Dat heeft iemand anders gedaan!

Dat heeft iemand anders gedaan!

Een studie naar slachtofferschap en modus operandi van identiteitsfraude in Nederland

L. Paulissen
J. van Wilsem

POLITIE & Wetenschap

Universiteit Leiden

In opdracht van:
Programma Politie & Wetenschap

Afbeelding omslag:
Alexey Caputin

Ontwerp:
Vantilt Producties & Martien Frijns

ISBN: 978 90 3524 847 2
NUR: 800, 624

Realisatie:
Reed Business, Amsterdam

Inhoud

Voorwoord

Identiteitsfraude is in toenemende mate een probleem in moderne samenlevingen. Door de continue ontwikkeling van ICT wordt steeds vaker bij identificatieprocedures gevraagd om digitale persoonsgegevens, via het online doorgeven van een BSN-nummer, creditcardgegevens, paspoortnummer of inloggegevens. Ook is er veel digitale persoonsinformatie te vinden op sociale-netwerksites zoals Facebook. Er wordt het nodige gespeculeerd over in hoeverre deze ontwikkelingen gepaard gaan met veiligheidsrisico's in de vorm van identiteitsfraude, maar een empirische vaststelling van de aard en omvang daarvan is nog maar beperkt beschikbaar. Ook bestaan er veel vragen over gedragingen die kunnen leiden tot vergroting of juist preventie van deze risico's. Deze studie is bedoeld als een aanzet om meer inzicht te krijgen in de aard, omvang en risicofactoren van slachtofferschap van identiteitsfraude. Aan de hand van een grootschalige, representatieve dataverzameling onder de Nederlandse bevolking wordt de aard en omvang van slachtofferschap van identiteitsfraude geschetst voor de periode 2008-2012. Daarnaast zijn in het voorjaar van 2014 interviews afgenomen onder experts uit het bedrijfsleven en de overheid, om duidelijk te krijgen op welke manieren burgers slachtoffer kunnen worden van identiteitsfraude en hoe daderstrategieën zich ontwikkelen. De studie komt daarmee tegemoet aan de wens die in de Politie & Wetenschap Call 2013 werd uitgesproken om meer zicht te krijgen op het fenomeen identiteitsfraude in Nederland.

Een aantal mensen zijn wij dank verschuldigd voor hun medewerking aan de totstandkoming van dit rapport. Allereerst dank aan de verschillende experts die wij hebben geïnterviewd van de volgende organisaties: de Landelijke Eenheid, het Centraal Meldpunt Identiteitsfraude en -fouten, Nationaal Skimmingpoint, Electronic Crimes Taskforce, Business Forensics, Nederlandse Vereniging van Banken, Fraudehelpdesk, het Expertisecentrum Identiteitsfraude en Documenten, Europol en Team Identiteitsfraude. Daarnaast danken wij de leescommissie, bestaande uit Wim Draaijer (Politieacademie), Wynsen Faber (Faber Organisatievernieuwing/Politieacademie), Nicole van der Meulen (RAND), Eileen Monsma (Staf Landelijke Eenheid) en Christianne de Poot (WODC/Hogeschool

Amsterdam), voor hun heldere en opbouwende commentaar op een tussentijdse versie van het rapport. Tot slot dank aan Marta Dozy en Adriaan Rottenberg, die vanuit Politie & Wetenschap het onderzoek hebben begeleid.

Leiden, februari 2015
Levy Paulissen en Johan van Wilsem

1

Aanleiding

> 'Hoe houd je je identiteit, hoe bewijs je wie je bent? Je wordt een digitaal nummer in een geanonimiseerde maatschappij. Hoe kunnen we dat nog relateren aan een fysieke persoon zonder in een soort van Kafka-achtige situatie te belanden?'
> – Respondent Nederlandse Vereniging van Banken

1.1 Achtergrond

Het fenomeen identiteitsfraude is niet nieuw, maar wel in ontwikkeling. Een van de oorzaken van die ontwikkeling is de digitalisering van de maatschappij. Volgens het Nationaal Cyber Security Centrum (NCSC, 2014) neemt het aantal toepassingen van ICT en internet nog altijd drastisch toe en zijn de Nederlandse burger, het bedrijfsleven en de overheden er steeds sterker van afhankelijk. De burger moet zich op allerlei manieren digitaal identificeren om toegang tot bepaalde diensten te krijgen. In bredere zin vinden veel van onze dagelijkse bezigheden plaats op het internet – internetbankieren, online winkelen, werken, communiceren met vrienden enzovoort. Gepaard hieraan wordt steeds meer van onze persoonsinformatie digitaal opgeslagen door overheden en bedrijven (Bijlsma e.a., 2014). Dit kunnen gebruikersnamen en wachtwoorden zijn, maar ook burgerservicenummers, woonadressen, document- en creditcardnummers. Dit is echter niet zonder risico, want deze opgeslagen informatie vormt voor daders van identiteitsfraude een aantrekkelijk doelwit. Aan de hand daarvan kan men zich immers (digitaal) voordoen als iemand anders en gebruikmaken van diensten – zoals een betaling verrichten of een aankoop doen. Uit een verkennend onderzoek van Schermer en Wagemans (2009) is gebleken dat de gemiddelde Nederlander in 250 tot 500 databanken staat geregistreerd.[1] Burgers en consumenten zijn mede afhankelijk van de nauwkeurig-

1 Wanneer een ruime definitie van het woord 'registratie' wordt gehanteerd, staat de gemiddelde Nederlander volgens de auteurs in duizenden databestanden geregistreerd. In deze ruime definitie van het woord 'registratie' zijn onder andere ook

heid waarmee bedrijven en overheden met hun persoonsgegevens omgaan. Voor hen is dit moeilijk te controleren en vaak weten consumenten ook niet waarmee ze precies akkoord gaan als ze een dienst van een bedrijf of overheid gebruiken, bijvoorbeeld qua privacyvoorwaarden (Bijlsma e.a., 2014). Bijlsma en anderen (2014) stellen: 'Via Facebook delen sommige mensen elk detail van hun persoonlijk leven en het is bijna volledig geaccepteerd dat Google e-mails leest waarvan de verzender of ontvanger een Gmail-adres heeft.' De auteurs vermelden daarnaast dat, hoewel dit bij veel mensen een negatief gevoel oproept, mensen wel gewoon apps downloaden en akkoord gaan met de voorwaarden van Facebook en Whatsapp. Ze constateren dat er sprake is van een privacyparadox: mensen zijn bang dat hun privacy wordt aangetast, maar handelen op een manier waarop dit juist gebeurt.

Niet alleen de hoeveelheid persoonsinformatie die daders kunnen stelen neemt toe, maar ook de methoden waarmee ze de informatie kunnen achterhalen, worden steeds uitgebreider en geavanceerder. Was een dader vroeger aangewezen op het stelen van post, nu zijn er talloze mogelijkheden beschikbaar, die onder andere met behulp van internet ingezet kunnen worden. Voorbeelden hiervan zijn skimming, phishing en het verspreiden van malware. Ook grootschalige datahacks vormen een steeds groter gevaar. In de onderzoeksperiode (april 2013 tot en met maart 2014) van het Cybersecuritybeeld Nederland door het NCSC (2014) is een aantal grootschalige datadiefstallen naar boven gekomen. Deze vonden plaats vanaf met malware besmette computers die weer onderdeel waren van een botnet.[2] Op deze manier zijn honderdduizenden tot enkele miljoenen gebruikersnamen en wachtwoorden buitgemaakt, onder andere van Google, Facebook en Twitter.[3]

Ook de sociale media hebben met het toenemende internetgebruik een hoge vlucht genomen. In 2014 hadden negen miljoen Nederlanders een Facebook-account. Voor LinkedIn ligt dit aantal op vierenhalf miljoen (Oosterveer, 2014). Communicatie loopt steeds minder via fysieke en telefonische wegen, maar is verplaatst naar sociale media. Sociale-mediagebruikers creëren een pro-

---

tijdelijke registraties, inactieve bestanden, nevenbestanden en bestanden die door het publiek over het algemeen niet worden geassocieerd met registratie meegenomen.

2 Een botnet is een netwerk van geïnfecteerde computers. De gebruikers van deze computers zijn zich van deze besmetting niet bewust (of ze hebben ondanks waarschuwingen van de antivirusscanner geen of onvoldoende actie ondernomen). Met een botnet kan de dader allerlei vormen van digitale criminaliteit plegen.

