPN-verbindingen te weren van online handelsplatformen. Na detectie kunnen frauduleuze accounts, advertenties en webshops (via een notice-and-take-down-verzoek) verwijderd worden om de criminelen een voet dwars te zetten.

Categorie 3. De derde en laatste categorie handelingsstrategieën is gericht op een grensoverschrijdende, integrale aanpak. Een verstoringsmogelijkheid is het oprichten van

een Europese publiek-private samenwerking (PPS) tussen bedrijven en overheidsorganisaties. In deze Europese PPS kunnen informatie over frauduleuze werkwijzen, persoonsgegevens van fraudeurs, frauduleus gebruikte bankrekeningnummers en andere relevante informatie gedeeld worden. Door het delen van deze gegevens wordt het gemakkelijker voor de aangesloten partijen om preventief te handelen met als doel potentiële slachtoffers te beschermen en fraudeurs tegen te werken. Hiermee wordt tevens de pakkans van fraudeurs vergroot (reactief). Hoewel dit onderzoek de focus niet legt op de opsporing van internationale aankoopfraude, is het vergroten van de pakkans wel een belangrijke handelingsstrategie in de strijd tegen internationale aankoopfraude.

Kanttekeningen. Er zijn verschillende kanttekeningen benoemd die de effectiviteit van verstoringsmaatregelen onder druk zetten. We gaan hier in op drie belangrijke kanttekeningen die naar voren zijn gekomen en wat daar mogelijk aan gedaan kan worden. Deze kunnen worden samengevat in: (1) wetgeving, (2) tegenstrijdige belangen, en (3) tijd en geld.
Een van de moeilijkheden die werd genoemd in de expertinterviews is dat de AVG de samenwerking tussen organisaties beperkt wat betreft het delen van informatie. Hoewel vervolgonderzoek moet uitwijzen of dit gevoel terecht is, lijkt hier dus wat te winnen. Mogelijk kunnen voor fraudebestrijding afspraken worden gemaakt met de Autoriteit Persoonsgegevens die het delen van informatie voor dit doeleinde kan bevorderen.
Een andere beperkende factor is dat verschillende partijen verschillende belangen dienen. Zo ervaren banken bijvoorbeeld geen direct nadeel bij aankoopfraude. Aanbieders van handelsplatformen en webshops hechten bijvoorbeeld meer waarde aan commerciële belangen dan aan veiligheidsbelangen. Hoewel veiligheid als belangrijk thema wordt gezien, heeft dit niet de hoogste prioriteit. Mogelijk dat de overheid een aanjagende rol kan innemen om betrokken partijen op te roepen om meer actie te ondernemen op dit vlak.
Tot slot spelen zaken als tijd en geld een rol. De huidige concurrerende markt vraagt om snelle acties (aankopen/transacties/accounts aanmaken). Uitgebreide veiligheidsprocedures werken daarbij vertragend. Dit staat een effectief geachte maatregel zoals betere identificatie en verificatie bijvoorbeeld in de weg. Vanuit commerciële belangen zou verificatie en identificatie ook in het voordeel kunnen werken, wanneer een organisatie zich richt op gebruikers die betrouwbaarheid van online aankopen hoog in het vaandel hebben. Wanneer grote groepen mensen dit oppikken, zullen andere organisaties mogelijk volgen.

7.1.4 *In hoeverre hebben de betrokken partijen een juridische zorgplicht jegens potentiële slachtoffers?*

Gelet op de resultaten uit de deskresearch heeft een particulier of een consument die een op het internet gekocht(e) en betaald(e) artikel of dienst niet geleverd heeft gekregen een aantal mogelijkheden om zijn recht te halen.

Hij of zij kan een handhavingsverzoek indienen tegen de handelaar/fraudeur bij de Autoriteit Consument en Markt (ACM), die bestuursrechtelijk kan handhaven. Hij kan een klacht indienen bij een geschillencommissie. Hij kan ook bij de burgerlijke rechter een actie starten jegens de handelaar/fraudeur op grond van art. 6:74 BW (tekortkoming in de nakoming van een verbintenis c.q. wanprestatie) of op grond van art. 6:162 BW (onrechtmatige daad) indien er sprake is van fraude in de precontractuele fase. De kans op succes hangt af van de bewijskracht en de pakkans van de handelaar/fraudeur. Indien de eiser het bewijs redelijk eenvoudig en snel kan leveren, is inwilliging van de eis door de rechter geen probleem. Het grootste probleem vormt de pakkans van de handelaar/fraudeur. Ook al zou de eis ingewilligd zijn, indien de handelaar/fraudeur niet meer te traceren is, staat men met lege handen.

Het in geval van online fraude aansprakelijk stellen van de tussenpersoon, zoals een ISP (Internet Service Provider), bank of PSP (Payment Service Provider), is lastig. Voor een ISP geldt dat zowel de access provider als de hosting provider zich kan beroepen op de vrijstelling van aansprakelijkheid, mits voldaan wordt aan de voorwaarden in art. 6:196c BW. In feite betekent dit dat hoe passiever en technischer de dienst van een provider is, hoe eerder hij een beroep kan doen op de vrijstelling van aansprakelijkheid. Bij banken lijkt er een tendens te zijn dat consumenten een sterkere positie krijgen en dat banken een actief fraudebeleid dienen te hebben, willen ze een geslaagd beroep kunnen doen op vrijstelling van de aansprakelijkheid. Bij de PSP's geldt hetzelfde als ze vallen onder het toezichtregime van De Nederlandsche Bank, gebaseerd op de Wet financiële transacties. Indien dit niet het geval is, dient deze tussenpersoon hoe dan ook te voldoen aan de in het maatschappelijk verkeer vereiste zorgvuldigheid. In dat laatste geval betekent het dat het slachtoffer moet bewijzen dat er in zijn geval sprake is van maatschappelijke onzorgvuldigheid en dat maakt het lastiger voor het slachtoffer omdat er geen toezichthouder is, die een dergelijk bewijs kan steunen of kan overnemen.

Jurisprudentie laat zien dat de positie van de consument in deze aansprakelijkheidsvraagstukken vaak sterker is dan die van de particuliere koper (zie ook par. 6.1). De rechter kijkt per geval of sprake is van vrijstelling van de aansprakelijkheid of niet. Daarbij kijkt hij naar de omstandigheden van het geval en hetgeen over en weer is gesteld, waarbij tevens een afweging van belangen leidend is, maar ook de beginselen van proportionaliteit en subsidiariteit.[2]

Daarnaast spelen momenteel diversie kwesties omtrent regelgeving. Een voorbeeld daarvan is dat socialemediabedrijven meer moeten doen om te voldoen aan de EU-regels voor consumenten.[3] Hoewel we ons in dit onderzoek hebben beperkt tot de 'juridische' zorgplicht, is een belangrijke vraag hoe het zit met de 'maatschappelijke' zorg-

2 Bijvoorbeeld Rechtbank Amsterdam 14 mei 2013, ECLI:NL:RBAMS:2013:CA0350; Rechtbank Amsterdam 25 juni 2015, ECLI:NL:RBAMS:2015:3984; Rechtbank Zeeland-West-Brabant 21 september 2016, ECLI:NL:RBZWB:2016:5832; HR 25 november 2005, ECLI:NL:HR:2005:AU4019 (Lycos/Pessers); Rechtbank Midden-Nederland 16 december 2015, ECLI:NL:RBMNE:2015:8974, alle gebaseerd op Wijsman (2017).

3 EC (2018). *Social media companies need to do more to fully comply with EU consumer rules*. Via: http://europa.eu/rapid/press-release_IP-18-761_en.htm.

plicht. Het is interessant om verder te onderzoeken in hoeverre benadeelden denken dat de betrokken partijen een zorgplicht hebben en wat ze ervan vinden dat partijen dat al of niet hebben. In dit onderzoek hebben we enig anekdotisch bewijs gevonden dat ingeeft dat benadeelden veelal teleurgesteld zijn in het optreden van de betrokken partijen. Vervolgonderzoek kan daar meer uitsluitsel over geven.

7.1.5 *Hoe kan internationale aankoopfraude worden bestreden, anders dan met opsporing?*

Nu wordt de hoofdvraag van het onderzoek beantwoord. In het onderzoek zijn verschillende manieren geïdentificeerd die potentie hebben om aankoopfraude vanuit het buitenland te verstoren.[4] Om de hoofdvraag te beantwoorden dragen we op basis van de hiervoor besproken reeks maatregelen drie strategieën aan die blijkens dit onderzoek kansrijk zijn om het probleem terug te dringen:

- toetsen effectiviteit weerbaarheidsprogramma's;
- versterken controles;
- versterken Europese samenwerking.

De eerste strategie is gericht op klanten/consumenten. Internetters weerbaarder maken is geen nieuw actiepunt. Er zijn verschillende voorlichtingscampagnes en talloze lijstjes met tips en tricks om veilig te handelen op internet. Het is daarom aanbevelenswaardig om onderzoek te doen naar de effectiviteit van (de combinatie van) maatregelen die gericht zijn op de gebruiker. Daarbij is het interessant om te onderzoeken wat het effect is van maatregelen die door meerdere afzenders worden onderschreven en gecommuniceerd (bijvoorbeeld door de politie én Marktplaats). De verwachting is dat de boodschap dan krachtiger is en beter blijft hangen. Tevens is het interessant om te onderzoeken wat de effecten zijn van gerichte maatregelen, bijvoorbeeld wanneer het gaat om specifieke risicoproducten. Het is eveneens aan te bevelen nader te onderzoeken op welke wijze en op welke termijnen internetters geconfronteerd moeten worden met dergelijke maatregelen. Indien maatregelen of programma's al effect hebben, is de duur ervan soms slechts tijdelijk (Jansen, 2018).
De tweede strategie omvat het versterken van controles. Enerzijds is deze strategie gericht op bedrijven en bestaat in dat geval uit preventieve controle van verkopers. Deze controle zal moeten bestaan uit het onmogelijk maken van handelingsmogelijkheden van fraudeurs, fraudeurs eerder te identificeren, en ze dat te laten weten. Dit lijkt een veelbelovende weg waarlangs effectieve maatregelen genomen kunnen worden. Indien partijen om commerciële redenen en/of andere motieven daar niet voor openstaan of er geen belang bij hebben – en het dus niet haalbaar lijkt – zullen we moeten accepteren dat fraude in de hand gewerkt kan blijven worden. De vraag is echter of economi-

4 Dit onderzoek richt zich op online aankoopfraude 'vanuit het buitenland'. Hoewel geen expliciete focus is gelegd op handelingsstrategieën om nationale online fraude te bestrijden, gelden de verstoringsmogelijkheden die hier worden aangemerkt ook voor andere (online) fraudes. In die zin is het belang van ons onderzoek dus breder dan alleen aankoopfraude vanuit het buitenland.

sche of bedrijfsmatige motieven het uitgangspunt moeten zijn. Het gaat immers ook om maatschappelijke verantwoordelijkheid. Vervolgonderzoek naar met name de haalbaarheid en de praktische implementatie is dus aan te bevelen. Een belangrijke vraag om te stellen is bijvoorbeeld hoe de juridische zorgplicht van betrokken partijen, zoals hostingbedrijven, registrars en de Kamer van Koophandel, zich verhoudt tot hun breder op te vatten maatschappelijke verantwoordelijkheid.

Anderzijds behelst de tweede strategie het invoeren van echtheidskenmerken (of controles/checks) en richt zich daarmee op de overheid en eventueel brancheorganisaties. Het probleem is fundamenteel, want het gaat om de vraag hoe van twee identiek lijkende dingen kan worden bepaald welke echt is en welke niet. Daarnaast is fraude alleen op te lossen als mensen die zaken doen via internet identificeerbaar zijn, bijvoorbeeld middels e-identificatie. Het invoeren van echtheidskenmerken kan effectief zijn, omdat het bepaalde acties van fraudeurs moeilijker maakt c.q. aan het daglicht brengt. Ook kan het controle/toezicht door anderen stimuleren. Belangrijk hierbij is de toetsbaarheid van een dergelijk kenmerk – en het gemak daarvan – in bijvoorbeeld een openbaar register.

Hoe echtheidskenmerken in positie kunnen worden gebracht is een onderwerp van nader onderzoek, waarbij inspiratie is op te doen uit hoe in de analoge wereld met echtheidskenmerken wordt omgaan. Offline hebben we bijvoorbeeld identificatiepapieren met echtheidskenmerken, geld met echtheidskenmerken en gebouwen met echtheidskenmerken. Nu al deze onderdelen online zijn gegaan, is het ook zaak dat we in die wereld echtheidskenmerken hebben. De vraag is hoe we dat online opnieuw gaan regelen. Daarbij is het van belang om aandacht te hebben voor de digitaal-technologische kant van echtheidskenmerken; hoe kan dit technisch worden gerealiseerd zodat het (a) niet – of op zijn minst zeer moeilijk – misbruikt kan worden en tegelijkertijd (b) gebruiksvriendelijk is, bijvoorbeeld hoe deze zijn te herkennen en te controleren. Het is eveneens belangrijk om te bepalen wie hiervoor verantwoordelijk is, zodat hier ook daadwerkelijk aan gewerkt kan worden.

De derde strategie heeft betrekking op Europese initiatieven. Een publiek-private samenwerking (PPS) op Europees niveau lijkt kansrijk om aankoopfraude – en aangrenzende online fraudes – te verstoren. Ook Schoorens (2010) ziet een PPS als mogelijkheid voor een optimale en aanhoudende preventie en aanpak van fraude. Voor een effectieve bestrijding van fraude moet de samenwerking wel structureel en sterk zijn.

Het is handig wanneer er in Europa een centraal meldpunt is voor fraude – waar mensen niet alleen meldingen kunnen doen wanneer zaken zijn misgegaan, maar waar men ook een check kan uitvoeren bij vermoedens van frauduleuze praktijken. Dit meldpunt kan gezien worden als startpunt voor internationale PPS. Mogelijk kan het centrale meldpunt per land een dependance hebben (bijvoorbeeld in de vorm van een Fraudehelpdesk), wat lijkt op de organisatie van het ECC Netwerk. Daarnaast moet dit meldpunt er niet alleen zijn voor burgers, maar moet hierbinnen ook worden samengewerkt met opsporings- en andere belanghebbende organisaties (waaronder politiediensten, banken en hostingbedrijven), zoals het Europees Bureau voor Fraudebestrijding OLAF. Belangrijk is dat er goede vastlegging, verslaglegging en onderzoek

plaatsvindt. Hierbij kan onder andere worden gedacht aan het hanteren van eenduidige definities, dezelfde meetmethoden en het delen van 'good practices'.
Op die manier – dus middels een grensoverschrijdende, integrale aanpak – is de verwachting dat er (sneller) een vuist kan worden gemaakt tegen fraude op internet. Er moeten nog wel een aantal hordes worden genomen om dit te kunnen realiseren. Denk bijvoorbeeld aan grensoverschrijdende gegevensdeling. Vervolgonderzoek is dan ook nodig naar hoe dit gerealiseerd kan en moet worden. Mogelijk dat de politiek, of overheid in bredere zin, daarin een aanjagende rol moet spelen. De Financial Intelligence Unit (FIU) zou daarvoor mogelijk als voorbeeld kunnen dienen.[5] Om de preventie en aanpak van aankoopfraude vanuit het buitenland effectief te laten zijn, moeten alle betrokken partijen (nationaal en internationaal) hun verantwoordelijkheid nemen. Het voorkomen en bestrijden van deze problematiek moet worden beschouwd als teamsport.
Tot slot, proactieve verstorings- en preventiemogelijkheden moeten de voorkeur krijgen om fraude aan te pakken – boven opsporing – omdat het voorkomt dat mensen slachtoffer worden van fraude. Het is daarom belangrijk dat de politie – in samenwerking met partners c.q. betrokken partijen – continu op zoek gaat naar mogelijkheden om fraudeurs een voet dwars te zetten. De drie aangereikte strategieën geven een handvat daarbij. Dit onderzoek biedt een reeks maatregelen die gebruikt kunnen worden om elk van die strategieën uit te werken.

7.2 Beperkingen

Het onderzoek kent een aantal beperkingen. Eén beperking heeft betrekking op zowel de dossierstudie als op de reconstructie. Ons onderzoek is gebaseerd op zaken waarvan aangifte is gedaan en slachtoffers die aangifte deden. Omdat er vermoedelijk een groot 'dark number' is, hebben we een (grote) groep potentiële kandidaten dus niet bereikt of kunnen bereiken met onze uitnodigingen. Daarnaast kwam in verschillende expertinterviews de zogenoemde 'Chinese fraude' aan bod; fraude via valse webshops uit China of die in Chinese handen zijn. Dit hebben wij niet in onze data teruggezien. Vermoedelijk hebben we deze zaken gemist, omdat bij dergelijke aankopen gebruik wordt gemaakt van betaling via creditkaart. Mogelijk dat het vergoedingenbeleid van creditcardmaatschappijen benadeelden ervan weerhoudt om aangifte/melding te doen bij de politie. Bovendien richtten we ons in dit onderzoek op vier Europese landen. Een laatste beperking in dit verband is dat het LMIO is toegerust voor de 'eenvoudige' vormen van oplichting. Dit betekent dat in dit onderzoek geen inzicht is verkregen in de meer 'complexe' zaken. Ter aanvulling, om de aanpak van aankoopfraude te verbeteren is het wenselijk om meer zicht te krijgen op de prevalentie. Niet alleen in algemene zin, maar juist ook voor de verschillende verschijningsvormen ervan.