3 Zie: http://t.co/F5qIraMwHa.

fiel met persoonlijke gegevens, en volgens het NCSC (2014) zorgt dit voor een ware dataexplosie: digitale gegevens zijn beschikbaar in een vorm en op een schaal die tot nu toe niet bestonden. Het is daarom niet vreemd dat dit type platform door de omvang en verscheidenheid aan informatie kwetsbaar is. Symantec Corporation (2014) stelt in dit licht dat de aard van phishing en spam aan het veranderen is en dat ze zich verplaatsen van e-mail naar sociale media. Hoewel het verband tussen sociale media en slachtofferschap van identiteitsfraude nog niet veelvuldig is onderzocht, toont onderzoek van Van Wilsem en anderen (2010) aan dat er een relatie bestaat tussen de hoeveelheid persoonlijke informatie die mensen op hun profielen zetten en de kans dat zij te maken krijgen met een onrechtmatige bankafschrijving. De auteurs geven echter wel aan dat er nog meer duidelijkheid moet komen over een oorzakelijke relatie tussen online zichtbaarheid en slachtofferschap van identiteitsfraude.

Wie wordt er slachtoffer van identiteitsfraude? Een belangrijk criminologisch aanknopingspunt voor deze vraag is de mate van gelegenheid die doelwitten bieden bij het uitvoeren van hun dagelijkse (online) bezigheden. Daarmee sluiten we aan bij de routineactiviteitentheorie van Cohen en Felson (1979), die veronderstellen dat het plaatsvinden van delicten mede afhankelijk is van blootstelling aan daders, nabijheid ten opzichte van daders, de mate van bescherming die het doelwit ondervindt en de mate van aantrekkelijkheid van het doelwit voor daders. Oorspronkelijk opgezet als een theorie ter verklaring van offline criminaliteit die de samenkomst vereist van dader en slachtoffer (zoals geweld en diefstal), is de routineactiviteitentheorie ook steeds meer toegepast ter verklaring van verschillen in risico's op online criminaliteit (Bossler, Holt & May, 2012; Reyns, 2013; Van Wilsem, 2013). Voor identiteitsfraude veronderstellen we daarbij dat uiteenlopende internetactiviteiten, zoals online bankieren en sociale-mediagebruik, leiden tot blootstelling van persoonsinformatie aan potentiële fraudeurs: hoe meer men deze activiteiten onderneemt, des te hoger het verwachte risico op slachtofferschap. Bescherming tegen daders heeft voor identiteitsfraude een technologische en een persoonlijke kant: de technologische kant wordt bepaald door de preventiemaatregelen die men neemt, de persoonlijke kant heeft meer met kennis van computers te maken – in hoeverre weet men waar de gevaren zitten en hoe zijn die te om-zeilen (Bossler e.a., 2012)? Aantrekkelijkheid van een doelwit voor identiteitsfraude wordt bepaald door de hoeveelheid waarde: in die zin wordt verwacht dat rijkere doelwitten aantrekkelijker zijn.

Wanneer is iemand slachtoffer geweest van identiteitsfraude? Hoe definiëren we dat? Voordat we ingaan op inhoudelijke aspecten van de thematiek van

identiteitsfraude, is het goed om eerst bij deze vraag stil te staan. Hoewel er vele verschijningsvormen zijn (PwC, 2013b), is het eindresultaat van identiteitsfraude meestal dat er op digitale wijze geld afhandig is gemaakt van het slachtoffer. Hierbij wordt vaak het onderscheid gemaakt tussen fraudegevallen waarbij is 'ingebroken' op de bankrekening en waarbij via andermans creditcard een illegale transactie heeft plaatsgevonden (bijvoorbeeld Harrell & Langton, 2013; Reyns, 2013). Daarnaast zijn er gevallen van identiteitsfraude waarbij het slachtoffer via een andere weg (financiële) schade lijdt (bijvoorbeeld omdat de dader ziektekosten op zijn naam heeft gemaakt, of een misdrijf heeft gepleegd). Slachtofferschap van identiteitsfraude is in de empirische analyses daarom aangemerkt als een incident waarbij de respondent in de enquête zelf aangeeft dat er ten onrechte een geldbedrag van de bankrekening is afgehaald, de creditcardgegevens zonder medeweten zijn gebruikt of er een andere vorm van misbruik van persoonsgegevens heeft plaatsgevonden. Daarmee beoogt de enquête dus niet een meting te zijn van identiteitsdiefstal (waarbij de fraude nog niet heeft plaatsgevonden, alleen de ontvreemding van persoonsgegevens), noch van het creëren van valse identificatiemiddelen. Bovendien sluit de meting (via zelfrapportage door het slachtoffer) niet uit dat er incidenten hebben plaatsgevonden die onder bovengenoemde noemer vallen maar die niet zijn gemeten, omdat het slachtoffer het in de enquête niet heeft aangegeven (bijvoorbeeld omdat hij/zij het is vergeten of er niet over wil praten).

1.2 Identiteitsfraude en de politie

Er zijn allerlei manieren waarop het internet anonimiteit in de hand werkt. Dit is een van de facetten die het opsporen van identiteitsfraude vaak ernstig bemoeilijkt. Digitale identiteiten zijn vaak lastig te koppelen aan onze identiteit in de fysieke wereld. Hoe kan iemand bijvoorbeeld bewijzen dat hij niet degene is geweest die met zijn inlog- en creditcardgegevens online een artikel heeft gekocht? Dat het rechtzetten van deze fouten lastig is en soms jaren kan duren, blijkt onder meer uit ervaringen van slachtoffers (Genova, 2014). Een tweede probleem is dat fraude met een identiteit vaak pas laat wordt ontdekt. Identiteitsfraudeurs proberen zo lang mogelijk onder de radar te blijven en dit doen ze bijvoorbeeld door telkens kleine geldbedragen van iemands rekening af te schrijven, zodat de diefstal niet opgemerkt wordt. Wanneer de fraude pas na enige tijd aan het licht komt, wordt het steeds lastiger het spoor naar de dader te volgen. Mensen weten ook vaak niet hoe en wanneer ze slachtoffer zijn

geworden. Komt het doordat ze ergens een kopie van hun identiteitsbewijs hebben afgegeven, of is hun computer geïnfecteerd met malware? Wanneer iemand erachter is gekomen dat hij/zij slachtoffer is geworden van identiteitsfraude, kan diegene ervoor kiezen aangifte te doen bij de politie. Voorheen was het voor de politie lastig een aangifte op te maken als er sprake was van identiteitsfraude; het werd dan bijvoorbeeld als valsheid in geschrifte of oplichting afgedaan. Hoewel het dus in sommige gevallen mogelijk was een bepaald identiteitsdelict onder een strafbaarstelling te scharen, viel niet alles hieronder. Mede door de toename van slachtofferschap op dit gebied, is identiteitsfraude sinds april 2014 als delict strafbaar gesteld.[4]

Omdat relatief veel slachtoffers van identiteitsfraude geen aangifte doen van het delict dat hun is overkomen (zoals overigens voor meer vormen van cybercrime geldt; zie Domenie e.a., 2013), is het werkaanbod dat bij de politie terechtkomt relatief klein. Mogelijk betreft het bovendien een selectie van de complexere zaken met hoge schadebedragen, waardoor deze delicten duidelijk afwijken van het standaardaanbod van criminaliteit dat zich bij de politie aandient (Wall, 2013). Hoewel er in de afgelopen tien jaar vele veranderingen zijn geweest die de politieorganisatie beter toegerust hebben gemaakt voor het opsporen van cybercrime (verandering wetgeving, beleidsprioritering, opleiding digitaal experts), is de conclusie wel dat '"digitaal" ten onrechte nog geen normaal en integraal onderdeel (is) van de politieorganisatie in de volle breedte' (Stol e.a., 2012). Na de opname van de aangifte van identiteitsfraude ondervindt de politie namelijk diverse moeilijkheden (Stol e.a., 2012): (a) er kunnen territorialiteitsproblemen spelen, omdat identiteitsfraude regelmatig gepleegd wordt door daders vanuit het buitenland, (b) samenwerkingsproblemen kunnen aan de orde zijn als organisaties in het bedrijfsleven erbij betrokken zijn (bijvoorbeeld hack van klantendatabase), (c) er spelen soms onduidelijkheden in de bevoegdheden van digitaal rechercheurs (Koops, 2012), en (d) het vergt vaak veel mankracht, omdat de hoeveelheid bewijsmateriaal regelmatig bijzonder groot is (in bytes) of anderszins moeilijk doorzoekbaar is, door bijvoorbeeld gegevensbeveiliging. Deze facetten tonen aan dat identiteitsfraude een complex probleem vormt voor politie en justitie. Onderzoek kan daarom bij-

4 Strafbaarstelling identiteitsfraude (Dijkhoff, 2014): 'Hij die opzettelijk en wederrechtelijk identificerende persoonsgegevens, niet zijnde biometrische persoonsgegevens, van een ander gebruikt met het oogmerk om zijn identiteit te verhelen of de identiteit van de ander te verhelen of misbruiken, waardoor uit dat gebruik enig nadeel kan ontstaan, wordt gestraft met een gevangenisstraf van ten hoogste vijf jaren of geldboete van de vijfde categorie.'

dragen aan de kennis en de informatiepositie op het gebied van identiteitsfraude verbeteren. Dit is van belang gezien de verwachte groei op het gebied van internetgebruik en dataopslag (Foresight, 2013) en de innovatie door online daders in het anoniem plegen van delicten.