5 FIU-Nederland levert op (inter)nationaal niveau een bijdrage aan de bestrijding van witwassen en financiering van terrorisme. Zie: https://www.fiu-nederland.nl/.

Het LMIO merkt een zaak aan als zijnde 'vanuit het buitenland' wanneer de benadeelde geld heeft overgemaakt naar een bankrekeningnummer in het buitenland. Het kan zijn dat dit nummer toebehoort aan een geldezel en dat de oplichter of de fraudeur zich in Nederland begeeft. De vraag is dan in hoeverre er daadwerkelijk sprake is van online aankoopfraude 'vanuit het buitenland' of dat in bepaalde gevallen beter gesproken kan worden van online aankoopfraude waarbij het geld 'naar het buitenland' verdwijnt. Om dit beter te identificeren of te achterhalen kan het waardevol zijn om in de meldingsprocedure naar aanvullende informatie te vragen, bijvoorbeeld over IP-adres, provider, tijdstip oplichting, et cetera.

Een interessant thema voor vervolgonderzoek is waarom verdachten ervoor kiezen om gebruik te maken van een buitenlands bankrekeningnummer. Hebben ze daarmee bijvoorbeeld het idee om beter onder de radar van de politie te blijven? Of worden ze aangestuurd door buitenlandse criminelen? Dit is van invloed op de effectiviteit van interventies. Denk bijvoorbeeld aan detectie op buitenlandse IP-adressen of het waarschuwen van geldezels in het buitenland, waarbij dat laatste een stuk lastiger is te realiseren.

Een ogenschijnlijke beperking van de slachtofferinterviews is dat er geen laagopgeleide personen zijn geïnterviewd. Wij veronderstellen echter dat het ontbreken van benadeelden onder laagopgeleiden vooral komt doordat laagopgeleiden minder slachtoffer worden van aankoopfraude (CBS, 2017). Tevens is er sprake van een vrij grote non-response (70%). De interviews hadden overigens niet tot doel om een representatief beeld te schetsen van alle aanvalsstrategieën. Daarvoor is het aantal interviewkandidaten te laag. Deze beperkingen hebben overigens naar vermoeden geen grote invloed op de resultaten, gezien het doel van deze studie.

Hoewel we met verschillende experts van diverse organisaties hebben gesproken, hebben we in dit onderzoek niet alle perspectieven kunnen meenemen. Zo hebben we in paragraaf 3.3 besproken dat een aantal benaderde partijen geen gehoor heeft gegeven aan het verzoek voor een interview. Daarnaast zijn er nog andere partijen die mogelijk interessante inzichten hadden kunnen opleveren wat betreft de (on)mogelijkheden van verstoring, zoals het Centraal Meldpunt Identiteitsfraude en -fouten (CMI) en de Autoriteit Persoonsgegevens. Bij het verder uitwerken en implementeren van verstoringsmaatregelen is het gewenst dat ook deze partijen aan tafel zitten.

Wat opvalt in het theoretische deel over de juridische zorgplicht is dat bepaalde bronnen gedateerd lijken. Recentere bronnen zijn niet aangetroffen. Toch was bepaalde informatie uit deze bronnen relevant voor dit onderzoek, omdat het vraagstuk van bijvoorbeeld de onrechtmatige daad klassiek is en de problemen die Van der Sloot benoemt in zijn artikel uit 2011 nog steeds actueel zijn. Dit geldt ook voor het boek van Alberdingk Thijm uit 2004. De onderwerpen die hij bespreekt zijn vijftien jaar later

nog steeds toepasbaar. In het boek van De Vey Mestdagh e.a. (2008) is de basis van het IT-recht en de hieruit voortvloeiende jurisprudentie uitgelegd, wat nog steeds actueel is en waarop recentere jurisprudentie voortbouwt.

7.3 Slotwoord

'Als het te mooi is om waar te zijn…' Deze quote van een van de benadeelden waarmee het rapport begint, illustreert dat aankoopfraude weerbarstige problematiek betreft. Aankoopfraude vindt plaats doordat mensen (worden verleid om) verkeerde beslissingen (te) nemen. Mensen handelen veelal impulsief en maken – ondanks dat hun onderbuikgevoel hen waarschuwt dat iets niet helemaal in de haak is – foute keuzes. Hoewel we op basis van de besproken maatregelen drie strategieën aandragen die kansrijk zijn om het probleem terug te dringen, zijn we door het complexe karakter van de onderzochte problematiek genoodzaakt om de verwachtingen enigszins te matigen. We zijn immers sterk afhankelijk van de menselijke factor. Voor een gedragsverandering op maatschappelijk niveau is een lange adem nodig. Daarnaast kunnen toekomstige ontwikkelingen, zowel op het gebied van online dienstverlening (nieuwe mogelijkheden) als criminaliteitspreventie (waar criminelen zich vervolgens weer op aanpassen), ervoor zorgen dat er nieuwe zwaktes ontstaan of worden ontdekt die misbruikt kunnen worden om slachtoffers te maken. Hoewel dé oplossing waarschijnlijk niet bestaat, dragen we met dit onderzoek wel oplossingsrichtingen aan die kunnen bijdragen aan veiligere online handel, zowel op nationaal als internationaal niveau.

Literatuurlijst

Alberdingk Thijm, Chr. (2004). *Het nieuwe informatierecht: Nieuwe regels voor het internet*. Den Haag: Academie Service.

Alleweldt, F., Kara S., e.a. (2011). *Consumer market study on the functioning of e-commerce and Internet marketing and selling techniques in the retail of goods*. Berlijn: Civic Consulting.

Blei Weissmann, Y.G. (2018). *Groene serie Verbintenissenrecht (art. 6:227b BW, aant. 1 t/m 118; art. 6:217 BW, aant. 3.131.4)*. Deventer: Kluwer.

Bloem, B. & Harteveld, A. (2012). *Horizontale fraude: Verslag van een onderzoek voor het Nationaal dreigingsbeeld 2012*. Zoetermeer: Dienst IPOL.

Borwell, J. (2017). *Wie wordt de digitale beurs gelicht? De persoonlijkheids- en demografische kenmerken van e-fraudeslachtoffers vergeleken.* Leeuwarden/Apeldoorn: NHL Hogeschool/Politieacademie (bachelor-scriptie).

Borwell, J., Jansen, J. & Stol, W. (2018). Persoonlijkheidskenmerken van e-fraudeslachtoffers. *Tijdschrift voor Veiligheid, 17*, 54-65.

Bossler, A.M. & Holt, T.J. (2010). The effect of self-control on victimization in the cyberworld. *Journal of Criminal Justice, 38,* 227-236.

Bunt, H.G. van de, Kleemans, E.R., e.a. (2007). *Organized crime in the Netherlands: Third report of the Organized Crime Monitor (summary)*. Verkregen via: https://english.wodc.nl/binaries/ob252_summary_tcm29-66835.pdf

CBS (Centraal Bureau voor de Statistiek) (2017). *Veiligheidsmonitor 2016.* Den Haag: Centraal Bureau voor de Statistiek.

Choo, K-K.R. (2011). The cyber threat landscape: challenges and future research directions. *Computers & Security, 30*, 719-731.

Cialdini, R.B. (2009). *Influence: Science and practice (vijfde editie).* Boston: Pearson Education, Inc.

CIPFA (Chartered Institute of Public Finance & Accountancy) (2016). *The local government counter fraud and corruption strategy.* Government UK: CIPFA Counter Fraud Centre.

Clarke, R.V. (2004). Technology, crime and crime science. *European Journal on Criminal Policy and Research, 1*(10), 55-63.

Cohen, L.E. & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. *American Sociological Review*, *44*, 588-608.

Conradt, C. (2012). Online auction fraud and criminological theories: The Adrian Ghighina case. *International Journal of Cyber Criminology, 6*(1), 912-923.

Cornish, D. (1994). The procedural analysis of offending and its relevance for situational prevention. *Crime Prevention Studies, 3*, 151-196.

Cornish, D.B. & Clarke, R.V. (2003). Opportunities, precipitators and criminal decisions: A reply to Wortley's critique of situational crime prevention. *Crime Prevention Studies, 16*, 41-96.

Cross, C., Richards, K. & Smith, R.G. (2016). The reporting experiences and support needs of victims of online fraud. *Trends and Issues in Crime and Criminal Justice, 518*, 1-14.

De Vey Mestdagh, C.N.J., Dijkstra, J.J. & Huisjes, S.C. (2008). *ICT-recht voor de praktijk*. Groningen/ Houten: Wolters-Noordhoff.

Domenie, M.M.L., Leukfeldt, E.R., Wilsem, J.A. van, Jansen, J. & Stol, W.Ph. (2013). *Slachtofferschap in een gedigitaliseerde samenleving: Een onderzoek onder burgers naar e-fraude, hacken en andere veelvoorkomende criminaliteit*. Den Haag: Boom Lemma Uitgevers.

ECC (European Consumer Centres Network) (2017). *Fraud in cross-border e-commerce.* Ierland: ECC-Net.

Esch, R.E. van (2004). De aanpassingswet elektronische handel. *Computerrecht, 17*, 107-115.

Europese Commissie (2016). *Consumers' attitudes towards cross-border trade and consumer protection 2016*. Verkregen via: https://publications.europa.eu/en/publication-detail/-/publication/af6a3712-9e77-11e7-b92d-01aa75ed71a1/language-en.

Europese Commissie (2017). Special Eurobarometer 464a: Europeans' attitudes towards cyber security. Verkregen via: http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/Survey/getSurveyDetail/ instruments/SPECIAL/surveyKy/2171.

Geldrop, A. van & Vries, T. de (2011). *Fraude loont, de toekomst van fraude en ICT.* Den Haag: SST Academy.

Hadlington, L. (2017). Human factors in cybersecurity: Examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. *Heliyon, 3*(7), 3:e00346.

Halevi, T., Lewis, J. & Memon, N. (2013). A pilot study of cyber security and privacy related behavior and personality traits. *Proceedings of the 22nd International Conference on World Wide Web*, 737-744.

Hartel, P., Junger, M. & Wieringa, R. (2011). *Cyber-crime science = Crime science + information security.* Enschede: Universiteit Twente.

Hulst, R.C. van der & Neve, R.J.M. (2008). *High tech crime, soorten criminaliteit en hun daders: Een literatuurinventarisatie.* Den Haag: Boom Juridische Uitgevers.

Hutchings, A. & Hayes, H. (2009). Routine activity theory and phishing victimisation: Who gets caught in the net? *Current Issues in Criminal Justice, 20*, 433–451.

Inspectie Veiligheid en Justitie (2015). *Aanpak van internetoplichting door de politie*. Den Haag: Ministerie van Veiligheid en Justitie.

Jansen, J. (2018). *Do you bend or break? Preventing online banking fraud victimization through online resilience*. Heerlen: Open Universiteit (proefschrift).

Jansen, J. & Leukfeldt, E.R. (2016). Phishing and malware attacks on online banking customers in the Netherlands: A qualitative analysis of factors leading to victimization. *International Journal of Cyber Criminology*, *10*(1), 79-91.

Jansen, J. & Leukfeldt, E.R. (2018). Coping with cybercrime victimization. An exploratory study into impact and change. *Journal of Qualitative Criminology and Criminal Justice, 6*(2), 205-228.

Janssen, V. (2014). *De zorgplicht van banken: In het perspectief van de hoedanigheid van partijen*. Tilburg: Universiteit van Tilburg (master-scriptie).

Kahneman, D. (2011). *Thinking, fast and slow.* London, UK: Penguin Group.

Kigerl, A. (2012). Routine activity theory and the determinants of high cybercrime countries. *Social Science Computer Review, 30*(4), 470-486.

Klerks, P. & Kop, N. (2007). *Maatschappelijke trends en criminaliteitsrelevante factoren: Een overzicht ten behoeve van het Nationaal dreigingsbeeld criminaliteit met een georganiseerd karakter 2008 – 2012.* Apeldoorn: Politieacademie.

Kruisbergen, E.W., Bunt, H.G. van de & Kleemans, E.R. (2012). *Georganiseerde criminaliteit in Nederland: Vierde rapportage op basis van de Monitor Georganiseerde Criminaliteit*. Den Haag: Boom Lemma Uitgevers.

Kruisbergen, E.W., Leukfeldt, E.R., Kleemans, E.R. & Roks, R.A. (2018). *Georganiseerde criminaliteit en ICT: Rapportage in het kader van de vijfde ronde van de Monitor Georganiseerde Criminaliteit.* Den Haag: Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC).

Leukfeldt, E.R. (2016). *Cybercriminal networks: Origin, growth and criminal capabilities*. Den Haag: Eleven International Publishers (proefschrift).

Leukfeldt, E.R., Domenie, M.M.L. & Stol, W.Ph. (2010). *Verkenning cybercrime in Nederland 2009.* Den Haag: Boom Juridische uitgevers.

Leukfeldt, E.R. & Stol, W.Ph. (2011). *Internetoplichters uitgelicht: E-fraudeurs en klassieke fraudeurs vergeleken.* Leeuwarden: NHL Hogeschool.

Leukfeldt, E.R. & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. *Deviant Behaviour, 37*(3), 263-280.

Michie, S., Stralen, M.M. van & West, R. (2011). The behaviour change wheel: A new method for characterising and designing behaviour change interventions. *Implementation Science, 6*(1), 1–11.

Modic, D. & Lea, S.E.G. (2011). How neurotic are scam victims, really? The Big Five and internet scams. *Paper gepresenteerd op The 2011 Conference of the International Confederation for the Advancement of Behavioral Economics and Economic Psychology*. Exeter: Verenigd Koninkrijk.

NFA (National Fraud Authority) (2011). *The strategic plan to reduce fraud*. Verkregen via: https://www.gov.uk/government/publications/nfa-fighting-fraud-together

Ngo, F.T. & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, *5*(1), 773-793.

Oerlemans, J.J. (2017). *Investigating cybercrime*. Utrecht: SIKS (proefschrift).

OLAF (European Anti-Fraud Office) (2017). *The OLAF report 2017*. Luxemburg: Publications Office of the European Union.

Parrish, J.L., Baily, J.L. & Courtney, J.F. (2009). A personality based model for determining susceptibility to phishing attacks. *Decision Sciences*, 285-296.

Pratt, T.C., Holtfreter, K. & Reisig, M.D. (2010). Routine online activity and internet fraud targeting: extending the generality of routine activity theory. *Journal of Research in Crime and Delinquency, 47*(3), 267-296.

Reep, C. (2017). *Fraude met online handel. Antwoorden uit de veiligheidsmonitor vergeleken met het politieregister.* Den Haag: Centraal Bureau voor de Statistiek.

Reyns, B.W. (2015). A routine activity perspective on online victimisation: Results from the Canadian General Social Survey. *Journal of Financial Crime, 22*(4), 396-411.

Schoorens, G. (2010). *Naar een nationale strategische aanpak van de strijd tegen fraude.* Verkregen via: http://www.cass.be/parket/leuven/documenten/rapport_Schoorens_NL%20def.pdf

Sloot, B. van der (2011). De verantwoordelijkheid voorbij: De ISP op de stoel van de rechter. *Tijdschrift voor Internetrecht, 2011*(5), 136-140.

SOANP (2015). *Strategische onderzoeksagenda voor de Politie 2015-2019: Voor een effectievere politie en een veiligere samenleving*. Apeldoorn: Politieacademie.

Stol, W. & Strikwerda, L. (2017). *Strafrechtspleging in een digitale samenleving*. Den Haag: Boom Juridische uitgevers.

Timmer, I. & Paffen, A.L.A.M. (2008). *Verbintenissenrecht begrepen*. Den Haag: Boom Juridische uitgevers.

Tompson, L. & Chainey, S. (2011). Profiling illegal waste activity: Using crime scripts as a data collection and analytical strategy. *European Journal on Criminal Policy and Research, 17*(3), 179-201.

Veenstra, S., Zuurveen, R. & Stol. W. (2016). *Cybercrime among companies*. Den Haag: Eleven International Publishing.

Verhage, A. (2014). Op zoek naar financieel-economische criminaliteit. *Criminografische ontwikkelingen III: Van (victim) survey tot penitentiaire statistiek, 9,* 89-112.

Wash, R. (2010). Folk models of home computer security. In: *Proceedings of the 6th Symposium on Usable Privacy and Security* (pp. 1–16).

Weulen Kranenbarg, M. (2018). *Cyber-offenders versus traditional offenders: An empirical comparison.* Amsterdam: Vrije Universiteit (proefschrift).

Wijsman, A. (2017). De civielrechtelijke weg om digitale verspreider te achterhalen. *Tijdschrift voor Aansprakelijkheid- en verzekeringsrecht, 97*(4).

Wilsem, J. van (2011). Bought it, but never got it: Assessing risk factors for online consumer fraud victimization. *European Sociological Review, 29*(2), 168-178.

Bijlage I: Definities van aankoopfraude

Over aankoopfraude vanuit het buitenland is weinig literatuur voorhanden. Daarom is gekeken naar literatuur over overkoepelende en meer bekende vormen van fraude. Aankoopfraude kan (zonder verdere uitsplitsing) namelijk ook worden aangeduid als een vorm van online fraude, ('cross border') fraude in e-commerce of fraude met online handel.

Online fraude is bedrog met als oogmerk het behalen van financieel gewin, waarbij ICT essentieel is voor de uitvoering. Hiermee wordt ook wel 'internetfraude' of 'internetoplichting' bedoeld (Leukfeldt, Domenie & Stol, 2010; Leukfeldt & Stol, 2011). Hiervan is aankoopfraude een van de meest voorkomende vormen (Bloem & Harteveld, 2012). Het Wetboek van Strafrecht kent het begrip fraude niet. Wanneer op slinkse wijze geld afhandig wordt gemaakt is er volgens art. 326 Sr sprake van 'oplichting'.

Fraude in (cross-border) e-commerce is volgens het European Consumer Centres Network oplichting na het online aanschaffen van producten uit het buitenland (ECC, 2017). Dit wordt verder gedefinieerd als fraude gepleegd door middel van online winkelen of met gebruik van chats, e-mails of zelfs software. Dit kan te maken hebben met valse veilingen, creditcard- en pinpasfraude, chequefraude, identiteitsdiefstal, phishing en producten die niet worden geleverd. Ronduit de meest voorkomende fraudes met internationale e-commerce bestaan uit aankoopfraude en daarom wordt literatuur over fraude in e-commerce in het huidige onderzoek ook gebruikt.

De Nederlandse politie gebruikt fraude met online handel om aankoop- en verkoopfraude te beschrijven (Reep, 2017). Om verder te specificeren zijn de meeste aangiften van oplichting van fraude met online handel, waar goederen wel betaald en niet geleverd zijn, oftewel aankoopfraude (Bloem & Hartveld, 2012; CBS, 2017). Daarom kan ook literatuur over fraude met online handel betrokken worden in het huidige onderzoek.

Kortom, deze definities bevatten niet het begrip aankoopfraude, zoals gedefinieerd in het huidige onderzoek. Aangezien aankoopfraude, zoals in het huidige onderzoek gedefinieerd, wel het grootste deel van de bovenstaande definities betreft, is literatuur met bovenstaande definities wel gebruikt. Indien literatuur een van de bovenstaande definities betreft, is deze ook zo aangeduid in dit onderzoek.

Bijlage II: Interviewprotocol benadeelden

Introductie

Wie zijn wij en wat gaan we doen

Waarom dit interview
De Onderzoeksgroep Cybersafety (NHL Stenden Hogeschool en de Politieacademie) voert onderzoek uit naar aankoopfraude vanuit het buitenland. Door met mensen in gesprek te gaan die te maken hebben gehad met deze fraudevorm willen we beter inzicht krijgen in het fraudeproces, zoals door het slachtoffer beleefd. Specifiek willen we daarbij inzichtelijk maken hoe daders te werk gaan en hoe deze fraudevorm kan worden voorkomen anders dan met opsporing. Aan de hand hiervan kunnen aanbevelingen worden gedaan aan consumenten die online aankopen doen, maar ook aan organisaties die dit faciliteren of daarin op andere wijze een rol spelen, zoals de politie. Dit heeft als groter doel om het aantal fraudezaken in de toekomst terug te brengen. Wij voeren dit onderzoek uit in opdracht van het programma Politie & Wetenschap en in samenwerking met het LMIO.

Belangrijk
Op specifieke vragen hoeft u – indien gewenst – geen antwoord te geven.

Wat doen we met de informatie uit het interview
We schrijven een onderzoeksrapport en daarnaast wetenschappelijke artikelen. Alle gegevens worden vertrouwelijk behandeld en anoniem verwerkt. Er zullen geen op de persoon herleidbare zaken in deze eindproducten worden opgenomen.

Opname
Vindt u het goed dat het gesprek wordt opgenomen? De opnames worden alleen gebruikt voor het uittypen van het gesprek en worden daarna gewist. Met name bij de open antwoorden is het van belang dat het antwoord van de respondent juist wordt weergegeven. Dit kan alleen door de antwoorden letterlijk op te schrijven tijdens het interview of door het gesprek op te nemen en later uit te werken. Deze laatste optie zorgt ervoor dat het interview zonder onderbrekingen kan worden afgenomen en uiteindelijk sneller kan worden afgerond.

Introductievragen

Als eerste wil ik u graag een aantal algemene vragen stellen met betrekking tot het gebruik van internet en het doen van online aankopen.

1. Hoe lang maakt u ongeveer gebruik van internet? (schatting in jaren)

2. Hoe frequent doet u online aankopen? (dagelijks, wekelijks, maandelijks, jaarlijks, sporadisch)
   a) In hoeverre is deze frequentie veranderd naar aanleiding van het incident?

3. Wat is uw algemene ervaring met betrekking tot het doen van online aankopen?
   a) In hoeverre is dit veranderd naar aanleiding van het incident?

4. In hoeverre vindt u het doen van online aankopen veilig?
   a) In hoeverre is dit veranderd naar aanleiding van het incident?

Slachtofferschap

Een van de aanleidingen om met u in gesprek te gaan is het feit dat u slachtoffer bent geworden van online aankoopfraude. Ik wil u nu een aantal vragen stellen over dit incident.

5. Kunt u in uw eigen bewoording uitleggen wat er volgens u is gebeurd?
(*De onderstaande elementen dienen in ieder geval aan bod te komen*)
   a) Wanneer heeft het incident plaatsgevonden?
   b) Via welk platform begon de aanval? (handelssite, webshop, sociale media, etc.)
   c) Welk productcategorie werd aangeboden? (elektronica, vakantiewoning, auto, etc.)
   d) Op welke wijze wonnen de criminelen uw vertrouwen? (bij iedere stap in het proces)
   e) Welke factoren speelden volgens u de belangrijkste rol waarom u meewerkte? (waarom was de fraude succesvol)
   f) Waren er momenten waarop u twijfelde aan de echtheid? (product, verkoper)
      i) Waaruit bleek dat?
      ii) Waarom gevoel niet gevolgd?
   g) Hebt u vooraf of naderhand de verkopende partij en/of het goed gecontroleerd, bijvoorbeeld op betrouwbaarheid, heling?
      i) Waarom wel? (op welke wijze, via welk kanaal)
      ii) Waarom niet? (bijvoorbeeld onbekend mee)
   h) Op welke wijze(n) werd gecommuniceerd? (systeem van betreffende platform, e-mail, telefoon, sms, WhatsApp, combinatie, anders)

i) Deed de crimineel zich voor als een particulier of als bedrijf?
   i) Uit eigen naam, of uit naam van een ander (identiteitsmisbruik)?
j) Gaf de crimineel aan in welk land hij/zij zich bevond?
k) In welke taal is gecommuniceerd?
l) Hebt u enig idee of de crimineel alleen werkte, of dat het ging om meerdere personen? (criminele groepering)
m) Op welke wijze hebt u geld overgemaakt naar de crimineel?
   i) Viel daarbij iets op? (bijvoorbeeld wel of juist niet via bepaalde betaaldienst, via een derde partij)
   ii) In hoeverre hebt u het bedrag in delen moeten betalen?
n) In hoeverre was er sprake van contact nadat u de betaling had verricht?
o) Hoe hebt u geconstateerd dat het mogelijk om fraude ging? (of bent u door iemand anders hierop geattendeerd)

6. Waarom denkt u dat u slachtoffer bent geworden?
   a) Wist u voorafgaande aan het incident dat u hiervan slachtoffer kon worden?
   b) Kunt u aangeven hoe groot u voorafgaande aan het incident de kans inschatte om slachtoffer hiervan te worden? (heel groot, groot, neutraal, klein, heel klein)
      i) Waarom? Hoe is dat nu?
   c) Hoe schatte u vooraf de impact hiervan in? (heel groot, groot, neutraal, klein, heel klein)
      i) Waarom? Wat konden volgens u de mogelijke gevolgen zijn van online aankoopfraude? Hoe is dat nu?
   d) Zijn er volgens u andere redenen waarom/waardoor u slachtoffer bent geworden?
   e) Hebt u een dergelijk incident in het verleden eerder meegemaakt?
      i) Zo ja, hoe lang is dat ongeveer geleden? Hoe kon het opnieuw gebeuren?

7. Wat voor impact heeft dit incident op u gehad?
   a) *Financieel*. Wilt u vertellen om wat voor schadebedrag het ging? Is het schadebedrag op een of andere manier vergoed?
   b) *Psychologisch/emotioneel*. In hoeverre heeft het incident voor u impact op psychologisch of emotioneel vlak? (bijvoorbeeld verminderd vertrouwen, geschrokken, boos, onzeker, hulpeloos)
   c) *Identiteitsfraude*. In hoeverre heeft het incident nasleep gehad, bijvoorbeeld dat uw identiteit is misbruikt?

8. Kunt u in uw eigen bewoording uitleggen wat hebt u gedaan toen u besefte te zijn opgelicht?

(De volgende elementen dienen in ieder geval aan bod te komen)

   a) Met welke partijen hebt u contact gehad? (nationaal/internationaal; belangrijkste redenen)
   b) In hoeverre contact gehad/proberen te leggen met en/of data verzameld over verkopende partij? (zelf, via vrienden, etc.)

c) Wat was voor u de belangrijkste reden om hiervan aangifte te doen bij de politie?
d) In hoeverre is uw zaak door de politie (of andere organisatie) opgepakt?
   i) Wat stemt u positief, wat stelt u teleur?

Preventie

9. Had het incident volgens u voorkomen kunnen worden?
   a) Op welke wijze?
      i) Wat had u nu anders gedaan?
   b) Welke andere partijen zouden daar een rol in moeten hebben? (platform, politie)
      i) Waarom? Hoe ziet die rol eruit?

10. Kunt u een dergelijk incident in de toekomst voorkomen?
    a) Welke maatregelen zou u nemen om in de toekomst dergelijke incidenten te voorkomen?
    b) Hoe groot schat u de kans dat het weer gebeurt? (heel groot, groot, neutraal, klein, heel klein?)
       i) Waarom? Wat denkt u dat de impact zal zijn? (groter, hetzelfde, lager)

11. In hoeverre kan de veiligheid van online aankopen volgens u worden verbeterd?
    a) Wat kunnen klanten zelf doen? Welke tip is het belangrijkst en waarom?
    b) Wat kan de politie doen? Welke tip is het belangrijkst en waarom?
    c) Wat kunnen andere partijen doen? Welke tip is het belangrijkst en waarom?
    d) Waar ligt volgens u de belangrijkste verantwoordelijkheid om deze vorm van fraude tegen te gaan? (bij uzelf en/of bij anderen)

Afsluitende vragen en afronding

12. Is er volgens u een onderwerp of gedachte niet aan de orde gekomen die u nog graag zou willen delen?

13. Tot slot zou ik graag uw geboortejaar willen noteren en uw hoogst genoten opleiding die u met een diploma hebt afgerond.
    a) Geboortejaar
    b) Hoogst genoten opleiding
    c) Geslacht (zelf invullen)

Respondent bedanken, opname eindigen en vervolgprocedure toelichten
Respondent de mogelijkheid bieden om de uitwerking van het interview te ontvangen en daar binnen twee weken commentaar op te geven.

Bijlage III: Uitnodigingsmail deelname interviews

Elke maand verkopen miljoenen mensen hun soms kostbare spullen via internet aan andere particulieren. Meestal gebeurt dit naar volle tevredenheid van alle partijen. Helaas zullen er altijd mensen zijn die de boel moedwillig oplichten. U betaalt keurig, maar ontvangt vervolgens niets. Of u wordt overgehaald om vast uw product op te sturen, maar ontvangt nooit een betaling. In beide gevallen bent u waarschijnlijk opgelicht. De politie, het Openbaar Ministerie, Marktplaats, banken en internetserviceproviders werken samen aan het terugdringen van internetoplichting. Zij vinden het belangrijk dat het vertrouwen in de handel via internet wordt beschermd, zodat mensen op een plezierige manier en in goed vertrouwen zaken met elkaar kunnen blijven doen. In 2017 is ongeveer 38.000 keer een dergelijke aangifte gedaan. Online aankoopfraude (geld betaald, maar geen product of dienst ontvangen) is een van de online fraudevormen. U bent slachtoffer geworden van deze vorm van fraude en heeft daar via www.politie.nl aangifte van gedaan. Uw aangifte is door de politie ontvangen en beoordeeld. Aan de hand van een aantal verwante aangiftes, het schadebedrag en/of de (eventuele) minderjarigheid of andere bijzondere omstandigheden in de persoon van een verdachte, worden zaken geselecteerd voor een voorbereidend opsporingsonderzoek. Het kan ook zijn dat uw aangifte niet is geselecteerd voor een opsporingsonderzoek.
De politie en haar partners is er alles aan gelegen om te onderzoeken hoe we slachtofferschap van online aankoopfraude kunnen voorkomen. Met andere woorden, hoe we samen, met meerdere partijen, maatregelen kunnen nemen zodat online aankoopfraude voorkomen kan worden, dan wel dat er een sterke afname plaatsvindt. Ondanks het feit dat uw aangifte mogelijk niet is geselecteerd voor een opsporingsonderzoek, hoop ik dat u wilt meewerken aan een interview voor een wetenschappelijk onderzoek.
Onderzoekers van de Onderzoeksgroep Cybersafety (NHL Stenden Hogeschool en de Politieacademie) proberen op verzoek van het programma Politie & Wetenschap inzicht te krijgen in de werkwijzen van daders, hoe het fraudeproces wordt beleefd door slachtoffers en hoe deze fraudevorm in de toekomst voorkomen kan worden. Een interview zal ongeveer 30 tot 45 minuten in beslag nemen en wordt in overleg afgenomen op een voor u handige locatie of via de telefoon.
Indien u wilt meewerken aan een vrijwillig en geanonimiseerd interview, kunt u dat aangeven door een reply te sturen op deze e-mail. U zult dan binnenkort via de mail benaderd worden door [projectleider] via het e-mailadres [e-mailadres] voor het maken van een afspraak. Inhoudelijk kan hij geen antwoord geven over de stand van zaken dan wel de voortgang van uw aangifte/zaak. Ik hoop dat u uw medewerking wilt verlenen aan dit onderzoek.

Bijlage IV: Interviewprotocol experts

Introductie

Wie zijn wij en wat gaan we doen
Allereerst ontzettend bedankt dat u mee wilt werken met ons onderzoek. De Onderzoeksgroep Cybersafety (NHL Stenden Hogeschool en de Politieacademie) voert onderzoek uit naar aankoopfraude vanuit het buitenland. Door in gesprek te gaan met experts willen we beter inzicht krijgen in verstoringsmogelijkheden van dit fraudeproces. Aan de hand hiervan kunnen aanbevelingen worden gedaan aan consumenten die online aankopen doen, maar ook aan organisaties die dit faciliteren of daarin op andere wijze een rol spelen, zoals de politie. Dit heeft als groter doel om het aantal fraudezaken in de toekomst terug te brengen. Wij voeren dit onderzoek uit in opdracht van het programma Politie & Wetenschap en in samenwerking met het LMIO.

Wat doen we met de informatie uit het interview
We schrijven een onderzoeksrapport en daarnaast wetenschappelijke artikelen. We zouden graag uw naam en de organisatie waarvoor u werkt willen gebruiken in het eindrapport. Uiteraard kan uw input ook anoniem verwerkt worden. Gaat u ermee akkoord dat uw naam als zijnde expert in het eindrapport wordt opgenomen?

Opname
Vindt u het goed dat het gesprek wordt opgenomen? De opnames worden alleen gebruikt voor het uittypen van het gesprek en worden daarna gewist. Deze laatste optie zorgt ervoor dat het interview zonder onderbrekingen kan worden afgenomen en uiteindelijk sneller kan worden afgerond.

Introductievragen

Als eerste wil ik u graag een aantal algemene vragen stellen over uw ervaring met online fraude en online aankoopfraude vanuit het buitenland. Vervolgens worden enkele aanvalsscenario's (MO's) voorgelegd en wil ik met u brainstormen over mogelijke verstoringsmogelijkheden. Tot slot stel ik enkele verstoringsmogelijkheden voor en vraag ik om uw mening over de effectiviteit en haalbaarheid hiervan.