1.3 Doelstelling

Het doel van dit onderzoek is om een recent overzicht te geven van slachtofferschap van identiteitsfraude in Nederland. Dit wordt gedaan door aan de hand van grootschalige, representatieve enquêtegegevens een beeld te schetsen van de omvang, aard, schade en risicofactoren van slachtofferschap van identiteitsfraude voor de periode 2008 tot 2012. Daarnaast wordt aan de hand van expertinterviews stilgestaan bij modus-operandiontwikkelingen van identiteitsfraudeurs.[5] Deze studie is niet de eerste Nederlandse studie die op basis van representatieve slachtoffergegevens identiteitsfraude in kaart brengt (Domenie e.a., 2013; PwC, 2013a; PwC 2013b; Van Wilsem e.a., 2013). Daarnaast geeft het proefschrift van Van der Meulen (2010) weer hoe verschillende actoren in Nederland, maar ook in de Verenigde Staten, identiteitsfraude faciliteren. Zij stelt dat er, onder andere in het kader van veiligheid en het inperken van risico's, steeds meer informatie wordt opgeslagen – fysiek en digitaal. Het ontbreken van de juiste barrières zorgt ervoor dat deze informatie toegankelijk is voor identiteitsdieven. Ook is door het toenemende gebruik van persoonlijke gegevens en de diverse inzet daarvan, de waarde van een identiteit gestegen. PricewaterhouseCoopers (2013b) heeft op basis van slachtofferenquêtes de omvang en schade voor 2012 geschat en stelt op basis van de gegevens dat 4,5 procent van de Nederlandse bevolking slachtoffer is geworden van een vorm van identiteitsfraude. De hieraan gepaarde schade bedraagt naar schatting 355 miljoen euro. In een eerdere studie heeft PwC (2013a) op basis van gegevens van het Centraal Meldpunt Identiteitsfraude en -fouten (CMI) gesteld dat het aantal meldingen bij het CMI stijgt. Van 2010 tot 2012 is het aantal meldingen zelfs met 80 procent toegenomen. Van Wilsem en anderen (2013) kijken onder andere naar individuele schadebedragen van slachtoffers van onrechtmatige bankafschrijvingen en stellen vast dat het gemiddelde brutoschadebedrag voor

5 De bespreking van deze modus operandi vindt plaats op inleidend niveau en vereist geen tot weinig voorkennis van het onderwerp.

slachtoffers in 2008 tot 2010 lag op 433 euro. Omdat meer dan 80 procent van de slachtoffers de brutoschade vergoed heeft gekregen blijft de nettoschade, uitzonderingen daargelaten, vaak dus beperkt onder deze groep.

Op het gebied van risicofactoren biedt de studie van Domenie en anderen (2013) een goed overzicht. In deze studie is geen relatie gevonden tussen achtergrondkenmerken en slachtofferschap van identiteitsfraude. Het risico op dit delict is gelijk verdeeld tussen bijvoorbeeld mannen en vrouwen, maar ook tussen jongeren en ouderen. Bepaalde internetactiviteiten dragen wel bij aan een verhoogd risico op slachtofferschap – voorbeelden hiervan zijn e-mailen, informatie zoeken op het internet en deelname aan datingsites.

Hoewel er dus al meerdere grootschalige studies zijn uitgevoerd naar het fenomeen identiteitsfraude en slachtofferschap, biedt de huidige studie een integraal beeld van de verschillende facetten uit de bovengenoemde onderzoeken, door zowel op de aard, omvang, schade en risicofactoren van slachtofferschap in te gaan als op modus operandi van fraudeurs. Meer concreet is het voor de politie van belang te weten wie slachtoffer wordt van dit delict, hoe groot de schade is bij slachtoffers en wie zich uiteindelijk bij hen meldt voor aangifte. In het bijzonder omtrent de risicofactoren, dat wil zeggen de kenmerken en gedragingen van doelwitten die tot een verhoogde kans op slachtofferschap kunnen leiden, biedt de huidige studie meer gedetailleerde antwoorden dan voorgaande studies. Dat komt door het gebruik van enquêtegegevens uit een grootschalige, representatieve steekproef onder het LISS-panel over veel internetgedragingen (zie 2.2 voor een verdere toelichting hierop).

Om een overzicht te kunnen geven van slachtofferschap van identiteitsfraude in Nederland in de periode 2008 tot 2012, zijn de volgende onderzoeksvragen opgesteld:

1 Hoe vaak deden slachtofferervaringen van identiteitsfraude zich in 2008-2010 en 2010-2012 voor met betrekking tot (a) onrechtmatige bankafschrijvingen, (b) misbruik van creditcard en (c) overige identiteitsfraudevormen (zoals aangeslagen worden voor een verkeersovertreding die een ander heeft begaan)?
2 In hoeverre betreft identiteitsfraude een delict dat een slachtoffer eenmalig meemaakt, of juist bij herhaling?
3 In hoeverre ondervinden slachtoffers van deze uiteenlopende fraudevormen initiële (bruto)- en definitieve (netto)schade? En hoe hoog is daarmee de geschatte totale financiële schade van identiteitsfraude op maatschappelijk niveau?

4 In hoeverre zijn er sociale groepen aan te wijzen die een verhoogd risico lopen op de onderscheiden fraudevormen, wat betreft geslacht, leeftijd, opleidingsniveau en inkomenspositie?
5 In welke mate dragen bepaalde gedragingen of kenmerken van mensen bij aan een verhoogd risico op slachtofferschap van identiteitsfraude, zoals riskante internetgedragingen en lage zelfcontrole?
6 Welke modus operandi hanteren daders van identiteitsfraude en in hoeverre is op dit gebied door de tijd heen een verschuiving te constateren?

De opbouw van dit rapport is als volgt. Ten eerste zullen in hoofdstuk 2 de kwantitatieve en kwalitatieve methoden worden uiteengezet die zijn gebruikt bij het beantwoorden van de onderzoeksvragen. In hoofdstuk 3 zal aandacht worden besteed aan de omvang en aard van slachtofferschap van identiteitsfraude. Ook herhaald slachtofferschap zal in dit hoofdstuk aan bod komen. In hoofdstuk 4 zal worden ingegaan op de financiële schade die slachtoffers, maar ook de maatschappij tussen 2008 en 2012 hebben geleden. Vervolgens zullen in hoofdstuk 5 de risicofactoren en risicogedragingen die samenhangen met slachtofferschap worden besproken. In hoofdstuk 6 wordt de laatste onderzoeksvraag beantwoord, door in te gaan op de diverse modus operandi bij identiteitsfraude. In elk hoofdstuk is daarnaast aandacht besteed aan de bestaande nationale en internationale literatuur over het onderwerp in dat hoofdstuk. Hoofdstuk 7 bevat ten slotte de conclusie en discussie.

2

Methoden

Dit hoofdstuk bevat een overzicht en uitleg van de gebruikte methoden voor het onderzoek naar slachtofferschap en modus operandi bij identiteitsfraude. Als eerste staan we kort stil bij de gehanteerde strategie voor de literatuuranalyse. Vervolgens gaan we in op de gebruikte kwantitatieve gegevens voor het onderzoek naar omvang, schade en risicofactoren van slachtofferschap van identiteitsfraude. Tot slot volgt een uitleg over het kwalitatieve onderzoek dat is uitgevoerd om de modus operandi van identiteitsfraudeurs in kaart te brengen.

2.1 Literatuuranalyse

Om de gevonden resultaten in deze studie te vergelijken met de resultaten uit eerdere nationale en internationale studies, is een literatuuranalyse uitgevoerd. De publicaties zijn gevonden via Web of Science, Google Scholar, online tijdschriften, via de literatuurlijsten van de gevonden artikelen en overige databases. Voor dit onderzoek zijn studies gebruikt die zijn gepubliceerd tussen 2004 en 2014. Artikelen die gepubliceerd zijn voor 2004, zijn vanwege de snelle ontwikkeling van dit delict en dus vanwege mogelijke gedateerdheid niet meegenomen in de analyse. Daarnaast zijn alleen westerse studies meegenomen in de analyse, omdat die het meest geschikt zijn om te vergelijken met de Nederlandse situatie. In totaal zijn 58 publicaties geanalyseerd en gebruikt voor de literatuuranalyse. Hier vallen ook krantenartikelen, online nieuwsartikelen en dergelijke onder. Wanneer alleen gekeken wordt naar wetenschappelijke publicaties, ligt het aantal op 48. Van deze studies zijn er 18 uitgevoerd in Nederland. De overige studies zijn gedaan in de Verenigde Staten, het Verenigd Koninkrijk, Canada en Australië. De meeste onderzoeken zijn gepubliceerd in 2012 en 2013 (n=18). Daarnaast is het aantal publicaties door de tijd heen (van 2004 tot 2014) stabiel. Per jaar zijn er tussen de drie en zes studies gepubliceerd die als relevant zijn aangemerkt voor dit onderzoek. De jaren 2004 en 2011 zijn uitzonderingen, onze selectie bevat voor die jaren één artikel.

2.2 Kwantitatief onderzoek

Voor het beantwoorden van de vragen betreffende de omvang, aard, herhaald slachtofferschap en risicofactoren van slachtofferschap van identiteitsfraude zijn kwantitatieve analyses uitgevoerd. Voor de uitvoering van deze analyse is gebruikgemaakt van gegevens uit een grootschalige, representatieve slachtofferenquête, het LISS-panel. Het Tilburgse onderzoeksinstituut CentERdata is de grondlegger van dit panel en neemt maandelijks, over uiteenlopende onderwerpen, online enquêtes af onder de deelnemers aan dit panel. Tegenover elke enquête die de respondent invult, staat een kleine financiële vergoeding. Wanneer een respondent niet beschikte over een computer en/of een internetverbinding, is een zogenaamde SimPC toegekend waarmee de enquête kan worden ingevuld.

In februari 2010 en februari 2012 zijn vragen in de enquête opgenomen over slachtofferschap van uiteenlopende vormen van identiteitsfraude, over de twee jaar voorafgaand aan de enquête. Gezamenlijk beslaan de metingen van 2010 en 2012 dan ook de periode 2008 tot 2012. De respondenten zijn allen 15 jaar of ouder en zijn door het Centraal Bureau voor de Statistiek via een random steekproeftrekking geselecteerd. Aan het LISS-panel mogen meerdere leden uit een huishouden deelnemen, mits 15 jaar of ouder.[6] In dit onderzoek wordt, wanneer er sprake is van meerdere *slachtoffers* in een huishouden, maar één slachtoffer meegenomen in het onderzoek om dubbeltellingen te voorkomen. Het zou dan namelijk om hetzelfde incident kunnen gaan. De steekproef is getrokken uit de Gemeentelijke Basisadministratie – alleen particuliere huishoudens en mensen die de Nederlandse taal beheersen zijn opgenomen in de steekproef. Vervolgens hebben de geselecteerde respondenten een brochure en brief thuisgekregen om ze te informeren over het panel. Daarna werden ze gebeld met een aantal vragen en om de deelname te bevestigen. In 2010 hebben 5764 respondenten de enquête ingevuld en in 2012 ligt dit aantal op 5709. De responspercentages liggen daarmee op 86,1 procent (2010) en 85,4 procent (2012) van het totaal aantal benaderde personen. Door het werken met een dergelijk grote steekproef kan zelfs bij een relatief zeldzaam verschijnsel, wat de meeste vormen van slachtofferschap zijn, een vrij nauwkeurige schatting worden gegeven van de prevalentie.

Het werken met gegevens uit een slachtofferenquête heeft als voordeel dat

6 In 2010 zijn er 1895 huishoudens waarvan meerdere leden hebben deelgenomen aan de enquête, in 2012 ligt dit aantal op 1874.

er minder sprake is van een *dark number* dan bijvoorbeeld bij politieregistraties: ook incidenten die slachtoffers niet bij politie of bank aangeven, kunnen in de enquête worden gemeld. Dit maakt de meting van de omvang van het probleem waarschijnlijk completer. Wel is het zo dat er in een enquête een beroep wordt gedaan op het geheugen van respondenten – en dit kan om uiteenlopende redenen onjuiste antwoorden opleveren. Enerzijds kunnen respondenten incidenten vergeten of besluiten ze niet te vermelden in de enquête. Anderzijds kunnen respondenten incidenten vermelden die buiten de referentieperiode van de enquête vallen – in dit geval twee jaar – omdat men het incident niet juist in de tijd weet te plaatsen. Foutloos zijn slachtofferenquêtes dus zeker niet op dit punt, hoewel ze voor omvangschattingen wel de voorkeur hebben boven officiële registraties (Bijleveld, 2006).

Een ander voordeel van het werken met slachtofferenquêtegegevens is dat er zowel wat betreft slachtoffers als niet-slachtoffers aanvullende informatie beschikbaar is over kenmerken van die personen. In tegenstelling tot registratiegegevens, waar deze achtergrondinformatie ofwel afwezig ofwel beperkt aanwezig is, kan aan de hand daarvan worden geschetst wat de slachtoffers en niet-slachtoffers van elkaar onderscheidt. Het LISS-panel biedt, ook in vergelijking met andere slachtofferenquêtes (CBS, 2013; Domenie e.a., 2013; PwC, 2013b), veel diepte-informatie over demografische kenmerken, persoonskenmerken en diverse internetgerelateerde gedragingen (sociale media, surfgedrag, preventieactiviteiten).

2.2.1 Beschrijving steekproef

In tabel 2.1 zijn de kenmerken van de respondenten uit 2010 en 2012 weergegeven. In de tabel is te zien dat de man-vrouwverdeling in beide perioden redelijk gelijk is. Dit geldt ook voor de leeftijd van de respondenten, hoewel ouderen (vanaf 55 jaar) in beide perioden het meest vertegenwoordigd zijn. Voor beide perioden is daarnaast te zien dat vmbo in de meeste gevallen de hoogst afgeronde opleiding is. Ten slotte wonen, in beide perioden, de meeste respondenten in een sterk stedelijk gebied, gevolgd door een matig stedelijk gebied. De minste respondenten wonen in een zeer sterk stedelijk gebied.

Tabel 2.1: Overzicht van achtergrondkenmerken van deelnemers aan het LISS-panel in 2010 en 2012

	2010 (N=5764)	2012 (N=5709)
Geslacht		
Man	46,3%	46,7%
Vrouw	53,7%	53,3%
Leeftijd		
15 t/m 24 jaar	11,4%	10,1%
25 t/m 34 jaar	12,6%	11,1%
35 t/m 44 jaar	16,2%	15,8%
45 t/m 54 jaar	18,7%	18,8%
55 t/m 64 jaar	21,9%	21,5%
65 jaar en ouder	19,3%	22,8%
Hoogst afgeronde opleiding		
Basisonderwijs	10,7%	9,8%
Vmbo	26,6%	25,8%
Havo/vwo	10,9%	11,1%
Mbo	21,7%	22,6%
Hbo	21,8%	22,7%
Wo	7,9%	8,1%
Mate van stedelijkheid		
Zeer sterk stedelijk	13,8%	12,3%
Sterk stedelijk	26,2%	26,3%
Matig stedelijk	23,1%	23,9%
Weinig stedelijk	21,8%	22,0%
Niet stedelijk	15,0%	15,4%

De bovenstaande verdelingen zijn vergeleken met bevolkingsgegevens van het CBS. Op die manier is nagegaan in hoeverre de kenmerken van de respondenten in het LISS-panel overeenkomen met de werkelijke verdeling in de Nederlandse populatie (zie bijlage 1, tabel B1.1). Uit deze vergelijking is gebleken dat in het LISS-panel wat meer vrouwen en minder mannen vertegenwoordigd zijn in vergelijking met de nationale populatie van 15 jaar en ouder, waarin er sprake is van een nagenoeg gelijke man-vrouwverdeling. Wanneer de leeftijdscategorieën vergeleken worden van de steekproef en de Nederlandse populatie, valt op dat deze niet veel van elkaar afwijken. In het LISS-panel zijn ouderen (vanaf 55 jaar) enigszins oververtegenwoordigd en zijn jonge mensen (15 t/m 34 jaar) wat ondervertegenwoordigd. Ook op het gebied van opleidingsniveau zijn enige verschillen te constateren. In het LISS-panel bevinden zich meer personen die laagopgeleid zijn en minder personen die als hoogste opleiding middelbaar beroepsonderwijs hebben afgerond, dan verwacht mag worden op

basis van de Nederlandse populatie. Het percentage hoogopgeleiden verschilt niet veel, maar ligt in het LISS-panel wat hoger. Ten slotte is ook de mate van stedelijkheid vergeleken. De drie middelste categorieën (sterk stedelijk, matig stedelijk en weinig stedelijk), komen voor de Nederlandse populatie en de respondenten in het LISS-panel redelijk goed overeen. De categorie 'zeer stedelijk' is echter in het LISS-panel ondervertegenwoordigd – andersom geldt dat de categorie 'niet stedelijk' oververtegenwoordigd is in het LISS-panel. Samenvattend zien we weliswaar wat verschillen in de verdeling van de beschreven achtergrondkenmerken tussen de Nederlandse bevolking en de deelnemers van het LISS-panel, maar blijven deze verschillen beperkt. Om te corrigeren voor discrepanties tussen de steekproef en de populatie – die mogelijk kunnen leiden tot een vertekend beeld – zijn de data gewogen op basis van geslacht, leeftijd, opleidingsniveau en stedelijkheid voor de schatting van de omvang van slachtofferschap van identiteitsfraude. Ondervertegenwoordigde groepen in het LISS-panel hebben daardoor een wat groter gewicht in de schatting gekregen en oververtegenwoordigde groep juist een wat kleiner gewicht.