1. Wat is uw functie?
2. In hoeverre hebt u in uw werk te maken met online fraude (algemeen)?
3. In hoeverre hebt u in uw werk te maken met online aankoopfraude vanuit het buitenland?
   a) Hoe frequent komt u in uw werk hiermee in aanraking?
   b) Worden door uw organisatie reeds (1) verstoringsmogelijkheden ingezet om online (aankoop)fraude (vanuit het buitenland) tegen te gaan en/of (2) andere partijen daartoe bewogen?

Crimescript brainstorm

*Ik wil u graag enkele crimescripts van aankoopfraude vanuit het buitenland voorgeleggen. *De overboekingen gaan dus allemaal naar een bankrekeningnummer in het buitenland. Vervolgens stel ik u enkele vragen over mogelijke verstoringsmaatregelen van de betreffende crimescripts.*

Crimescript-categorie 1:
Een fraudeur plaatst een valse advertentie van een auto op AutoScout24. De fraudeur wint vertrouwen door veel kennis én documentatie te hebben van de betreffende auto en het slachtoffer vrijwillig een identiteitsbewijs op te sturen. Het afgesproken bedrag voor de aanbetaling wordt overgemaakt door het slachtoffer. De fraudeur stuurt een bevestiging met daarin een valse Track&Trace-code (die wel werkt), omdat de auto in het buitenland zou staan. Op een gegeven moment lijkt het transport van de auto vast te lopen bij een landsgrens. Het totaalbedrag van de auto moet worden voldaan om het transport te kunnen voortzetten. Het slachtoffer maakt het resterende bedrag over. De fraudeur houdt enige tijd contact voordat het contact definitief wordt verbroken.

Crimescript -categorie 2:
Fraudeurs maken een valse webshop waar gereedschap wordt verkocht. De webshop ziet er professioneel uit. Om legitiem te lijken is een KvK-nummer opgenomen en is een klantenservice aanwezig door middel van chat. Een advertentie van deze webshop wordt geplaatst op Facebook. Indien Facebook-gebruikers deze advertentie 'liken', zien hun connecties dit automatisch ook, wat zorgt voor vertrouwen (verondersteld wordt dat de connectie ervaring heeft met het bedrijf). Benadeelden bestellen een product en het product wordt vervolgens niet geleverd. Contact met de fraudeurs is daarna niet meer mogelijk.

Crimescript -categorie 3:
Op Airbnb is een account met positieve recensies gehackt. Een bestaand vakantiehuis wordt aangeboden voor een goedkope prijs. Na reactie van potentiële slachtoffers op Airbnb verloopt het verdere contact via privé-e-mail. In de e-mails en bij het versturen van huurinformatie en de factuur wordt gebruikgemaakt van het logo van Airbnb. Vervolgens betaalt het slachtoffer de factuur. De fraudeur stuurt een bevestiging van betaling en reservering. Enige tijd later is de advertentie verdwenen en realiseert het slachtoffer zich opgelicht te zijn.

Crimescript -categorie 4:
Een fraudeur reageert op een 'gezocht'-advertentie van concertkaarten voor Coldplay op Marktplaats. De fraudeur biedt kaarten aan en een prijs wordt afgesproken. Het slachtoffer maakt het geld over en stuurt de fraudeur een bewijs van betaling. De fraudeur laat vervolgens niets meer van zich horen.

4. Welke verstoringsmaatregelen kunnen volgens u worden uitgevoerd? (per categorie)
   a) Wat voor effect (hoog/laag) verwacht u bij de betreffende maatregel? (effectiviteit)
   b) Hoe uitvoerbaar (korte/lange termijn) acht u deze maatregelen? Wat is ervoor nodig om de betreffende maatregel te laten slagen? (haalbaarheid)

5. Welke partijen spelen een rol bij de verstoring? (per voorgestelde maatregel)
   a) Hoe kunnen deze partijen daartoe worden bewogen? (evt. doorvragen op zorgplicht)
   b) Hoe kan de politie hieraan een bijdrage leveren?
   c) Hoe kan de klant hieraan een bijdrage leveren?

Mogelijke verstoringsmaatregelen

Uit onze eerdere resultaten zijn enkele verstoringsmaatregelen naar voren gekomen. Deze wil ik graag aan u voorleggen.

I. IBAN-Naam Check binnen EU:
In Nederland bestaat de mogelijkheid om het IBAN te controleren op naam. Men wordt bij het overmaken gewaarschuwd als rekeningnummer en naam niet overeenkomen. Een IBAN-Naam Check binnen de Europese Unie zou een verstoringsmaatregel kunnen zijn.

II. Awareness-campagne:
In onze analyse heeft slechts één vijfde van de klanten vooraf de verkopende partij gecontroleerd. In de meeste gevallen konden de benadeelden negatieve recensies vinden en trokken zelf de conclusie dat ze waren opgelicht. Een voorlichtingscampagne kan informatie geven over online fraude en aansporen tot controle op de verkopende partij en aangeboden product/dienst.

III. Certificatie handelswebsites:
Via handelssites, zoals Marktplaats en eBay, kunnen fraudeurs gemakkelijk hun slag slaan. Marktplaats kan een certificaat aan betrouwbare accounts geven. Dit kan bijvoorbeeld door een blauw vinkje te geven (vergelijkbaar met Twitter).

IV. RDW-controlesysteem eigenaar/kenteken:
Bij de aankoop van een auto kan niet gecontroleerd worden of de verkoper ook de eigenaar van de auto is. Het RDW zou een systeem kunnen ontwikkelen waar men dit kan controleren. In verband met privacywetgeving moeten het kenteken en de naam van de verkoper ingevoerd worden en wordt als antwoord alleen 'waar' of 'niet waar' gegeven.

6. In hoeverre kan deze maatregel online aankoopfraude vanuit het buitenland verstoren? (effectiviteit) (per individuele verstoringsmaatregel)

7. In hoeverre is deze maatregel uitvoerbaar? (haalbaarheid)

8. Welke actoren zijn belangrijk om deze maatregel uit te voeren?
   a) Hoe kunnen deze partijen daartoe worden bewogen? (evt. doorvragen op zorgplicht)
   b) Wat kan de politie hieraan bijdragen?
   c) Wat kan de klant hieraan bijdragen?

9. Hoe groot acht u de kans dat deze verstoringsmaatregel werkelijk aankoopfraude vanuit het buitenland verstoort? (combinatie effectiviteit en haalbaarheid)

Afsluitende vragen en afronding

10. Hebt u nog andere ideeën voor verstoringsmaatregelen?

11. Is er volgens u een onderwerp of gedachte niet aan de orde gekomen die u nog graag zou willen delen?

Respondent bedanken, opname eindigen en vervolgprocedure toelichten
Respondent de mogelijkheid bieden om de uitwerking van het interview te ontvangen en daar binnen twee weken commentaar op te geven.

Bijlage V: Effecten en impact van internationale aankoopfraude

Hoewel de interviewkandidaten allen minimaal één incident hebben meegemaakt met online aankopen, gaven de meesten (n = 19) aan dat de algemene ervaring positief is en dat dit niet is veranderd naar aanleiding van het incident (n = 11). De anderen gaven aan het betreffende platform waarop of product waarmee ze zijn opgelicht wel negatiever te beoordelen (n = 8).

Vier kandidaten gaven aan dat zij het doen van online aankopen sinds het incident onveiliger vinden. Een van deze kandidaten lichtte toe: 'Het is riskant. Ik voel me niet echt beschermd als er iets mis gaat. Dat gevoel van onveiligheid is sterker geworden na dit incident' (B11). Een ander benadrukte sceptischer te zijn geworden, omdat hij dacht dat het doen van online aankopen meer gereguleerd zou zijn. Een andere kandidaat gaf aan angstig te zijn en terug te willen naar een situatie van contante betalingen.

De meeste kandidaten gaven aan online aankopen over het algemeen wel veilig te vinden (n = 16), in ieder geval wat betreft de bekendere, erkende websites. Zo benoemde een kandidaat: 'Er zijn meer goede mensen die online handelen, dan slechte' (B4). Ook zijn zaken genoemd als het 'gelijk oversteken'-principe van Marktplaats en aankoopbescherming met PayPal, die bevorderend werken voor het veiligheidsgevoel. Een andere kandidaat zei dat hij veiligheid in relatie tot online aankopen op twee manieren beoordeelt. 'Enerzijds is het veilig, omdat er in Nederland dan wel in het buitenland veel bekende partijen zijn (…). die op correct wijze – tot mijn ervaring – correcte zaken aanbieden. Anderzijds, op iets abstracter, algemener niveau, (…) vraag ik mij als niet-expert weleens af of mobiele bankapps en creditcardaankopen – waarbij alle gegevens van de creditcard worden gevraagd – allemaal wel correct beveiligd zijn' (B9). Ook gaf een kandidaat aan dat online aankopen risicovoller zijn, bijvoorbeeld omdat de verkoper vaak moeilijk te controleren is. Daarnaast gaf iemand aan dat het voor hem lastig is te bepalen in hoeverre online aankopen veilig zijn, met name wanneer het gaat om onbekende websites. 'Maar als het er officieel uitziet, dan ga je toch een keer in de fout. Dat is bij mij ook gebeurd' (B2). Tevens zei iemand: 'Als je echt iets heel graag wilt, dan ben je bereid om aan de veiligheidskant in te leveren, zoals voor een concert waar je graag heen wilt' (B20).

Daarnaast gaven de meeste benadeelden aan dat ze wisten dat ze op een dergelijke manier opgelicht konden worden (n = 17). 'Dat soort dingen hoor je natuurlijk heel vaak. In programma's als Opgelicht, Radar en Kassa is het aan de lopende band aan de hand' (B12). Eveneens gaven de meesten aan dat ze dachten dat het hen niet zou overkomen ('optimism bias') en/of dat ze dachten dat het minder professioneel opgezet zou

zijn (n = 15). 'Het overkomt altijd een ander' (B7). 'Vooraf had ik de kans op nul ingeschat, want als ik ook maar 1% twijfel over een aankoop, dan gaat het niet door' (B1). '(…) Ook kijk ik vaak die programma's met Alberto Stegeman, en dan denk je: daar trap je toch niet in? En nu gebeurt het bij jezelf, haha' (B19). Drie benadeelden hadden geen weet van deze oplichtingsvorm. Deze personen hadden een incident meegemaakt met huurwoningen en vakantiehuizen via een website of via Airbnb.

Zes benadeelden gaven aan dat ze nooit meer in dergelijke oplichtingspraktijken gaan trappen of dat de kans daarop aanzienlijk is verkleind, omdat ze nooit meer op de gekozen wijze aankopen zullen doen. Aan de andere kant gaf een van hen aan dat hij dat ook voorafgaande aan het incident gezegd zou hebben. 'Als het weer zo geloofwaardig is en ik het de prijs en het risico waard vind, dan zie ik het mezelf toch wel weer doen. Misschien heb ik weinig zelfcontrole of zoiets' (B10).

Drie anderen gaven aan niet te kunnen zeggen dat ze nooit meer slachtoffer van een dergelijke fraude zullen worden. Een benadeelde lichtte dit als volgt toe: 'De daders gebruiken steeds andere technieken om mensen op te lichten. Daarom is het moeilijk te beantwoorden of ik verwacht opnieuw slachtoffer te kunnen worden' (B4). Ook werd aangegeven dat de kans aanwezig is en/of mogelijk wel iets hoger ligt dan ze aanvankelijk hadden gedacht (n = 5). 'De kans dat het nog een keer gebeurt is aanwezig. Het is soms een gok. Als ik iets echt graag wil, dan ben ik bereid om het risico te nemen. (…) Als je zo graag ergens naar toe wilt, dan ben je waarschijnlijk wel bereid dat als er al signalen zijn om die te negeren en toch tot de koop over te gaan. Tenzij het echt "obvious" is' (B20)

Het incident dat de geïnterviewde benadeelden hebben meegemaakt had voor allen financiële effecten. Bijna alle benadeelden hebben hun geld niet terug gekregen. Er waren twee uitzonderingen. In één geval kreeg een benadeelde de helft van het bedrag terug via zijn rechtsbijstandverzekering. In het andere geval kon de bank de transactie nog op tijd blokkeren. Daarnaast was er een geval waarbij de frauduleuze overboeking in opdracht van iemand anders werd gedaan, waardoor de benadeelde in kwestie geen financiële effecten ervaarde.

In acht gevallen is sprake van financiële impact; ingegeven doordat benadeelden aangaven dat ze veel geld zijn kwijtgeraakt. Een benadeelde gaf aan 'zo goed als blut' te zijn (B7). Een andere benadeelde gaf aan niet meer op vakantie te kunnen. Zij gaf eveneens aan dat de financiële kosten gedeeld werden met de vrienden die mee zouden op vakantie. Anderen gaven aan dat het voor hen om een 'behoorlijk', 'flink', 'groot', of 'aardig' bedrag ging. Een benadeelde gaf aan dat de financiële impact groot was, maar tegelijkertijd dat hij dit wel kon dragen.

Voor sommigen was het monetaire aspect niet, of minder, van belang (n = 5). Een benadeelde zei dat hij voor zichzelf een financiële barrière heeft voor het doen van dergelijke aankopen en daarom de financiële impact niet groot was. Een andere gaf aan: 'Ik zei al op dag één tegen mijn broertje; "*d*mn* man, ik ben zo iemand die zo'n *risk* neemt". Ik ben er dus ook niet kapot van dat ik dit geld ben verloren. Ik wou steeds het risico nemen. Het doet mij niet zoveel pijn. Ik kan er zelfs wel een beetje om lachen. Ik heb gegokt en verloren' (B10). Weer een andere gaf aan: 'We leven nog en we gaan toch op

vakantie' (B2). Een andere benadeelde gaf aan dat het bedrag financieel te managen was en dat de kosten werden gedragen door iedereen die mee wilde op vakantie. Bovendien werd een nieuwe vakantievilla geboekt.

Voor een groot deel van de benadeelden was het naast een vervelende ervaring niet veel meer dan dat. Dit werd bijvoorbeeld gerationaliseerd doordat er geen sprak was van een inbraak of fysiek geweld. Twee anderen gaven aan geen impact te voelen, maar wel dat ze zich een tijdje teleurgesteld en bedrogen hebben gevoeld. Dit had betrekking op het anderen moeten meedelen van het slechte nieuws of op het gebrek aan politieoptreden. Ook waren sommige benadeelden boos op de daders (n = 4) en voelden ze zich teleurgesteld in zichzelf, waren ze boos op zichzelf of voelden ze zich dom (n = 4). 'Ik vind het wel erg stom, haha. Ik snap nog steeds niet dat ik zo impulsief heb gehandeld' (B19). Anderen balen ervan dat ze erin zijn getrapt (n = 2) of schamen zich ervoor (n = 1). Tot slot gaf een benadeelde aan iets wantrouwiger te zijn geworden.

Voor een ander deel van de benadeelden was er wel degelijk sprake van psychologische en emotionele impact (n = 6). Drie van hen gaven aan een of meerdere slapeloze nachten te hebben gehad. Ook was er sprake van schaamte en gaf iemand aan ervan te hebben gehuild. Een andere benadeelde gaf aan de impact niet te kunnen omschrijven, maar wel dat hij een maand lang chagrijnig was. Daarnaast kreeg het vertrouwen in anderen een behoorlijke deuk (n = 2). 'Ik verwacht niet dat anderen mij dit aandoen' (B1). Een benadeelde gaf aan erg geschrokken te zijn. Ook hij ervaarde emoties zoals hierboven beschreven, zoals boos zijn en zich dom voelen. Tevens gaf deze benadeelde aan geen vertrouwen meer te hebben in Marktplaats, de politie en in online aankopen. Voor een benadeelde zat de teleurstelling en verdriet in het feit dat ze is opgelicht terwijl ze iets voor haar baas moest regelen. Ze durfde dan ook moeilijk aan haar baas te vertellen wat haar was overkomen. Dit geldt ook voor een andere benadeelde die zich schuldig en verantwoordelijk voelde; niet alleen voor haar eigen vakantiegeld, maar ook voor dat van haar vrienden.

Twee benadeelden die last hadden van psychologische en emotionele impact gaven ten tijde van het interview aan daarvan weer hersteld te zijn of ervan te herstellen. Een benadeelde gaf aan nog steeds last te hebben van de situatie. 'Accepteren gaat echt niet. Het is als een aanrijding, dat is op je netvlies gebrand, dat is een trauma' (B14). Deze mevrouw gaf aan het gevoel te hebben 'steeds tegen de muur te lopen' en heeft het idee dat 'niemand ons helpt', refererend naar de organisatie waarmee ze contact had gezocht. Ze vindt dat frustrerend. Tot slot gaf de benadeelde die deels financieel was gecompenseerd aan dat dit de psychologische en/of emotionele impact niet wezenlijk veranderde.

Een benadeelde gaf aan het aspect dat hij een kopie van zijn paspoort had opgestuurd heel erg te vinden. Dat kunnen ze volgens hem gebruiken om andere mensen op te lichten. 'Dan zie ik straks mijn naam online verschijnen met daarbij "hij heeft mijn geld gejat"' (B10). Een andersoortige impact die eenmaal is beschreven is dat het zorgelijk is hoe mensen in aanraking komen met malafide partijen. Daarmee wordt gedoeld op het misbruiken van de sociale kring. Een webwinkel kan namelijk als vertrouwd worden bestempeld als een connectie deze bijvoorbeeld 'liket' op Facebook.

Dit kan er mogelijk voor zorgen dat mensen ruzie met elkaar krijgen, omdat een malafide webshop is aangeraden, geliket door een connectie, 'dat vind ik eng' (B17).
Tot slot gaven benadeelden aan dat ze een wijze les hebben geleerd; ze zijn zich er nog meer van bewust en dus voorzichtiger (n = 7). 'Van elke ervaring word je alerter voor de volgende aankopen' (B4) of 'Ik ben wel voorzichtiger geworden' (B13). Dit geldt ook voor het aspect dat er met minder voor de hand liggende producten gefraudeerd wordt. Aan de andere kant voelen ze zich nu soms ook minder kundig. 'Wat had ik achteraf anders moeten doen?' (B1).

Aangezien de manier van werven via het LMIO plaatsvond is het logisch dat alle benadeelden die we hebben gesproken online aangifte hebben gedaan. De belangrijkste redenen om aangifte te doen zijn: de politie helpen de daders op te sporen c.q. te pakken te krijgen (n = 9); voorkomen van aankoopfraude bij anderen (n = 7); proberen het geld terug te krijgen – alsook dat van eventuele andere benadeelden – (n = 7); het bemoeilijken voor daders om aankoopfraude succesvol uit te voeren, bijvoorbeeld door de valse webshop uit de lucht te halen (n = 4); en het feit dat de daders een kopie van hun identiteitsbewijs hebben en daarmee mogelijk identiteitsfraude kunnen plegen (n = 2). Redenen die slechts één keer werden genoemd zijn: vanuit de hoop dat men op de lange termijn beter is beschermd tegen online oplichting, vanuit een rechtvaardigheidsgevoel, en omdat de bank dat adviseerde. Twee benadeelden belden of zochten contact via de e-mail met buitenlandse politiediensten in de betrokken landen. Dat leverde echter niets op of er werd doorverwezen naar de Nederlandse politie. Een indicatie van wat dit bij benadeelden teweegbracht is opgenomen in het tekstkader.

Bij benadeelden heerste een gevoel van teleurstelling en onbegrip over het vervolg op de aangifte. Sommigen gaven aan zich niet te herinneren informatie van de politie te hebben ontvangen. Anderen gaven aan alleen een standaardbericht te hebben gekregen. Dit had bijvoorbeeld betrekking op een bevestiging van de ontvangst van de aangifte en/of een algemeen bericht dat de zaak niet wordt opgepakt. 'Het is dan heel teleurstellend dat als ze de bank weten, het bankrekeningnummer weten, de website weten, het e-mailadres weten, er niets mee wordt gedaan. Dat zijn digitale dingen waarmee je volgens mij wel iets mee kan doen. Volgens mij moet je je verifiëren, valideren als je bij de bank een rekening opent. Dan mag je wel iets meer doen dan mij geautomatiseerd een gestandaardiseerd een berichtje sturen met "we doen er niets mee"' (B18).
Een andere benadeelde gaf het volgende aan: 'Je krijgt de indruk dat dit soort voorvallen een lage prioriteit hebben voor de politie en men er dus niet achteraan gaat. (…) Daarbij komt dat als je het vanuit strafrechtelijk oogpunt bekijkt dat het wellicht door twee of meer mensen is gedaan en is er dus sprake van een criminele organisatie, die ook nog eens internationaal werkt. Strikt genomen zou de politie het serieus kunnen nemen' (B9). Meneer gaf aan het wel te begrijpen in verband met prioritering, maar had meer verwacht. Dit begrip werd tevens beaamd door twee andere benadeelden. Anderen gaven aan niet

blij te zijn dat de zaak niet wordt opgepakt, omdat de oplichters gewoon met hun werk door kunnen gaan. Twee benadeelden gaven aan dat de daders ten tijde van het interview nog steeds actief zijn. 'Daar zit wil een stuk frustratie, boosheid. (…) De daders zijn dus in staat om meer slachtoffers te maken' (B4).

Twee benadeelden deden naast aangifte anoniem hun verhaal op een Europese website waar informatie geplaatst kan worden over internetoplichting, zoals over de transacties die plaatsvonden, welke websites en e-mailadressen werden gebruikt, et cetera. Een benadeelde gaf aan dat het om een internationaal Interpol-meldpunt voor internetfraude ging. De andere herinnerde zich de naam niet meer van de betreffende website. Een andere benadeelde maakte melding van het incident bij de Fraudehelpdesk.
Drie benadeelden belden de buitenlandse bank waarnaar ze het geld hadden overgemaakt. Daarop kwamen ze echter niet verder. Ook hebben negen benadeelden contact gezocht met hun eigen bank, maar dat leverde ook vaak niets op, zie tekstkader.

Banken lijken zich hierbij meestal te beroepen op privacywetgeving of geven aan dat het geld niet is terug te halen, vaak met dien verstande dat men zelf het geld had overgemaakt en dat met SEPA-betalingen het geld direct wordt overgemaakt. In één geval gaf een benadeelde aan dat de bank een terugbetaalverzoek heeft gedaan bij een buitenlandse bank. Daarbij vertelde de bank dat het terugstorten van het geld kan plaatsvinden binnen een paar dagen, binnen een paar maanden, of helemaal niet. In één geval werd duidelijk dat de bank adviseerde om aangifte te doen. In een ander geval werd bekend dat de bank ook aangifte had gedaan. Tot slot had in één geval de bank succes om het overgemaakte bedrag te blokkeren.

Een benadeelde nam contact op met iDEAL. Meneer had verwacht dat bij iDEAL-betalingen ook 'een soort van veiligheid' was ingebouwd (B16), maar dat bleek na de verkregen uitleg niet zo te zijn. Meneer werd meegedeeld dat iDEAL niets voor hem kon doen en dat hij zijn geld kwijt was.[1]
Negen benadeelden zochten contact met het platform waarop of waardoor ze in contact zijn gekomen met de verkoper. Dit contact had niet veel effect voor hen. In vier van de negen gevallen werd aangegeven dat het platform de betreffende advertentie en/of het account had verwijderd. Eén van hen gaf aan het vreemd te vinden dat de adverten-

1 iDEAL biedt geen zogenoemde 'chargebackregeling', zoals wel bij PayPal- en creditcardbetalingen het geval is. Zie ook: https://www.consumentenbond.nl/online-kopen/betalen-met-ideal.

tie pas vier dagen na de melding van Marktplaats werd gehaald. In een ander geval gaf het platform alleen aan het misbruik te hebben bevestigd. In het geval waarin Airbnb werd benaderd, werd aangegeven dat Airbnb niet aansprakelijk is en dat dit in de voorwaarden staat. Deze benadeelde heeft tevens drie advocaten naar haar zaak laten kijken en ook die concludeerden volgens haar dat Airbnb niet aangeklaagd kon worden, aangezien de voorwaarden stellen dat Airbnb niet verantwoordelijk is voor fraude.
Vier benadeelden gaven aan dat het moeilijk was om eBay en Marktplaats te bereiken. Een van hen gaf aan het vervelend te vinden dat ze geen reactie kreeg. 'Het is een soort van jouw winkel. Dan moet je daar ook verantwoordelijkheid voor dragen' (B11). Ook versterkte het uitblijven van een reactie door deze partijen het gevoel van onveiligheid bij de benadeelde.
Twee benadeelden zochten contact met de tussenpartij of met de daadwerkelijke partij in geval van naamsmisbruik. In een van deze gevallen gaf mevrouw aan bij Rent4Sure haar geld terug te willen. De betreffende partij gaf echter aan dat hun naam was misbruikt en dat het betreffende rekeningnummer niet het IBAN is van Rent4Sure. Hoewel zij het voorval betreurden, konden zij niets voor mevrouw betekenen. Wel hebben ze er een notitie van gemaakt. In het andere geval gaf het bedrijf waarvan de naam was misbruikt aan aangifte te doen bij de Spaanse politie. Daar is echter niets meer van vernomen.
Twee benadeelden zochten contact met hun verzekeringsmaatschappij betreffende rechtsbijstand. Een van hen heeft de helft van het aankoopbedrag teruggekregen. Bij de andere was de aanvraag nog in behandeling op moment van het interview. Een benadeelde heeft contact gehad met een softwarebedrijf dat Track&Trace-codes levert. In verband met privacy konden ze de betreffende interviewkandidaat niet helpen.

Sommige benadeelden gaven aan dat ze bepaalde acties hebben overwogen, maar niet hebben doorgezet. Een benadeelde gaf aan geen contact te hebben gezocht met zijn bank, omdat meneer wist dat het geld niet teruggehaald kon worden. Een benadeelde gaf aan dat ze geen contact heeft gezocht met haar verzekering, omdat ze dat niet durfde in verband met een recente verzekeringsclaim en uit schaamte. In twee gevallen hebben benadeelden geen contact gezocht met het platform waarop ze zijn opgelicht. Een van hen vulde daarbij aan: 'Ik verwacht niet dat ze mij kunnen helpen' (B10). Een andere benadeelde gaf aan melding te willen doen bij Interpol, maar kon geen algemeen meldpunt vinden.

Een van de benadeelden eindigde het interview met zijn conclusie dat de betrokken partijen allemaal niet thuis gaven. Marktplaats, Airbnb, de bank en de politie hebben niets voor meneer kunnen doen om zijn zaak op te lossen. 'Het is gewoon het Wilde Westen' (B3).

Bijlage VI: Overige casusbeschrijvingen van interviewkandidaten

In deze bijlage zijn alle overige casussen uiteengezet die niet zijn behandeld in paragraaf 4.3. Het gaat in totaal om 11 casussen uit de categorieën: auto's (kandidaten 10 en 13), elektronica (kandidaat 9), vakantiewoningen (kandidaten 5, 14 en 18), huurwoningen (kandidaten 3 en 15), sociale media (kandidaat 16) en hacken (kandidaten 1 en 4).

Oplichting met auto's

Kandidaat 10 (hierna aangeduid met meneer) maakte gebruik van de website Auto-Scout24 om een auto te zoeken. Via de website kwam hij in contact met een verkoper die aangaf dat hij woonachtig is in Noorwegen – van oorsprong Noors is – en dat de auto die hij wilde daar nu ook was. Meneer gaf aan dat de verkoper werkte voor een 'groene-energiebedrijf' in Nederland en nu voor een dergelijke organisatie in Noorwegen werkt. De verkoper bood aan om de auto op te sturen via een transportbedrijf. Eveneens vermeldde hij daarbij dat de auto, indien die niet bevalt, binnen vijf dagen kosteloos retour gestuurd kon worden. Ook vroeg de verkoper om een kopie van een identiteitsbewijs voordat de verkoop kon beginnen. Meneer stuurde een kopie van zijn paspoort en maakte de helft van het totaalbedrag over zodat overgegaan kon worden tot verscheping van de auto. Voor de verscheping werd een transportbedrijf ingezet (AB Transport Service Ltd.) en er werd een Track&Trace-code gegeven, zodat meneer het transport van de auto kon volgen.

Meneer maakte na het besluit tot aankoop de eerste helft (800 euro) van het totaalbedrag over. Op een gegeven moment had meneer het idee, op basis van de Track&Trace-informatie, dat het transport vastliep bij de grens met Denemarken. Rond die tijd ontving hij een e-mail van de verkoper daarover met het verzoek de andere helft van het totaalbedrag over te maken. Daarbij zaten officieel uitziende overheidsdocumenten die afkomstig waren van 'het ministerie van export of transport'. Daarin werd gesuggereerd dat betalen in twee keer niet was toegestaan en dat daarom het hele bedrag dus betaald moest worden. 'Die documenten waren met stempel en al.' Daarbij kreeg meneer eveneens te horen dat als hij dat niet zou doen, hij 75% van zijn eerste 800 euro zou verliezen.

'Hier had ik ook weer: het is vast een scam. Maar in mijn achterhoofd had ik van: eh, ik verlies sowieso 75%, misschien meer. Als het een scam is heb ik al 800 euro verloren, maar

*als het geen scam is … Hij had een goed verhaal met die documenten en dus dacht ik f*ck it, ik stuur hem die rest van die 800 euro op. (…) Die 75% weg plaatst je in zo'n positie van zal ik mijn losses nemen en gewoon naar huis gaan, of zal ik de rest geven met de kans op winnen. En ik nam constant die kans om meer te winnen. Maar het huis wint altijd.'*

Een tijdje nadat meneer het tweede bedrag had overgemaakt raakte de auto weer bij een grens in Denemarken vast. Hij werd door de verkoper gevraagd om nog een bedrag over te maken, zodat de vrachtwagen kon doorrijden. Daarop gaf hij te kennen dat de verkoper een dief was en alleen maar uit was op zijn geld. De verkoper gaf aan dat dat niet zo was en vermeldde daarbij dat hij maar 25% van het bedrag zou krijgen. Hier zat meneer weer in eenzelfde denkpatroon: 'Of ik verlies die 1.600 euro, of ik verlies nog eens 600 euro extra voor die kans dat die auto er nog komt.' Voordat meneer die 600 euro overmaakte, vroeg hij eerst het kenteken van de betreffende vrachtwagen op bij het transportbedrijf. Hij ontving details van een Duits kenteken en de naam van het schip waarmee de auto een oversteek zou maken. Met die gegevens op zak zocht meneer telefonisch contact met de klantenservice van 'die poort in Denemarken'. De mevrouw die hij sprak wilde niet ingaan op zijn vragen en soms hing ze meteen op, omdat meneer Engels sprak. Voor het overmaken van de laatste 600 euro had meneer nog een controle uitgevoerd. Hij vroeg de verkoper om een kopie van zijn paspoort. Dat deed de verkoper, wat op dat moment genoeg vertrouwen wekte bij meneer om voor de derde keer een bedrag over te maken: 'Hij is ten minste wel echt wie hij zegt dat hij is.'

Voordat meneer de helft van het bedrag overmaakte, nam hij eerst contact op met de verkoper. Omdat hij nogal sceptisch was, wilde hij weten welk transportbedrijf gebruikt zou worden. Hij heeft meerdere malen zonder succes geprobeerd te bellen met de verkoper. Toen hij een e-mail stuurde werd een reactie teruggestuurd dat het om 'AB Transport Service Ltd.' zou gaan. Meneer geloofde nu iets meer dat het wel zou kunnen kloppen, want hij kon een KvK-nummer van dat bedrijf vinden in Engeland.
Meneer dacht dat als zij [de mevrouw van de klantenservice] wat duidelijker was geweest hij misschien het laatste bedrag niet had overgemaakt, omdat achteraf bleek dat de route die de auto zou afleggen helemaal niet bestond. Voor wat betreft de paspoortkopie dacht meneer achteraf dat het waarschijnlijk een kopie is geweest van iemand die eerder is opgelicht, omdat hij zelf ook een kopie van zijn paspoort had moeten opsturen.

Meneer gaf aan de geldbedragen voor de auto overgemaakt te hebben naar een Kroatisch bankrekeningnummer. Meneer gaf aan dat er in het Engels werd gecommuni-

ceerd met de verkoper en het transportbedrijf. Naast e-mailcontact was er ook telefonisch contact. Meneer gaf aan verschillende mensen aan de lijn te hebben gehad. Uitzondering was de eerste e-mail die meneer ontving van de verkoper. Die was in gebroken Nederlands, 'vermoedelijk vertaald in Google Translate'. Meneer merkte achteraf op dat er altijd rond dezelfde tijd werd gereageerd op zijn e-mails, zowel door de verkoper als door het transportbedrijf. Dat vond hij verdacht. 'Ik weet het niet. Ik was blind of zo. Ik negeerde dat gewoon. Het kan ook toeval zijn dacht ik dan.' Tevens gaf meneer aan het idee te hebben dat hij met meerdere mensen e-mailcontact heeft gehad; de e-mails leken niet door dezelfde persoon getypt te zijn. Na doorvragen over de verzonden paspoortkopie gaf meneer aan niet te hebben gemerkt dat zijn identiteit is misbruikt.