2.2.2 Slachtofferschap identiteitsfraude

Om *slachtofferschap* vast te stellen, is de respondenten gevraagd aan te geven of ze de twee voorafgaande jaren slachtoffer zijn geworden van de volgende vormen van identiteitsfraude: (a) 'er is geld van de bankrekening afgeschreven zonder dat u daar toestemming voor had gegeven', (b) 'uw creditcardnummer werd achterhaald en, buiten uw medeweten, gebruikt voor een aankoop', (c) 'iemand heeft uw persoonlijke gegevens gebruikt voor identiteitsfraude (bijvoorbeeld doordat iemand zich voor u uitgaf na het begaan van een overtreding, bij het gebruikmaken van medische zorg, of de aanvraag van een hypotheek)'.

De respondenten konden hier 'ja', 'nee' of 'wil ik niet zeggen' op antwoorden. Daarnaast is ook gevraagd *hoe vaak* ze in die twee jaar slachtoffer zijn geworden van dat misdrijf. Om vast te stellen of de respondenten *schade* hebben geleden is aan slachtoffers van bankfraude gevraagd hoeveel geld (in euro's) was afgeschreven van de bankrekening. Daarna is gevraagd of ze deze oorspronkelijke (bruto)schade niet, geheel of deels vergoed hebben gekregen. Ten slotte is de vraag gesteld hoeveel financiële schade ze uiteindelijk hebben geleden door het incident (nettoschade). Aan slachtoffers van creditcardfraude zijn deze aanvullende vragen – vanwege ruimtebeperkingen – niet gesteld. Aan slachtoffers van overige fraude is gevraagd hoeveel geld en tijd ze kwijt zijn geweest aan het

rechtzetten van het incident. Aangezien deze groep erg klein is, zal hier niet verder op worden ingegaan.

2.2.3 Overige respondentkenmerken

Aan alle respondenten zijn vragen gesteld over aanvullende kenmerken. De volgende *achtergrondkenmerken* zijn daarbij onderscheiden: geslacht, leeftijd, stedelijkheid woonplaats, netto-maandinkomen, opleidingsniveau, alleenstaand zijn. Daarnaast is een uitgebreid scala aan *internetgedragingen* toegevoegd aan de analyses, zoals internetbankieren, chatten en online aankopen doen. Ook is er informatie over het gebruik van sociale media, zoals het aantal sociale-netwerksites waarop men een profiel heeft, en meer specifiek of men de volgende zaken daarop heeft geplaatst: (a) achternaam, (b) leeftijd, (c) adres, (d) telefoonnummer, (e) e-mailadres en (f) foto's. Verder is geschat hoeveel kennis van computers respondenten hebben en in hoeverre ze hun computer thuis hebben beschermd door middel van (a) firewall, (b) virusscanner, (c) antispy-software, (d) trojanscanner, (e) spamfilter en (f) wifi-beveiliging. Ten slotte is gemeten over hoeveel zelfcontrole de respondent beschikt. Over een aantal variabelen volgt hieronder een toelichting.

Zelfcontrole

In de analyses is de variabele impulsiviteit meegenomen, die een afspiegeling biedt van de mate van zelfcontrole van een respondent. De vraag is of mensen met een hoger niveau van impulsiviteit, en dus met een lager niveau van zelfcontrole, meer kans lopen op slachtofferschap. Hiervoor is een schaalvariabele aangemaakt (Cronbach's $\alpha = 0.736$ (2010) en $\alpha = 0.733$ (2012)).[7] Respondenten hebben 12 stellingen met 'oneens' of 'eens' beantwoord, waaruit hun mate van impulsiviteit is gebleken zoals, 'ik zeg en doe vaak dingen zonder rekening te houden met de gevolgen', 'ik denk vaak onvoldoende na voordat ik iets doe' en 'ik maak geregeld afspraken zonder na te denken of ik ze ook daadwerkelijk kan nakomen'. Wanneer iemand hier hoog op scoort, kan gezegd worden dat diegene een laag niveau van zelfcontrole heeft.

7 Cronbach's Alpha neemt een waarde aan die aangeeft of respondenten consistent hebben geantwoord op de vragen in de schaalvariabele. Deze waarde moet boven de 0.70 liggen voor een betrouwbaar resultaat.

Sociale media

In de enquête zijn ook vragen opgenomen over het gebruik van sociale media. Aan de respondenten is gevraagd of ze een of meerdere profielen op sociale-netwerksites hebben. De respondenten konden dit aangeven voor 13 sites, zoals Facebook, LinkedIn, Youtube en Hyves. Aan de hand van die vragen is één variabele opgesteld, die aangeeft van hoeveel sociale-netwerksites de respondenten lid zijn. In deze context is ook gevraagd welke persoonlijke gegevens ze naar waarheid hebben ingevuld op de sites waar ze lid van zijn. Dit is gevraagd voor de persoonsgegevens achternaam, leeftijd, adres, telefoonnummer, e-mailadres en foto's. Gekeken is of de respondent die gegevens wel of niet op ten minste een van de sites heeft vermeld.

Computerbeveiliging

Naast het gebruik van sociale media is ook gekeken naar beveiligingsmaatregelen die de respondenten hebben getroffen op hun computer. Op de vraag of ze bepaalde maatregelen hadden geïnstalleerd, konden de respondenten 'ja', 'nee' of 'weet ik niet' antwoorden. De preventiemaatregel die de respondent heeft genomen, is alleen geteld als de respondent aangaf die voorafgaand aan het slachtofferschap te hebben geïnstalleerd. De vraag die in dit kader beantwoord moest worden luidt als volgt: 'Hebt u de onderstaande maatregel(en) genomen nadat u slachtoffer bent geweest van een digitaal misdrijf'. Alleen als dit niet het geval is, is er meer zekerheid over de causale volgorde en kan worden gekeken of het nemen van preventieve maatregelen ook werkelijk invloed heeft op slachtofferschap.

Kennis van computers

Ten slotte is een variabele aangemaakt die beoogt in te schatten hoeveel verstand de respondent van computers heeft. Dit wordt namelijk beschouwd als een indicator voor de mogelijkheden tot persoonlijke bescherming tegen cybercrime, die dus van invloed kan zijn op slachtofferschap (zie ook Bossler e.a., 2012). Voor de aanmaak van deze variabele is gevraagd of respondenten wisten welke beveiligingsmaatregelen ze op hun computer hadden genomen, voor in totaal vijf maatregelen (zoals firewall en virusscanner). Van hoe meer

maatregelen respondenten dit niet wisten, des te lager is de ingeschatte kennis van computers. Weliswaar is dit geen sluitende meting voor dit concept, maar wel de enige die met deze gegevens mogelijk is.