Bij doorvragen kunnen benadeelden zich mogelijk aanvullende zaken herinneren die vertrouwen wekten om door te gaan met de aankoop. Meneer gaf aan dat hij het vertrouwen boven het wantrouwen stelde, omdat hij bij aanvang officiële documenten kreeg toegestuurd over de auto. Hierin werd aangegeven 'dat de auto was gekeurd, door wie, er zat een stempel op, en al die dingen'. Meneer herinnerde zich ook dat de verkoper steeds namen gaf, wat vertrouwen wekte. De verkoper gaf de naam van zichzelf, van de chauffeur en van de 'sales persoon' die verantwoordelijk was voor de betreffende transactie. Hij kreeg tevens hun telefoonnummers en had hen ook aan de lijn gehad. Achteraf vond hij het vreemd dat wanneer er niet werd opgenomen dat hij dan 'iets van Lyca Mobile' hoorde. 'Dat is wel sceptisch als het om bedrijven gaat.' Meneer had tevens navraag gedaan bij Noorse en Engelse chatgroepen (zogenoemde 'discourse chats') om uit te zoeken wat er gevonden kon worden over het Noorse energiebedrijf waarvoor de verkoper werkte en het Engelse transportbedrijf dat het product zou vervoeren. De reden hiervoor was dat meneer dacht dat zij effectiever zouden kunnen zoeken op Google dan hij, omdat zij de taal kennen. In beide groepen kwam het advies dat hij beter geen zaken kon doen met deze partijen. 'De communicatie [op de chatgroepen] liep niet heel lekker. Misschien heb ik daarom dit advies genegeerd.'

Meneer vond het gebruik van een Kroatisch rekeningnummer vreemd, maar zocht zelf de verklaring in: 'Het zou kunnen zijn dat ze [het groene-energiebedrijf waar de verkoper werkt] daar hun moeder-company hebben.' Ook kreeg meneer steeds een referentienummer mee dat hij in de beschrijving van de overschrijving moest typen, wat bij hem vertrouwen wekte. Bij het sturen van een kopie van zijn paspoort had meneer wantrouwen. 'Ik wist al een beetje dat het een scam was. Maar van persoon ben ik een beetje een risico-"taker" weet je. En die auto ziet er zo mooi uit. En ik wilde die auto super graag. Dus probeerde ik te geloven dat het echt was.' Daarnaast verwachtte meneer niet dat ze zo geloofwaardig te werk gingen. 'Van tevoren dacht ik: die lui komen met zo'n Pakistaans accent en zo. (…) Ik ben wel een beetje onder de indruk hoe slim ze dit gedaan hebben.'

Kandidaat 13 (hierna aangeduid met meneer) zocht al een tijd naar een specifieke oldtimer uit de jaren dertig. Via AutoScout24 kwam meneer in contact met een verkoper van het bedrijf 'US Oldtimers Import'. De auto zou in de Verenigde Staten staan en kon opgestuurd worden naar Nederland. Via de e-mail werd een identiteitsbewijs opgestuurd van de verkoper, wat vertrouwen wekte. Ook in het persoonlijke contact werd het vertrouwen van meneer gewonnen. De verkoper wist namelijk veel te vertellen over de auto; 'hij was goed voorbereid'. Uiteindelijk is meneer overgegaan tot koop en maakte 10% van het aankoopbedrag over via overschrijving naar een Italiaans bankrekeningnummer; op naam van de persoon die op het identiteitsbewijs stond. De auto zou na de aanbetaling worden bezorgd bij meneer thuis. Zodra de auto geleverd zou zijn, moest meneer het resterende bedrag betalen. Meneer realiseerde zich dat hij was opgelicht doordat er na de aanbetaling geen contact meer is geweest met de verkoper; noch via de telefoon noch via de e-mail.

Meneer had contact gehad via e-mail en meerdere malen via de telefoon. Bij het telefonisch contact sprak de verkoper in de 'wij-vorm', wat duidde op een bedrijf. Tevens vertrouwde hij de aankoop, omdat hij wel vaker een auto via het internet had aangeschaft. De communicatie verliep in het Engels; de verkoper sprak goed Engels met een Italiaans accent. Meneer had tijdens het aankoopproces geen argwaan. Bij doorvragen kwam wel naar voren dat meneer via Google Maps het adres van het bedrijf had gecontroleerd. Meneer kwam daarbij uit op een industrieterrein in Italië, wat voor hem vertrouwd leek. Tevens gaf meneer aan na dit incident nogmaals op eenzelfde wijze te zijn opgelicht. Ditmaal met de aanschaf van elektronica vanuit Frankrijk.

Oplichting met elektronica

Kandidaat 9 (hierna aangeduid met meneer) was op zoek naar een camera. Bij toeval stuitte meneer op een Spaanse website die de camera aanbood voor zo'n 1.000 euro onder de standaard vraagprijs; 'het was een vrij dure camera'. Na een paar dagen sudderen, bekeek meneer opnieuw de website. 'Deze zag er uitermate professioneel uit. Met alle disclaimers, alle Kamer van Koophandel-gegevens die je maar kunt verzinnen, et cetera. Het enige is, dat check je normaal niet, en zeker niet als het in het buitenland is.' Ook de productbeschrijving leek te kloppen en er was een chatfunctie aanwezig, waar meneer gebruik van had gemaakt. Meneer gaf aan dat er in het Engels werd gecommuniceerd en dat hij heel professioneel te woord is gestaan; hij kreeg meteen en correct antwoorden op zijn vragen. 'Al dat soort zaken geven het idee dat het hier een professionele, goede, betrouwbare partij betreft.' Nadat meneer de bestelling had voltooid met een creditcardbetaling, ontving hij per e-mail een bevestiging, zoals gebruikelijk is. Ook dit zag er op het oog goed en correct uit. De volgende dag kreeg meneer een e-mail met het bericht dat de betaling per creditcard geen doorgang kon vinden.

Daarbij kwam het verzoek om het bedrag middels overschrijving te voldoen, waarna de bestelling meteen in gang kon worden gezet. Nadat meneer had betaald via overschrijving, kreeg hij netjes een bevestiging dat het product tweeënhalve week later zou worden bezorgd.

'Hier [na het ontvangen van de e-mail] had ik beter moeten opletten. Dit is een vreemd verzoek.' Meneer gaf aan hier niet goed opgelet te hebben, omdat hij 'nog wat moe' was van een lange reis. 'Ik dacht: het zal wel. Ik had dat in die gemoedstoestand dus niet moeten doen.' Bij de overschrijving viel hem nog iets op. De naam van de begunstigde was namelijk anders dan de naam van het bedrijf waarmee hij dacht zaken te doen. Hoewel dat wel in de e-mail werd genoemd, was dat vreemd. 'Je zou verwachten dat de bank gerelateerd is aan de bedrijfsnaam of de handelsnaam van het bedrijf. Dat had mij ook moeten triggeren op z'n minst, maar dat heeft het niet gedaan.'

Meneer gaf aan dat de website van het koeriersbedrijf – die hij niet kende – er ook erg professioneel uitzag. Alle informatie die men zou verwachten stond erop en er werd een Track&Trace-code bijgeleverd, waarvan de route normaal leek. Dat hij het bedrijf niet kende was niet vreemd, omdat dit achteraf helemaal niet bleek te bestaan. 'Blijkbaar doen ze veel moeite om tot het laatste moment betrouwbaar te blijven.' De Track&Trace ging lang door en ook bleven de daders reageren op momenten dat meneer contact met hen zocht. Meneer dacht dat ze dit wellicht deden omdat de instanties dan minder snel achter hen aangaan. Op een gegeven moment viel op dat het pakje qua afstand al een week geen progressie maakte. Uit doorgestuurde e-mailwisseling kon worden opgemaakt dat de verkoper aangaf dat er mogelijk vertraging was ontstaan door de paasvakantie. Later kreeg meneer alsnog bericht dat het pakketje in Amsterdam was aangekomen; twee dagen later dan gepland. Echter, in verband met een tussendoor komend verblijf in het buitenland, gaf meneer via e-mail aan de ontvangst van het pakket nog tweeënhalve week te willen uitstellen. Daar werd bevestigend op gereageerd. Toen hij ook daarna het pakket niet kreeg, schreef meneer hen dat hij beter naar de gegevens van de verkoper en het koeriersbedrijf had gekeken, maar dat die niet klopten. Daarop ontving meneer geen reactie meer, en werd het voor hem duidelijk dat hij was opgelicht. Ook werkte de chatfunctie niet meer. Meneer gaf daarbij aan dat deze functie mogelijk werd geblokkeerd op basis van zijn account of IP-adres.

Oplichting met vakantiewoningen

Benadeelde 5 (hierna aangeduid met mevrouw) wilde een vakantieappartement in Nederland boeken voor haar baas. Via een zoekslag op Google kwam mevrouw uit bij de website ShortStayApartments. Via de website kwam mevrouw in contact met een persoon achter de website om een en ander in orde te maken. Het contact vond plaats via

e-mail, in het Engels. Mevrouw maakte het overeengekomen bedrag van 1.450 euro over via internetbankieren naar een Spaans bankrekeningnummer. Een dag later nam de verhuurder contact op dat er iets was misgegaan. Ze werd verzocht het geld terug te vragen en opnieuw een overboeking te doen, maar ditmaal naar een Pools bankrekeningnummer. Zo gezegd, zo gedaan. Na de overboeking werd er nog een tijdje heen en weer gemaild, bijvoorbeeld over de bevestiging van de reservering en het reserveringsnummer. Ook werd beloofd dat de baas verdere details zou ontvangen, zoals over de transfer van het vliegveld naar het appartement en over de sleuteloverdracht. Haar baas heeft deze informatie echter niet ontvangen, waarop mevrouw probeerde telefonisch contact te zoeken. Dit lukte niet, maar ze kreeg wel een e-mail van de verhuurder dat ze lastig bereikbaar was, omdat ze in de Verenigde Staten zou verblijven. Daardoor zou de communicatie verder gaan via e-mail. Mevrouw ontving echter een 'onbezorgd-mail' toen ze via e-mail contact wilde opnemen. Ook bleek de advertentie niet meer te bestaan toen ze die wilde opzoeken. Op dat moment werd duidelijk dat mevrouw was opgelicht.

Bij doorvragen bleek dat er een valse website was gemaakt waarin het merk van ShortStayApartments werd misbruikt. Mevrouw vroeg namelijk aan haar Nederlandse collega om met het bedrijf te bellen. Die gaven aan dat de verhuurder niet voor het bedrijf werkte en dat meerdere mensen slachtoffer hiervan waren. Het viel mevrouw achteraf gezien wel op dat op de website geen telefoonnummer stond. Voor de rest had ze geen enkel idee dat het om een fraudepoging ging. Er waren geen 'red flags'. De website en ook het e-mailverkeer leken legitiem. Het zag er professioneel uit, en mevrouw kreeg bij vragen vrijwel direct antwoord. De overboeking naar Spanje deed geen alarmbellen rinkelen, omdat er werd gecommuniceerd dat de eigenaar daar woonde. Het enige dat mevrouw nog steeds vreemd vond, was waarom ze het geld in eerste instantie moest laten terugstorten.

Benadeelde 14 (hierna aangeduid met mevrouw) was op zoek naar een vakantiehuis in Spanje om daar samen met haar gezin en een aantal vrienden te verblijven. Via Airbnb vond mevrouw een geschikt appartement en zocht contact met de verhuurder. Deze nam contact met mevrouw op en vroeg om haar privé-e-mail, zodat ze een aantal extra foto's kon doorsturen. Het contact verliep in het Engels. De foto's leken goed en mevrouw wilde overgaan tot huur. Voordat ze akkoord gaf, controleerde mevrouw het adres van de accommodatie. Ook dat leek in orde. Als mevrouw het bedrag in een keer zou voldoen, zou dat een korting opleveren. Mevrouw ontving daarvoor een link in een e-mail die verwees naar een valse Airbnb-pagina. Mevrouw probeerde het bedrag te voldoen via creditcard, maar dat mislukte. Op de betreffende pagina was een chatfunctie aanwezig om met een servicemedewerker te praten. Deze medewerker hielp mevrouw om de betaling via de creditcard te laten slagen, maar ook dat mislukte. De

medewerker stelde voor om mevrouw een factuur te sturen in pdf, zodat mevrouw via internetbankieren het geld alsnog zou kunnen overmaken. Mevrouw heeft via SEPA het totaalbedrag van 4.200 euro overgemaakt naar een Iers bankrekeningnummer. Na de betaling ging het contact nog even door. Zo werd er door de verhuurder contact opgenomen met de vraag of er ook een transfer geregeld moest worden. Op een gegeven moment gaf de verhuurder aan zich in de Verenigde Staten te bevinden. Dit wekte argwaan bij mevrouw en ze bezocht daarom de advertentie nogmaals. Echter, de advertentie bestond niet meer. Mevrouw realiseerde zich te zijn opgelicht.

Bij doorvragen gaf mevrouw aan de aankoop te vertrouwen, omdat de website authentiek leek. Ook vertrouwde mevrouw de verhuurder, omdat ze haar foto's stuurde, met haar meedacht en doordat het contact open en soepel verliep. Ook de factuur leek echt te zijn.

Benadeelde 18 (hierna aangeduid met meneer) werd gevraagd om de betaling in orde te maken voor een vakantievilla in Spanje waar zijn vrouw met een aantal vriendinnen vakantie kon vieren. Een van de vriendinnen zag de villa op de website VPTenerife en had deze gereserveerd. Zonder enige validatie of verificatie zocht meneer contact met de verhuurder en maakte daarna een bedrag van 2.000 euro (helft huur en helft borg) over naar een Spaans bankrekeningnummer. Meneer had de bank vooraf gecontroleerd; deze bleek echt en was gelokaliseerd in Barcelona. Meneer had geen verdere controles uitgevoerd, omdat hij alleen de betaling hoefde te regelen. Meneer kreeg de optie om het bedrag in een keer te voldoen, wat hem een korting van 250 euro opleverde, maar mocht het ook in meerdere delen overmaken. Drie weken na de betaling zou de villa worden getoond aan de andere vriendinnen, maar toen was de website verdwenen. 'Toen wisten we eigenlijk wel genoeg.'

Bij doorvragen gaf meneer aan dat er geen enkele twijfel was. Dat kwam met name doordat de vriendin die had geboekt er al eens eerder was geweest. De website bevatte meerdere vakantievilla's en de betreffende villa stond tevens op andere websites en de prijzen daarop waren vergelijkbaar. Ook de omschrijving, de brief in de e-mail, en de communicatie waren duidelijk en verliepen in correct Engels. 'Het zag er gewoon erg professioneel uit.' Wel gaf meneer aan het achteraf vreemd te vinden dat er niet via creditcard betaald kon worden, maar dat de betaling via overboeking voldaan moest worden. Ook vond hij bij nader inzien de website zelf niet zo professioneel. 'Als ik achteraf nadenk hoe die site eruitziet dan had ik wel moeten begrijpen waarom er geen betaalopties via creditcard of iDEAL en dergelijke mogelijk waren.'

Oplichting met huurwoningen

Benadeelde 3 (hierna aangeduid met meneer) wilde een appartement huren in een grote stad in Nederland. De aanleiding hiervoor was zakelijk van aard. Meneer kwam via Marktplaats in contact met een particuliere verhuurder uit Duitsland. Deze verhuurder gaf in het e-mailcontact aan dat ze de betaling liever afhandelde via een 'agent', in dit geval Airbnb. Ze liet op een later moment weten langs een Airbnb-kantoor te zijn gegaan om een huurcontract te regelen en gaf daarbij aan dat een contactpersoon van Airbnb de registratie en dergelijke zou afhandelen met meneer. Vervolgens nam deze contactpersoon via een gespooft e-mailadres met hem contact op. Daarop heeft meneer vervolgens een kopie van zijn paspoort opgestuurd en een eerste betaling van 1.040 euro gedaan, waarvan de helft een maand huur betrof en de andere helft een borg. De verhuurder hield contact met meneer en gaf aan dat er meer gegadigden waren die het appartement wilden huren. Zij vroeg meneer om een snelle reactie op de vraag of hij het appartement voor een jaar wilde huren en om meer geld over te maken. Dat kon hij dan overmaken naar het rekeningnummer van de man van de verkoper en Airbnb hoefde daarvan niet op de hoogte gesteld te worden. Meneer maakte vervolgens nog een bedrag over. Het contact verliep op verzoek van de verhuurder daarna in het Duits in plaats van in het Engels. Tevens gaf de verhuurder aan niet meer gebeld te willen worden. Uiteindelijk maakte meneer voor de derde keer een bedrag over naar een Pools bankrekeningnummer.

Benadeelde 15 (hierna aangeduid met mevrouw) was op zoek naar een appartement in een grote stad in Nederland. Mevrouw had zich al op een aantal websites ingeschreven, maar zag uiteindelijk een geschikte woning voorbij komen op Marktplaats, waarop mevrouw reageerde. Ze ontving een reactie van iemand die aangaf dat ze het appartement aanbood 'voor een vriendin die niet zo handig is met het aanmaken van een Marktplaats-account'. Daarbij gaf ze een e-mailadres door waarop mevrouw contact kon zoeken. Dat heeft mevrouw gedaan en het contact verliep heel prettig en vond plaats in het Nederlands. De verhuurder gaf een naam op die overeen kwam met de naam in het e-mailadres. Op een gegeven moment gaf de verhuurder aan dat ze het appartement wel wilde laten zien, maar dat het fysiek niet mogelijk was. De verhuurder gaf aan al jaren met haar man in Londen te wonen; ter bevestiging had de verhuurder haar adres doorgestuurd. Omdat ze oorspronkelijk uit Nederland kwam, hield ze het appartement aan en wilde het verhuren. Daarop gaf ze aan het een en ander via een tussenpersoon te willen regelen, namelijk via Rent4Sure. Mevrouw kon aan deze tussenpartij het overeengekomen bedrag betalen. Als het appartement beviel, dan werd het geld doorgestuurd aan de verhuurder. Beviel het niet, dan zou mevrouw het geld weer retour krijgen. Mevrouw volgde de instructies die de verhuurder haar gaf en er zou een datum voor sleuteloverdracht worden afgesproken. Een bedrag van 1.000 euro – waarvan de helft huur betreft en de andere helft borg – werd overgemaakt naar een Iers bankrekeningnummer en mevrouw stuurde volgens afspraak een screenshot van de transactie. Daarna heeft mevrouw niets meer van de verhuurder vernomen. Ook probeerde ze nog via WhatsApp contact te zoeken. Hoewel ze kon zien dat het nummer online was, lukte dat niet. 'Je weet natuurlijk ook niet zeker dat die persoon achter het nummer zit.' Na twee dagen geen contact vermoedde mevrouw dat het niet klopte.

Bij doorvragen gaf mevrouw aan dat er geen sprake was van argwaan. Ze had het huis tevens op Funda zien staan, waarbij dezelfde foto's werden gebruikt. Ze had tevens bij het appartement gekeken en zag dat er een verhuurbord aanwezig was. Ze had zelfs aangebeld, maar niemand deed open. Mevrouw heeft tevens het bedrijf Rent4Sure vooraf gecontroleerd en dit bleek te bestaan. Tevens had het bedrijf goede recensies, zowel van Engelse als van Nederlandse klanten. Ook de tussenpartij leek dus legitiem. Het enige opmerkelijke wat mevrouw zich nog herinnerde was dat de overboeking in eerste instantie niet slaagde, omdat de naam niet werd 'gepakt'. De verhuurder gaf aan dat ze 'R4S' moest gebruiken, en toen lukte het wel. Daarnaast gaf mevrouw aan het niet vreemd te vinden dat iemand anders dan de verhuurder de advertentie op Marktplaats had gezet. 'Ik heb ook in België gewoond en daar kun je geen Marktplaats-account aanmaken. Dan krijg je de melding van "Wij vertrouwen dit niet, je moet in Nederland wonen, jouw IP-adres moet Nederlands zijn anders kun je geen Marktplaats-account aanmaken".' Op een later moment ontving mevrouw bericht van Marktplaats met de mededeling dat degene met wie mevrouw contact had gehad geblokkeerd was, en dat ook andere mensen die contact met deze persoon hadden waren gewaarschuwd.

Oplichting via sociale media

Kandidaat 16 (hierna aangeduid met meneer) kwam op Facebook een advertentie tegen waarin klusmateriaal werd aangeboden. Meneer werd via de advertentie doorgelinkt naar een, volgens hem Amerikaanse, webwinkel waar hij een bestelling plaatste. Omdat meneer de prijs goed vond en nog vijf minuten pauze had, besliste hij om nog een bestelling te plaatsen op dezelfde webwinkel. 'Het materiaal was heel goedkoop aangeboden; eigenlijk waarvan je het idee krijgt "het is te mooi om waar te zijn"'. Toch had meneer geen argwaan. De website wekte vertrouwen bij meneer, omdat er via iDEAL betaald kon worden. In beide gevallen betaalde hij via iDEAL en zijn de bedragen overgeschreven naar een Belgisch bankrekeningnummer.

Een paar dagen na de bestelling zag meneer een andere, vergelijkbare advertentie op Facebook. Die linkte door naar een veel minder betrouwbaar uitziende webwinkel. Daarop besloot meneer de webwinkel waar hij had besteld en het bijstaande e-mailadres te controleren via Google. Hij vond dat deze bekend stonden als onbetrouwbaar; er waren meerdere meldingen van gemaakt. Achteraf leek het e-mailadres er niet betrouwbaar uit te zien en vond meneer het vreemd dat er helemaal geen klantenservice aanwezig was op de website. Meneer heeft nog contact gezocht met de webwinkel via de e-mail. Daarop werd gereageerd dat de levertijd 30 dagen zou bedragen en meneer die 30 dagen maar rustig moest afwachten. Meneer gaf aan dat de e-mailwisseling in gebrekkig Engels was. 'Toen wist ik eigenlijk ook wel genoeg.'

Omdat de prijs zo mooi was en hij in zijn pauze zat, dacht meneer niet lang over de aankoop en plaatste 'halsoverkop' de bestellingen. Met name de tijdsdruk speelde volgens meneer een belangrijke rol waarom hij de 'verkeerde keuzes' heeft gemaakt en niet 'voorzichtig genoeg' was. Hij had vooraf geen controles uitgevoerd. Er was geen contact tussen meneer en de verkoper. Het ging zoals normaal gesproken iets via een webshop wordt gekocht. Meneer gaf eveneens aan die week drie keer te zijn opgelicht. De andere twee zaken hadden betrekking op Marktplaats-advertenties. Voor die zaken heeft meneer ook aangifte gedaan.

Oplichting waarbij hacken een rol speelt

Kandidaat 1 (hierna aangeduid als meneer) was voor zijn zoon op zoek naar een bepaald type gitaar en had er een gezien op de Duitse eBay. De betreffende gitaar is voor 'liefhebbers' en de specifieke beschrijving van het artikel deed vermoeden dat een liefhebber deze van de hand wilde doen. Door de specifieke en correcte informatie in de beschrijving had meneer geen argwaan dat de advertentie vals zou zijn. De verkoper deed zich voor als een particulier en kwam uit Duitsland. De communicatie vond eveneens in het Duits plaats via e-mail. Na de betaling nam meneer contact op met de vraag wanneer het product geleverd zou worden. De verkoper gaf daar nog antwoord op, waarna het contact werd verbroken. Na vijf dagen constateerde meneer te zijn opgelicht. Na contact te hebben gehad met eBay vertelden ze hem dat het account waarmee hij contact had gehad was gehackt.

Tevens is doorgevraagd of er zaken speelden die mogelijk leken te wijzen op fraude of waarbij extra vertrouwen is gewekt om door te gaan met de aankoop. Meneer gaf aan geen argwaan te hebben gehad. Daarvoor had hij meerdere redenen. Als eerste gaf hij aan eerdere positieve ervaringen te hebben met het aanschaffen van producten via de Duitse eBay. Ten tweede had meneer niet verwacht dat er sprake zou zijn van oplichting bij een dergelijk product. 'Bij producten zoals camera's of een iPhone zou ik eerder argwaan hebben.' Ten derde gaf hij aan verschillende checks te hebben gedaan om te kijken of de advertentie echt was. Het bleek dat de verkoper al twintig jaar actief was en positieve beoordelingen had. 'Als het account maar een week oud was, had ik geen aankoop gedaan.' Ten vierde heeft hij gevraagd om foto's en het serienummer van de gitaar. Ook die bleken na controle te kloppen.

Kandidaat 4 (hierna aangeduid met meneer) was op zoek naar een specifiek type ventilator. Via Marktplaats kwam meneer in contact met een bedrijf dat die ventilator zou verkopen. De ventilator was scherp geprijsd, 'maar niet zo scherp dat het verdacht was'. De communicatie vond plaats via Marktplaats en WhatsApp en geschiedde in het Nederlands. Bij de aanschaf vertelde de verkoper dat het geld overgemaakt moest worden naar een Duits rekeningnummer. Meneer deed dit en ontving vervolgens, zoals hem werd beloofd, een Track&Trace-code. Hoewel deze er legitiem uitzag, werkte de code niet. Daarop zocht meneer contact met de verkoper en die vertelde dat de bezorgers vertraging hadden en dat de code de volgende dag wel actief zou worden. Echter, de code bleef inactief. Daarop besloot meneer te bellen met het nummer van de handelsonderneming die hij had opgezocht. De gegevens van de onderneming bleken via hacking in het bezit te zijn gekomen van criminelen. Deze criminelen gebruikten de verkregen gegevens om onder de naam van de onderneming valse advertenties te plaatsen. 'Alle informatie, zoals adres en KvK-nummer, is overgenomen in de advertentie. Dat was goed doordacht gedaan.' De onderneming wist van de oplichting af. Bovendien hadden ze hiervan al aangifte gedaan. Toen wist meneer zeker dat hij was opgelicht.

Ook deze benadeelde gaf aan geen argwaan te hebben gehad. De website zag er erg betrouwbaar uit volgens hem en bevatte verifieerbare informatie. Bovendien stond erbij vermeld dat het product afgehaald kon worden. Ook heeft hij vooraf verschillende controles uitgevoerd. Via Marktplaats heeft hij het rekeningnummer en telefoonnummer gecontroleerd die in de advertentie werden genoemd en die leken legitiem. Het Duitse rekeningnummer was wel een alarmbel voor meneer. Hij vroeg de reden daarvoor op bij de verkoper. Die gaf aan dat het bedrijf vlak bij de Duitse grens ligt en dat in verband met kosten al jaren zaken worden gedaan met een Duitse bank. Meneer controleerde het adres van het bedrijf en zag inderdaad dat dit vlak bij de Duitse grens ligt, wat het voor hem aannemelijk maakte. Achteraf gezien was het telefoonnummer ook een alarmbel. Het telefoonnummer in de advertentie kwam namelijk niet overeen met een andere bron op internet. Hij rationaliseerde voor zichzelf dat het goed mogelijk is dat iemand meerdere telefoonnummers heeft. Ook controleerde hij hoe lang het bedrijf actief was op Marktplaats, wat vertrouwen wekte. 'Ik zou geen zaken doen met iemand die slechts een maand actief is.'

Leden Redactieraad Programma Politie & Wetenschap

Uitgaven in de reeks Politiekunde

1. ***Criminaliteit in de virtuele ruimte***

   P. van Amersfoort, L. Smit & M. Rietveld, DSP-groep, Amsterdam/ TNO-FEL, Den Haag, 2002

2. ***Cameratoezicht. Goed bekeken?***

   I. van Leiden & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem, 2002

3. ***De 10 stappen van Publiek-Private Samenwerking (PPS)***

   J.C. Wever, A.A. van Pel & L. Smit, DSP-groep, Amsterdam/TNO-FEL, Den Haag, 2002

4. ***De opbrengst van projecten. Een verkennend onderzoek naar de bijdrage van projecten aan diefstalbestrijding***

   C.J.E. In 't Velt, e.a., NPA-Onderzoeksgroep, LSOP, Apeldoorn, 2003

5. ***Cameratoezicht. De menselijke factor***

   A.Weitenberg, E. Jansen, I. van Leiden, J. Kerstholt & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem/TNO, Soesterberg, 2003

6. ***Jeugdgroepen in beeld. Stappenplan en randvoorwaarden voor de shortlistmethodiek***

   H.B. Ferwerda & A. Kloosterman, Advies- en Onderzoeksgroep Beke & Politieregio Gelderland-Midden, Arnhem, 2004 (vierde druk 2006)

7. ***Hooligans in beeld.Van informatie naar aanpak***

   H.B. Ferwerda & O. Adang, Advies- en Onderzoeksgroep Beke, Arnhem/ Onderzoeksgroep Politieacademie Apeldoorn, 2005

8. ***Richtlijnen auditieve confrontatie***

   J.H. Kerstholt, A.G. van Amelsfoort, E.J.M. Jansen & A.P.A. Broeders, TNO Defensie en Veiligheid, Soesterberg/Politieacademie, Apeldoorn/ NFI, Den Haag, 2005

9. ***Niet verschenen***

10. ***De opsporingsfunctie binnen de gebiedsgebonden politiezorg***

    O. Zoomer, IPIT, Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2006

11. Inzoomen en uitzoomen op Zaandam

I. van Leiden & H.B. Ferwerda, Advies- en onderzoeksgroep Beke, Arnhem 2006

12. Aansprakelijkheidsmanagement politie. Beschrijving, analyse en handreiking

E.R. Muller, J.E.M. Polak, C.J.J.M. Stoker m.m.v. M.L. Diepenhorst & S.H.E. Janssen, COT, Instituut voor Veiligheids- en Crisismanagement, Den Haag/Faculteit der Rechtsgeleerdheid Universiteit Leiden, 2006

13. Cold cases – een hot issue

I. van Leiden & H.B. Ferwerda, Advies- en onderzoeksgroep Beke, Arnhem, 2006

14. Adrenaline en reflectie. Hoe leren politiemensen op de werkplek?

A. Beerepoot & G. Walraven e.a., DSP-groep BV, Amsterdam/Walraven onderzoek en advies, 2007

15. Tussen aangifte en zaak. Een referentiekader voor het aangifteproces

W. Landman, L.A.J. Schoenmakers & F. van der Laan, Twynstra Gudde, adviseurs en managers, Amersfoort, 2007

16. Baat bij de politie. Een onderzoek naar de opbrengsten voor burgers van het optreden van de politie

M. Goderie & B. Tierolf, m.m.v. H. Boutellier & F. Dekker, Verwey-Jonker Instituut, Utrecht, 2008

17. Hoeveel wordt het vandaag? Een studie naar de kans op voetbalgeweld en het veiligheidsbeleid bij voetbalwedstrijden

E.J. van der Torre, R.F.J. Spaaij & E.D. Cachet, COT, Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2008

18. Overbelast? De administratieve belasting van politiemensen bij de afhandeling van jeugdzaken

G. Brummelkamp & M. Linssen, EIM, Zoetermeer, 2008

19. Geografische daderprofilering. Een inventarisatie van randvoorwaarden en succesfactoren

G. te Brake & A. Eikelboom, TNO Defensie en Veiligheid, Soesterberg, 2008

20. Solosurveillance. Kosten en baten

S.H. Esselink, J. Broekhuizen & F.M.H.M. Driessen, Bureau Driessen, 2009

21. Onderzoek naar de mogelijke meerwaarde van AWARE voor de politie. Ervaringen met een nieuwe aanpak van belaging door ex-partners

M.Y. Bruinsma, J. van Haaf, R. Römkens & L. Balogh, IVA Beleidsonderzoek en Advies, i.s.m. INTERVICT/Universiteit van Tilburg, 2008

22. Gebiedsscan criminaliteit en overlast. Een methodiekbeschrijving

B. Beke, E. Klein Hofmeijer & P. Versteegh, Bureau Beke, Arnhem, 2008

23. Informatiemanagement binnen de politie. Van praktijk tot normatief kader

V. Bekkers, M. Thaens, G. van Straten & P. Siep; m.m.v. A. Dijkshoorn, Center for Public Innovation, Erasmus Universiteit Rotterdam, 2009

24. Nodale praktijken. Empirisch onderzoek naar het nodale politieconcept

H.B Ferwerda, E.J van der Torre & V. van Bolhuis, Bureau Beke, Arnhem/ COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2009

25. Rellen om te rellen. Een studie naar grootschalige openbare-ordeverstoringen en notoire ordeverstoorders

I. van Leiden, N. Arts & H.B. Ferwerda, Bureau Beke, Arnhem, 2009

26a. Verbinden van politie- en veiligheidszorg. Politie en partners over signaleren & adviseren

W. Landman, P. van Beers & F. van der Laan, Twynstra Gudde, Amersfoort, 2009

26b. Politiepolitiek. Een empirisch onderzoek naar politiële signalering & advisering

E.J.A. Bervoets, E.J. van der Torre & J. Dobbelaar m.m.v. N. Koeman, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2009

27. De politie aan zet: de aanpak van veelplegers in Deventer

I. Bakker & M. Krommendijk, IPIT, Enschede, 2009

28. Boven de pet? Een onderzoek naar grootschalige ordehandhaving in Nederland

O.M.J. Adang (redactie), S.E. Bierman, K. Jagernath-Vermeulen, A. Melsen, M.C.J. Nogarede & W.A.J. van Oorschot, Politieacademie, Apeldoorn, 2009

29. Rellen in Ondiep. Ontstaan en afhandeling van grootschalige ordeverstoring in een Utrechtse achterstandswijk

G.J.M. van den Brink, M.Y. Bruinsma (redactie), L.J. de Graaf, M.J. van Hulst, M.P.C.M. Jochoms, M. van de Klomp, S.R.F. Mali, H. Quint, M. Siesling, G.H. Vogel, Politieacademie, Apeldoorn, 2010