2.3 Kwalitatief onderzoek

Om de onderzoeksvraag omtrent de modus operandi te beantwoorden, zijn interviews afgenomen onder experts op het gebied van identiteitsfraude. Aangezien slachtoffers vaak niet weten hoe ze met identiteitsfraude in aanraking zijn gekomen, zijn verschillende organisaties benaderd om meer zicht te krijgen op de werkwijze van identiteitsfraudeurs. Dit is gedaan via meerdere methoden. Ten eerste is een aantal experts in ons netwerk benaderd. Volgens de sneeuwbalmethode is vervolgens aan die experts gevraagd of zij contact wilden leggen met andere experts in hun netwerk. Ten slotte is ook bekeken welke organisaties nog meer relevant zouden zijn voor het onderzoek, en deze zijn telefonisch of via een e-mailadres op de website benaderd. In totaal zijn 12 respondenten van negen organisaties geïnterviewd. De volgende organisaties hebben deelgenomen aan het onderzoek: Centraal Meldpunt Identiteitsfraude en -fouten (CMI), Nederlandse Vereniging van Banken (NVB), Nationaal Skimmingpoint, Electronic Crimes Taskforce (ECTF), Europol, Business Forensics, Fraudehelpdesk, Team Identiteitsfraude (TIF) en het Expertisecentrum Identiteitsfraude en Documenten (ECID) van de Koninklijke Marechaussee. Hiermee is een breed scala aan organisaties vertegenwoordigd, zowel publiek als privaat, die ieder deels weer met andersoortige problematiek omtrent identiteitsfraude worden geconfronteerd. Bij het CMI is een senior medewerker geïnterviewd met ruime ervaring op het gebied van identiteitsfraude en administratie (GBA) van burgers. Het CMI is, zoals de naam al indiceert, een meldpunt voor burgers die in aanraking zijn gekomen met identiteitsfraude. De respondent van het CMI is op de hoogte van de aard van deze meldingen, de hoeveelheid meldingen en welke ontwikkelingen zich op dit gebied voordoen. Tijdens het interview met de NVB is gesproken met een afdelingshoofd die vanuit haar functie ruime ervaring heeft met beheersing van identiteitsfraude met een financiële component. Bij Europol is een gesprek gevoerd met drie medewerkers, onder wie een operationeel teamleider van de afdeling EC3 (afdeling digitale criminaliteit Europol) en twee strategisch analisten. Allen zijn ze betrokken bij het uitvoeren van opsporingsonderzoeken, werken ze samen met nationale en internationale partners en zijn ze goed geïnformeerd over de laatste trends en

ontwikkelingen. Daarnaast is bij Business Forensics en Skimmingpoint gesproken met respectievelijk de managing partner van het bedrijf en het unithoofd Recherche Expertise waaronder Skimmingpoint valt. De medewerker van Skimmingpoint is expert op het gebied van skimming en om die reden is er ook voor gekozen aan deze respondent alleen vragen over skimming te stellen. De respondent van Business Forensics heeft veel ervaring in de private sector op het gebied van onder andere *big data* en *data security*. Bij het ECTF zijn twee interviews afgenomen, één met een oud-projectleider en één met een huidig projectleider; beide respondenten zijn altijd nauw betrokken geweest bij projecten op het gebied van financiële identiteitsfraude en werkten daarin ook nauw samen met het bankwezen. Daarnaast is bij de Fraudehelpdesk en de Koninklijke Marechaussee respectievelijk gesproken met een fraude-expert en de leidinggevende van team ECID. De medewerker van de Koninklijke Marechaussee was voornamelijk gespecialiseerd in identiteitsfraude middels het misbruiken van een identiteitsbewijs. De respondent geïnterviewd van de Fraudehelpdesk is op de hoogte van meldingen die binnenkomen en de ontwikkelingen en trends die daaraan gerelateerd zijn. Ten slotte is de medewerker van Team Identiteitsfraude voornamelijk gespecialiseerd op het gebied van het misbruiken van identiteitsbewijzen en werkt daarbij nauw samen met de gemeente Amsterdam (voor een overzicht van de gehouden interviews zie bijlage 2, tabel B2.1).

Om de resultaten goed met elkaar te kunnen vergelijken, maar ook om de experts de ruimte te geven dieper op hun expertise in te gaan, is gekozen voor het houden van semigestructureerde *face-to-face* interviews. De vragenlijst is voor afname van de interviews naar de experts gestuurd, zodat ze zich goed konden voorbereiden op de inhoud van de vragen en eventueel cijfers en dergelijke konden presenteren. Hoewel de meeste interviews face-to-face zijn afgenomen, zijn twee interviews om praktische redenen telefonisch gehouden.[8] Vanwege transcriptie zijn alle interviews, met toestemming van de respondent, met een voicerecorder opgenomen. De interviews duurden alle tussen de 60 en 90 minuten. Alvorens de interviews bij de respondenten zijn afgenomen, is een pilotinterview afgenomen bij een respondent die werkzaam is bij de Landelijke Recherche en bekend is met het onderwerp. Deze pilot is gehouden om te kijken of de vragen duidelijk en begrijpelijk waren en of bepaalde vragen toegevoegd of verwijderd moesten worden.

Elk interview startte met vragen aan de respondent over zijn of haar achtergrond en huidige functie. Vervolgens zijn de volgende onderwerpen aan bod

8 Business Forensics en Skimmingpoint.

gekomen: populaire methoden om identiteitsfraude te plegen, methoden die aan het verdwijnen zijn, technisch ingewikkelde methoden, samenwerking tussen daders, taakverdeling tussen daders, het internationale karakter van identiteitsfraude, het maken van winst door daders, sociale-netwerksites, corrupte medewerkers en overige ontwikkelingen. Daarnaast is tijdens de interviews aan de respondenten een schema getoond met de modus operandi die in de literatuur naar voren kwamen (zie bijlage 2, figuur B2.1). Aan de respondenten is gevraagd of ze deze indeling terugzagen in de praktijk. Vanwege de diversiteit aan respondenten en hun kennis op het gebied van identiteitsfraude, waren de respondenten niet altijd in staat alle vragen te beantwoorden die hun waren gesteld (de respondenten van het ECTF hebben bijvoorbeeld voornamelijk kennis over de modus operandi malware en phishing, omdat ze zich richten op 'electronic crime'). Wanneer dit het geval is, is dit in de resultatensectie aangegeven. Na afronding van de interviews, zijn deze getranscribeerd en geanalyseerd (zie bijlage 2 voor het volledige interview).

2.4 Samengevat

- Naast een uitgebreide literatuuranalyse omtrent slachtofferschap van identiteitsfraude zijn er voor dit onderzoek ook kwantitatieve en kwalitatieve gegevens verzameld.
- De kwantitatieve gegevens zijn afkomstig uit het LISS-panel en in februari 2010 en februari 2012 door het Tilburgse onderzoeksbureau CentERdata verzameld.
- Het betreft in beide gevallen een representatieve steekproef van huishoudens onder de bevolking van 16 jaar en ouder, van ruim 5700 respondenten.
- Er zijn uitgebreide gegevens verzameld over slachtofferschap van identiteitsfraude en kenmerken van de respondent, zoals internetgebruik, gebruik van beschermingsmaatregelen voor de pc en zelfcontrole.
- Kwalitatieve gegevens zijn verzameld via halfgestructureerde interviews bij 12 experts op het gebied van identiteitsfraude, onder meer van het Centraal Meldpunt Identiteitsfraude, de Nederlandse Vereniging van Banken en het fraudedetectiebureau Business Forensics. Deze waren vooral bedoeld om zicht te krijgen op de door identiteitsfraudeurs gehanteerde modus operandi.

3

Aard en omvang van slachtofferschap

Hoe vaak deden slachtoffererervaringen van identiteitsfraude zich in 2008-2010 en 2010-2012 voor met betrekking tot (a) onrechtmatige bankafschrijvingen, (b) misbruik van creditcard en (c) overige identiteitsfraudevormen (zoals aangeslagen worden voor een verkeersovertreding die een ander heeft begaan)?

In hoeverre betreft identiteitsfraude een delict dat een slachtoffer eenmalig meemaakt, of juist bij herhaling?

3.1 Analyse van Nederlandse literatuur

Om de twee bovenstaande onderzoeksvragen te beantwoorden, is ten eerste nagegaan wat er tot dusver bekend is in de literatuur over de omvang, aard en herhaald slachtofferschap van identiteitsfraude. Na bestudering van de publicaties over de *omvang* van identiteitsfraude, is het niet mogelijk een eenduidig beeld daarvan te schetsen. Dit ligt onder andere aan het feit dat de studies vaak verschillende definities hanteren, en daardoor identiteitsfraude uiteenlopend operationaliseren. Zo wordt in de ene studie identiteitsfraude als algemeen begrip gemeten, in andere studies wordt gevraagd naar specifieke verschijningsvormen (zoals creditcardfraude) en een derde groep zijn studies die specifiek vragen naar identiteitsfraude die men op digitale wijze is overkomen. In de analyse van de literatuur hebben we deze verschillende operationaliseringen meegenomen. Dat geldt niet voor slachtofferloze vormen van identiteitsfraude die aan de hand van fysieke documenten wordt gepleegd, bijvoorbeeld waarbij de dader zijn of haar eigen paspoort heeft vervalst.

Volgens de resultaten van de Nederlandse studies is ongeveer 12 tot 16 procent van de Nederlandse bevolking *ooit* slachtoffer geweest van een vorm van identiteitsfraude (Dynamics/Fellowes, 2012; PwC, 2013b). De schattingen voor de omvang van slachtofferschap *per jaar* lopen flink uiteen, van 0,9 tot 5 procent (Van Wilsem, 2012; Domenie e.a., 2013, CBS, 2013; PwC, 2013b). Het onder-

zoek van PricewaterhouseCoopers (2013b) onderscheidt verschillende vormen van identiteitsfraude en is afgenomen onder een representatieve steekproef van de Nederlandse bevolking. Deze studie geeft ook een goed beeld van de *aard* van identiteitsfraude, door een onderscheid te maken in financiële, digitale, medische, criminele en overige identiteitsfraude. Uit de resultaten is gebleken dat bijna de helft, namelijk 46 procent van de slachtoffers, de dupe is geworden van financiële fraude. Deze vorm wordt gevolgd door fraude via het internet (18%), overige fraude (15%), criminele fraude (11%) en medische fraude (9%). Naast PricewaterhouseCoopers (2013b) zijn ook de studies van Domenie en anderen (2013) en het Centraal Bureau voor de Statistiek (2013) gebaseerd op een representatieve steekproef onder Nederlandse burgers. Deze studies geven dus een goed inzicht in de omvang en aard van in de studie gemeten varianten van identiteitsfraude in Nederland. Wanneer gekeken wordt naar alleen identiteitsfraude met een *digitale component* lopen de cijfers van 0,8 tot 1,5 procent slachtoffers in Nederland per jaar (Domenie e.a., 2013; CBS, 2013). Wanneer ook andere (offline) vormen van identiteitsfraude worden meegenomen, liggen de cijfers rond 4,5 procent slachtoffers per jaar (PwC, 2013b).[9]

Uit de literatuuranalyse is verder gebleken dat er zeer weinig bekend is over herhaald slachtofferschap van identiteitsfraude. Slechts één Nederlandse studie heeft hier onderzoek naar gedaan (Van Wilsem e.a., 2010). Van de onderzochte respondenten (n= 983) heeft 4,3 procent een onrechtmatige bankafschrijving meegemaakt in de twee jaar voor de enquête – hiervan is 25 procent herhaald slachtoffer geworden. De respondenten in deze studie waren echter allen student of scholier en vormen dus een selectieve steekproef. Bovendien was de steekproefgrootte van circa duizend, gezien de zeldzaamheid van met name *herhaald* slachtofferschap, aan de kleine kant. Meer inzicht in herhaald slachtofferschap is dan ook gewenst, ook omdat het plausibel is te veronderstellen dat als de identiteit van iemand kwetsbaar is gebleken, het voor een dader interessant is deze meerdere malen te misbruiken.

9 Een vorm van identiteitsfraude die in maar weinig studies is onderzocht, is fraude met documenten. Uit een studie van het Expertisecentrum Identiteitsfraude en Documenten (2014) is gebleken dat fraude met documenten stijgt. Dit zijn documenten die ter controle worden aangeboden bij de Falsification Schiphol Desk (FSD) en waar fraude mee is gepleegd. In 2013 is fraude geconstateerd bij 2,7 procent van de documenten die werden aangeboden. In 2012 en 2011 bedroeg dit percentage 2,4 procent en in 2010 lag dit op 2,3 procent. Het ECID stelt wel dat het niet is vast te stellen of deze stijging verklaard kan worden door een werkelijke toename van documentfraude, of dat er externe factoren van belang zijn die deze cijfers beïnvloeden. Dit rapport is een intern, niet-openbaar document en is om die reden niet opgenomen in de literatuur.

3.2 Analyse van internationale literatuur

De resultaten uit de literatuur over identiteitsfraude in Nederland zijn vergeleken met resultaten uit de Verenigde Staten, Europa, Australië en Canada. Uit een grootschalige, representatieve *survey* (n=69.814) gehouden onder de Amerikaanse bevolking (NCVS), is gebleken dat in 2012 circa 7 procent van de burgers slachtoffer is geworden van een of meer vormen van identiteitsfraude (Harrell & Langton, 2013). De survey richtte zich op misbruik van een bestaand account (van telefoonabonnementen tot creditcardaccounts), misbruik van gegevens om een nieuw account te openen en misbruik van gegevens voor frauduleuze doeleinden. Andere Amerikaanse studies op het gebied van identiteitsfraude laten uiteenlopende cijfers zien. De cijfers lopen uiteen van 4,6 procent in 2002 (Anderson, 2006), 2 procent in 2005 (Copes e.a., 2010), 3,7 procent in 2005 (Anderson e.a., 2008) tot 9,2 procent in 2012 (Holt & Turner, 2012). De tijdreeks die door Javelin Strategy and Research (2014) op basis van periodieke slachtofferenquêtes onder de Amerikaanse bevolking is vastgesteld, laat zien dat er een stijging was in het aantal slachtoffers van *existing account fraud* tussen 2006 en 2009 en dat er sinds de daling van 2010 weer een gestage stijging is, tot een niveau van 5 procent van de Amerikaanse bevolking in 2013 (circa 13 miljoen personen). Een alternatieve databron vormen de meldingen van het Amerikaanse Identity Theft Resource Center (ITRC). Hier melden zich slachtoffers van met name ernstige vormen van identiteitsfraude, die vaak ook met veel financiële en emotionele gevolgen gepaard gaan (ITRC, 2013). Als instrument voor omvangsschatting is zij echter niet geschikt, gezien het beperkte aantal van 201 slachtoffers dat werd geregistreerd.

In Australië is volgens Smith en Hutchings (2014) 20,8 procent van de bevolking ooit slachtoffer geworden van misbruik van persoonlijke informatie. Deze resultaten zijn afkomstig uit een representatieve survey afgenomen onder bijna vijfduizend respondenten. Ook is de respondenten gevraagd of ze slachtoffer zijn geworden van identiteitsfraude in het jaar voorafgaand aan de survey (2012 tot 2013). Dit percentage lag op 9,4 procent. De meeste respondenten zijn slachtoffer geworden van misbruik van hun bankrekening (35,4%), gevolgd door een koop op hun naam (32,5%) en het aanvragen van een lening of krediet op hun naam (8,1%). Ten slotte blijkt dat in Canada elk jaar ongeveer één miljoen burgers slachtoffer worden van identiteitsfraude. Dit percentage fluctueert van 4 tot 9,1 procent van de totale bevolking per jaar (Sproule & Archer, 2008).

Ook binnen Europa zijn er enkele studies gedaan naar de prevalentie van identiteitsfraude. Onderzoek van Dynamics/Fellowes (2012) laat zien dat 17

procent van de Europeanen *ooit* slachtoffer is geworden van identiteitsfraude. Het Verenigd Koninkrijk is in deze studie koploper met 24 procent. De UK National Fraud Authority (2012) stelt dat 9,4 procent van de Britse burgers in 2011 slachtoffer is geworden van identiteitsfraude. Na het Verenigd Koninkrijk volgen Rusland (20%), Spanje (18%) en Polen (17%). Volgens het onderzoek van Dynamics/Fellowes is 12 procent van de Nederlandse bevolking ooit slachtoffer geweest van identiteitsfraude. Europol (2013) schat op basis van een onderzoek van de Europese Commissie dat 8 procent van de Europese internetgebruikers identiteitsdiefstal heeft meegemaakt. De periode waarvoor deze 8 procent geldt, wordt in het rapport niet gespecificeerd.

De internationale literatuur naar de aard van identiteitsfraude laat zien dat het misbruiken van een creditcard in de Verenigde Staten de meest prevalente vorm van identiteitsfraude is (Newman & McNally, 2005; Anderson, 2006; Winterdyk & Thompson, 2008; Sproule & Archer, 2008; Copes e.a., 2010). Vaak wordt er in de Amerikaanse literatuur ook een onderscheid gemaakt tussen identiteitsfraude met een bestaand account en identiteitsfraude waarbij persoonlijke gegevens worden misbruikt om een nieuw account te openen. Uit de resultaten is gebleken dat identiteitsfraude met een bestaand account de meest voorkomende vorm is (Anderson e.a., 2008; Copes e.a., 2010; Harrell & Langton, 2013). In Nederlandse studies wordt dit onderscheid niet gemaakt. Herhaald slachtofferschap wordt, net als in de Nederlandse literatuur, in de internationale literatuur naar identiteitsfraude weinig onderzocht. Smith en Hutchings (2014) stellen op basis van een Australische studie dat iets minder dan de helft van de slachtoffers (46,3%) dacht dat ze herhaald slachtoffer waren geworden. Ten slotte concluderen Newman en McNally (2005) op basis van wetenschappelijke literatuur dat 65 procent[10] van de slachtoffers van identiteitsfraude, binnen vijf jaar weer slachtoffer wordt van een vorm van identiteitsfraude.