30. Burgerparticipatie in de opsporing. Een onderzoek naar aard, werkwijzen en opbrengsten

A. Cornelissens & H. Ferwerda (redactie), met medewerking van I. van Leiden, N. Arts & T. van Ham, Bureau Beke, Arnhem, 2010

31. ***Poortwachters van de politie. Meldkamers in dagelijks perspectief***

J. Kuppens, E.J.A. Bervoets & H. Ferwerda, Bureau Beke, Arnhem & COT, Den Haag, 2010

32. ***Het integriteitsbeleid van de Nederlandse politie: wat er is en wat ertoe doet***

M.H.M. van Tankeren, Onderzoeksgroep Integriteit van Bestuur, Vrije Universiteit Amsterdam, 2010

33. ***Civiele politie op vredesmissie. Uitzendervaringen van Nederlandse politie - functionarissen***

H. Sollie, Universiteit Twente, Enschede, 2010

34. ***Ten strijde tegen overlast. Jongerenoverlast op straat: is de Engelse aanpak geschikt voor Nederland?***

M.L. Koemans, Universteit Leiden, 2010

35. ***Het districtelijk opsporingsproces; de black box geopend***

R.M. Kouwenhoven, R.J. Morée &. P. van Beers, Twynstra Gudde, Amersfoort, 2010

36. ***Balanceren tussen alert maken en onrust voorkomen. Publiekscommunicatie over seriële schokkende incidenten (casestudy Lelystad)***

A.J.E. van Hoek, m.m.v. P.F. van Soomeren, M.D. Abraham & J. de Kleuver, DSP-groep, Amsterdam, 2011

37. ***Sturing van blauw. Een onderzoek naar operationele sturing in de basispolitiezorg***

W. Landman, m.m.v. M. Malipaard, Twynstra Gudde, Amersfoort, 2011

38. ***Onder het oppervlak. Een onderzoek naar ontwikkelingen en (a)select optreden rond preventief fouilleren***

J. Kuppens, B. Bremmers, E. van den Brink, K. Ammerlaan & H.B. Ferwerda, m.m.v. E.J. van der Torre, Bureau Beke, Arnhem/COT, Den Haag, 2011

39. ***Naar eigen inzicht? Een onderzoek naar beoordelingsruimte van en grenzen aan de identiteitscontrole***

J. Kuppens, B. Bremmers, K. Ammerlaan & E. van den Brink, Bureau Beke, Arnhem/COT, Den Haag, 2011

40. ***Toezicht op zedendelinquenten door de politie in samenwerking met de reclassering***

H.G. van de Bunt, N.L. Holvast & J. Plaisier, Erasmus Universiteit, Rotterdam/Impact R&D, Amsterdam, 2012

41. ***Daders over cameratoezicht***

H.G.A. van Schijndel, A. Schreijenberg, G.H.J. Homburg & S. Dekkers, Regioplan Beleidsonderzoek, Amsterdam, 2012

42. ***Aanspreken op straat. Het werk van de straatcoach in al zijn verschijnings - vormen***

L. Loef, K. Schaafsma & N. Hilhorst, DSP-groep, Amsterdam, 2012

43. ***De organisatie van de opsporing van cybercrime door de Nederlandse politie***

N. Struiksma, C.N.J. de Vey Mestdagh & H.B. Winter, Pro Facto, Groningen/ Kees de Vey Mestdagh, Groningen, 2012

44. ***Politie in de netwerksamenleving. De opbrengst van de politiële netwerkfunctie voor de kerntaken opsporing en handhaving openbare orde en de sturing hierop in de gebiedsgebonden politiezorg***

I. Helsloot, J. Groenendaal & E.C. Warners, Crisislab, Renswoude, 2012

45. ***Tegenspraak in de opsporing. Verslag van een onderzoek***

R. Salet & J.B. Terpstra, Radboud Universiteit Nijmegen, 2012

46. ***Tunnelvisie op tunnelvisie? Een verkennend en experimenteel onderzoek naar de besluitvorming door VKL-teams met betrekking tot het onderkennen van tunnelvisie en andere procesaspecten***

I. Helsloot, J. Groenendaal & B. van 't Padje, Crisislab, Renswoude, 2012

47. ***M.-waarde. Een onderzoek naar de bijdrage van Meld Misdaad Anoniem aan de politionele opsporing***

M.C. van Kuik, S. Boes, N. Kop, M. den Hengst-Bruggeling, T. van Ham & H. Ferwerda, Politieacademie, Apeldoorn/Bureau Beke, Arnhem, 2012

48. ***Seriebrandstichters. Een verkennend onderzoek naar daderkenmerken en delictpatronen***

Y. Schoenmakers, A. van Wijk & T. van Ham, Bureau Beke, Arnhem, 2012

49. ***Van wie is de straat? Methodiek en lessen voor de politie om ongrijpbare veiligheidsfenomenen grijpbaar te maken – op basis van vijf praktijkcasus***

H. Ferwerda, T. van Ham, B. Bremmers, K. Tijhof & M. Grotens, Bureau Beke, Arnhem, 2013

50. ***Recherchesamenwerking in de Euregio Maas-Rijn. Knooppunten, knelpunten en kansen***

H. Nelen, M. Peters & M. Vanderhallen, Politieacademie, Apeldoorn/ Universiteit Maastricht, 2013

51. ***De operationele politiebriefing onderzocht. Een onderzoek naar de effectiviteit van de operationele politiebriefing***

A. Scholtens, J. Groenendaal & I. Helsloot, Crisislab, Renswoude 2013

51a. ***De operationele politiebriefing onderzocht (2). Een actie(vervolg) onderzoek om tot een effectievere politiebriefing te komen***

A. Scholtens, Crisislab, Renswoude 2015

52. ***Sociale media: factor van invloed op onrustsituaties?***

R.H. Johannink, I. Gorissen & N.K. van As, Politieacademie Apeldoorn/ VDMMP, Houten, 2013

53. ***De terugkeer van zedendelinquenten in de wijk***

C.E. Huls & J.G. Brouwer, Politieacademie, Apeldoorn/Rijksuniversiteit Groningen/Centrum voor Openbare Orde en Veiligheid, Groningen, 2013

54. ***Van meld- naar aantoonplicht. Een onderzoek naar een systeem van digitale surveillance***

C. Veen & J.G. Brouwer, Politieacademie, Apeldoorn/Rijksuniversiteit Groningen, 2013

55. ***Heterdaadkracht in twee Haagse pilotgebieden***

B. van Dijk, J.B. Terpstra & P. Hulshof, Politieacademie, Apeldoorn/ DSPgroep, Amsterdam, 2013

56. ***Inzet op Maat. Onderzoek naar kenmerken en mogelijkheden van duurzame inzetbaarheid van oudere medewerkers***

H. de Blouw, I.R. Kolkhuis Tanke & C.C. Sprenger, Politieacademie, Apeldoorn, 2013

57. ***Interventies in de opsporing. Impulsen in kwaliteit en effectiviteit van het opsporingsproces***

R.M. Kouwenhoven, R.J. Morée & P. van Beers, Twynstra Gudde, Amersfoort, 2013

58. ***De plaats delict in beeld. Fotografie in de dagelijkse en gesimuleerde praktijk***

G. Vanderveen & J. Roosma, Instituut voor Strafrecht & Criminologie, Universiteit Leiden, 2013

59. ***Jeugdgroepen van toen. Een casusonderzoek naar de leden van drie criminele jeugdgroepen uit het einde van de vorige eeuw***

H. Ferwerda, B. Beke & E. Bervoets, Bureau Beke, Arnhem/Beke Advies, Arnhem/LokaleZaken, Rotterdam, 2013

60. ***Tussen hei en hoofdbureau. Leiderschapsontwikkeling bij de politie***

W. Landman, M. Brussen & F. van der Laan, Twynstra Gudde, Amersfoort, 2013

61. ***Gemeentelijk blauw. Het dagelijks werk van gemeentelijke handhavers in beeld***

E. Bervoets, J. Bik & M. de Groot, LokaleZaken, Rotterdam, 2013

62. Excessief geweld op en om de voetbalvelden. Praktijkonderzoek naar omvang, ernst en aanpak van 'voetbalgeweld'

P. Duijvestijn, B. van Dijk, P. van Egmond, M. de Groot, D. van Sommeren & A. Verwest, DSP-groep, Amsterdam, 2013

63. Beeld van gezag bij de politie. Maatschappelijke verbeelding en de impact van gezagsbeelden op burgers

H. de Mare, B. Mali, M. Bleecke & G. van den Brink, m.m.v. Motivaction, Tilburg University, Stichting IVMV, Leiden, 2014

64. Informatiegestuurde dienders. Informatiesturing tussen theorie en praktijk

A. van Sluis, P. Siep, V. Bekkers, m.m.v. M. Thaens & G. Straten, Center for Public Innovation, Erasmus Universiteit, Rotterdam, 2014

65. Hard op weg. Onderzoek aanpak verkeersveelplegers

B. Bieleman, M. Boendermaker, R. Mennes & J. Snippe, Intraval, Groningen/Rotterdam, 2014

66. Tussen hulp en hype. De inzet van opsporingsberichtgeving in ontvoeringszaken

Y.M.M. Schoenmakers, J.V.O.R. Doekhie & J.C. Knotter, Yvette Schoenmakers Onderzoek en advies, Weesp, 2014

67. Nachtdienst bij de politie en verkeersveiligheid. Onderzoek naar ervaringen van politieagenten met verkeersonveiligheid in woon-werkverkeer na de nachtdienst

P. Boekhoorn, BBSO, Nijmegen, 2014

68. Buit van woninginbraak. Onderzoek onder inbrekers en helers

J. Snippe, M. Sijtstra, R. Mennes & B. Bieleman, Intraval, Groningen/Rotterdam, 2014

69. Privaat blauw. Portiers, evenementbeveiligers en voetbalstewards op risicovolle locaties en tijdens risicovolle momenten

E. Bervoets & S. Eijgenraam, LokaleZaken, Rotterdam, 2014

70. Met grof geschut. Reconstructie van een moordonderzoek binnen de criminele woonwagenwereld

I. van Leiden, B. Bremmers & H. Ferwerda, Bureau Beke, Arnhem, 2014

71. Met fluwelen handschoenen? Politie en de omgang met verwarde personen in Amsterdam

J. Kuppens, T. Appelman, T. van Ham & A. van Wijk, Bureau Beke, Arnhem, 2015

72a. Vermisten op de kaart. Aard en omvang van langdurige vermissingen

I. van Leiden & M. Hardeman, Bureau Beke, Arnhem, 2015

73. ***Van intel tot operatie. De impact van veiligheidsanalisten bij de aanpak van misdaad***

M. den Hengst, M. Bruinsma, Y. Schoenmakers, W. Niepce, Bureau Bruinsma, Tilburg, 2015

74. ***De bestuurlijke rapportage. Gezamenlijke inspanning in de aanpak van (georganiseerde) criminaliteit en overlast***

I. Gorissen, m.m.v. R.H. Johannink, PBLQ, Den Haag, 2015

75. ***De aangifte van delicten bij de multichannelstrategie van de politie***

P. Boekhoorn & J. Tolsma, Bureau Boekhoorn/Radboud Universiteit, Nijmegen, 2016

76. ***Die pakken we toch niet op? Afstemming tussen politie en Openbaar Ministerie in zaken van veelvoorkomende aangiftecriminaliteit***

R. Kouwenhoven & L. Kleijer-Kool, Twynstra Gudde, Amersfoort, 2016

77. ***Het real-time informeren van noodhulpeenheden. Een onderzoek naar de RTI-functie om frontlijnpolitiefunctionarissen snel te voorzien van relevante informatie***

A. Scholtens, M. den Hengst & R. Waterreus, Crisislab, Renswoude/ Politieacademie, Apeldoorn, 2016

78. ***Hoe lang kun je 'schijt hebben'? Dertien desisters uit criminele jeugdgroepen aan het woord***

C.E. Hoogeveen, A.E. van Burik & B.J. de Jong, m.m.v. E.M. Klooster, Bureau Alpha, 's-Hertogenbosch/VanMontfoort, Woerden, 2016

79. ***Onbenutte kansen. Een onderzoek naar het gebruik van restinformatie in de opsporing***

A. van Wijk & L. Scholten, m.m.v. B. Bremmers, Bureau Beke, Arnhem, 2016

80. ***Verbale leugendetectie-wizards***

G. Bogaard & E.H. Meijer, Maastricht University, Maastricht, 2016

81. ***Mensenhandel in de prostitutie opsporen zonder aangifte? Een vervolgonderzoek om de doorzettingsmacht van de politie te verduidelijken***

M. Goderie, m.m.v. R. Kool, Goderie Onderzoek, Klarenbeek, 2016

82. ***De onvindbaren. Op zoek naar voortvluchtige veroordeelden in Nederland***

Y. Schoenmakers, I. de Groot, J. van Zanten, A. van Rooyen & J. Baars, Yvette Schoenmakers onderzoek & advies, Amsterdam, 2017

83. ***Elke dump is een plaats delict. Dumping en lozing van synthetisch drugsafval: verschijningsvormen en politieaanpak***

Y. Schoenmakers, S. Mehlbaum, M. Everartz & C. Poelarends, Yvette Schoenmakers onderzoek & advies, Amsterdam, 2016

84. ***Naar handhaafbare noodbevelen en noodverordeningen. Een analyse van het gemeentelijke noodrecht***

A.J. Wierenga, C. Post & J. Koornstra, Rijksuniversiteit Groningen, Centrum voor Openbare Orde en Veiligheid, 2016

85. ***Vermisten op het spoor. Rechercheren naar langdurige vermissingen***

I. van Leiden & M. Hardeman, Bureau Beke, Arnhem, 2017

86. ***De aard van het beestje. Kenmerken en achtergronden van dierenmishandelaars***

A. van Wijk & M. Hardeman, Bureau Beke, Arnhem, 2017

87. ***Modus operandi van de recherche. De rechercheprakijk in moord- en verkrachtingszaken***

A. van Wijk, I. van Leiden & M. Hardeman, Bureau Beke, Arnhem, 2017

88. ***Over grenzen in de sport. De rol van de politie in de aanpak van seksueel grensoverschrijdend gedrag in de sport in samenwerking met relevante partners***

A. van Wijk, M. Hardeman, L. Scholten & M. Olfers, Vrije Universiteit Amsterdam, Bureau Beke, Arnhem, 2017

89. ***Defensiehulp. Legergroene bijstand aan de politie bij handhaving van de rechtsorde***

E. Bervoets, m.m.v. S. Eijgenraam, T. Dijkhuizen & J. van de Werken, Bureau Bervoets, Amersfoort, 2017

90. ***Tussen onder en boven. Productie en distributie van softdrugs in Noord-Nederland***

J. Snippe, R. Mennes, M. Sijtstra & B. Bieleman, Intraval, Groningen/Rotterdam, 2017

91. ***Vechten op afspraak. Inzicht in het fenomeen en input voor de ontwikkeling van een politiestrategie***

T. van Ham, L. Scholten, A. Lenders & H. Ferwerda, Bureau Beke, Arnhem, 2018

92. ***Notoire straten. Over de lokale inbedding van georganiseerde criminaliteit***

S. Mehlbaum, Y. Schoenmakers & J. van Zanten, Mehlbaum Onderzoek, Amsterdam, 2018

93. ***Ondermijning door criminele 'weldoeners'***

M. Bruinsma, R. Ceulen & T. Spapens, m.m.v. C. Deij, Tilburg University, Tilburg/Bureau Bruinsma, Tilburg, 2018

94. ***Kiezen voor politie. Een onderzoek onder mbo-studenten met een migratie - achtergrond in het veiligheidsdomein***

S. de Winter-Koçak, E. Klooster & M. Day, m.m.v. S. Mehlbaum, M. van Vugt & K. Leschonski, Verwey-Jonker Instituut, Utrecht, 2018

95. ***Doe-het-zelf-surveillance. Een onderzoek naar de werking en effecten van WhatsApp-buurtgroepen***

S. Mehlbaum & R. van Steden, m.m.v. M. van Dijk, Vrije Universiteit Amsterdam, Mehlbaum Onderzoek, Amsterdam, 2018

96. ***Een klacht is een gratis advies***

G. Jacobs, T. Hak, G. Vanderveen, M. Flory, T. Thuis, S. Valkeman & M. Franken, Erasmus Universiteit, Rotterdam, 2018

97. ***Voortgezet crimineel handelen tijdens detentie: je gaat het pas zien als je het doorhebt***

A. Verwest, W. Buysse, P. van Egmond, D. Hofstra, DSP-groep, Amsterdam, 2019

98. ***Zorg voor kinderen bij aanhouding van ouders; Best practices uit binnen- en buitenland***

J. Reef, N. Ormskerk, Universiteit Leiden, 2019