3.3 *Analyse LISS-paneldata*

Voor dit rapport is naast een literatuurinventarisatie ook nieuw onderzoek verricht via analyses op het LISS-paneldata (zie hoofdstuk 2), om de omvang, aard en herhaald slachtofferschap van identiteitsfraude in kaart te brengen. Deze

10 Dit percentage is gebaseerd op een surveyonderzoek in de Verenigde Staten (*n*=4057) van de Federal Trade Commission. Zie Synovate (2003). *Federal Trade Commission – Identity Theft Survey Report*. McLean, VA. http://www.ftc.gov/os/2003/09/synovatereport.pdf.

resultaten gelden voor Nederland voor de periode 2008 tot 2012. De omvang is berekend voor de uiteenlopende verschijningsvormen afzonderlijk (onrechtmatige bankafschrijving, misbruik van een creditcard en misbruik van persoonlijke informatie voor fraudeleuze doeleinden) en in totaal. Uit de resultaten is gebleken dat 3,5 procent van de respondenten in de periode 2008 tot 2010 slachtoffer is geworden van een onrechtmatige bankafschrijving (zie tabel 3.1). Voor misbruik van een creditcard ligt dit percentage op 1,0 procent en voor de overige fraude (ook wel misbruik persoonlijke informatie genoemd) op 0,3 procent. Opgeteld is de omvang van identiteitsfraude voor deze drie gezamenlijk 4,6 procent in de periode 2008 tot 2010. Voor de periode 2010 tot 2012 blijkt dat de afzonderlijke vormen nagenoeg gelijk in om-vang zijn gebleven: 3,5 procent werd slachtoffer van een onrechtmatige bankafschrijving, 0,9 procent van creditcardfraude en 0,4 procent van overige fraude. Het aantal personen dat tussen 2010 en 2012 slachtoffer is geworden van een van deze vormen van identiteitsfraude is ongewijzigd ten opzichte van de periode daarvoor: 4,6 procent.

Tabel 3.1: Percentage slachtofferschap gedurende 2008 tot 2010 en 2010 tot 2012 [11, 12]

Omvang	2008-2010	2008-2010 95% BI	2010-2012	2010-2012 95% BI
Bank	3,6	[3,1, 4,1]	3,5	[3,0, 4,0]
Creditcard	1,0	[0,7, 1,2]	0,9	[0,7, 1,2]
Overige fraude	0,3	[0,2, 0,4]	0,4	[0,2, 0,6]
Totaal	4,6	[4,1, 5,2]	4,6	[4,0, 5,1]
N	5764		5709	

Een ander grootschalig en representatief Nederlands onderzoek op dit gebied van PricewaterhouseCoopers (2013b) laat weliswaar een nagenoeg vergelijkbaar percentage zien van 4,5 procent voor het jaar 2012, maar verschilt op twee belangrijke aspecten van onderhavige studie. Ten eerste heeft de PwC-studie betrekking op een periode van één jaar in plaats van twee, en de PwC-studie hanteert een andere en ruimere definitie van identiteitsfraude.[13] Wanneer ande-

11 Gewogen op basis van geslacht, leeftijd, opleidingsniveau en urbanisatiegraad.

12 95%-betrouwbaarheidsintervallen: de ondergrens en bovengrens zijn hierbij aangegeven.

13 Hierbij wordt onderscheid gemaakt naar a) financiële identiteitsfraude, b) criminele identiteitsfraude, c) misbruik van naam en BSN bij een huisarts of ziekenhuis, d) identiteitsfraude op het web, bijvoorbeeld gebruik van naam om op het internet producten aan te schaffen en e) overige vormen (PwC, 2013b).

re westerse landen met de uitkomsten uit de data worden vergeleken, valt op dat andere westerse landen een hoger prevalentiepercentage hebben. Zo is in de Verenigde Staten 7 procent van de bevolking in 2012 slachtoffer geworden van identiteitsfraude, terwijl dat in het Verenigd Koninkrijk (2011) en Australië (2012-2013) 9,4 procent was. Hoewel de percentages voor Nederland hieronder liggen moet bij de vergelijking met andere landen uiteraard de nodige voorzichtigheid in acht worden genomen, gezien de verschillen die er zijn in vraagstelling, steekproeftrekking en wijze van afname van de enquête.

Naast de prevalentie is ook in kaart gebracht hoe de verschillende vormen van identiteitsfraude zich verhouden tot elkaar (tabel 3.2). Dat levert voor de twee perioden 2008 tot 2010 en 2010 tot 2012 een vergelijkbaar beeld op. De grote meerderheid (meer dan 70%) betrof slachtofferschap van bankfraude. Het aandeel van creditcardfraude schommelde in beide perioden rond de 20 procent, terwijl de overige fraude 6 à 7 procent[14] van het totaal in beslag nam. Dit is al met al een ander beeld dan in de Verenigde Staten, waar creditcardfraude juist de meest prevalente manier van identiteitsfraude is (bijvoorbeeld Harrell & Langton, 2013).

Tabel 3.2: Aard van identiteitsfraude gedurende 2008-2010 en 2010-2012, in procenten

	2008-2010	2010-2012
Bank	74,2	71,7
Creditcard	19,6	21,1
Overig	6,2	7,2
Totaal	100	100
N	260	265

Ten slotte is gekeken naar herhaald slachtofferschap en aan slachtoffers van verschillende vormen van slachtofferschap gevraagd hoe vaak ze slachtoffer zijn geworden van hetzelfde delict in een tweejaarsperiode. De resultaten zijn weergegeven in tabel 3.3.

14 Slechts een klein aantal respondenten valt in de categorie misbruik van persoonlijke informatie ('Overig' in tabel 3.2). Om enig zicht te krijgen op de ervaringen van deze slachtoffers, is hun gevraagd de situatie te typeren waar ze zich in bevonden. Dit leverde uiteenlopende antwoorden op, zoals gebruikmaken van medische diensten, aanvragen van een financieel product en overtreding begaan, allen op naam van het slachtoffer.

Tabel 3.3: Aantal keer slachtofferschap bankfraude, creditcardfraude en overige fraude in tweejaarsperiode, 2008-2010 en 2010-2012 in procenten

	Bankfraude		Creditcardfraude		Overige fraude	
	2008-2010	2010-2012	2008-2010	2010-2012	2008-2010	2010-2012
1 keer	68,3	74,0	85,1	81,6	100	81,8
2 keer	21,7	16,0	10,6	12,2	-	9,1
> 2 keer	10,0	10,0	4,3	6,1	-	9,1
Totaal	100	100	100	100	100	100
N	180	181	47	49	10	11

In tabel 3.3 is te zien dat de meeste slachtoffers van alle vormen van identiteitsfraude, een delict eenmalig meemaken. Wanneer er sprake is van herhaling, blijft het veelal beperkt tot twee incidenten binnen de bestudeerde tweejaarsperiode. Wanneer de fraudevormen onderling worden vergeleken is te zien dat herhaald slachtofferschap onder bankfraude het meest voorkomt, maar dat dit in de periode 2010 tot 2012 door de respondenten wel wat minder wordt gerapporteerd in vergelijking met 2008 tot 2010, van 31,7 naar 26 procent. Herhaald slachtofferschap van creditcardfraude wordt echter in de periode 2010 tot 2012 juist wat meer gerapporteerd dan in de periode daarvoor, van 14,9 naar 18,3 procent.

3.4 Samengevat

- In de perioden 2008-2010 en 2010-2012 is 4,6 procent van de Nederlandse bevolking van 16 jaar en ouder slachtoffer geweest van identiteitsfraude via een frauduleuze bankafschrijving, misbruik van de creditcard of een overige manier van identiteitsmisbruik.
- In beide perioden is bankfraude duidelijk de meest voorkomende vorm.
- Binnen de tweejaarsperiode is er meestal sprake van eenmalig slachtofferschap. Voor bankfraude geldt dat circa één op de drie à vier slachtoffers herhaald slachtoffer is geweest.

4

Financiële schade

In hoeverre ondervinden slachtoffers van deze uiteenlopende fraudevormen financiële schade? Hoe hoog is de initiële schade (bruto), de definitieve schade (netto), en hoe hoog is daarmee de geschatte totale financiële schade voor identiteitsfraude op maatschappelijk niveau?

4.1 Analyse van Nederlandse literatuur

Slachtoffers van identiteitsfraude hebben vaak te maken met financiële schade, bijvoorbeeld omdat er geld van hun bankrekening is afgeschreven. Net zoals de omvang en aard van identiteitsfraude, laat de schade die gemoeid is met identiteitsfraude een wisselend beeld zien in de wetenschappelijke literatuur. In de meeste studies wordt het onderscheid gemaakt tussen *brutoschade* en *nettoschade*. De brutoschade is de initiële schade van het slachtoffer – het oorspronkelijk afgeschreven bedrag – en de nettoschade is de restschade die het slachtoffer uiteindelijk overhoudt na een eventuele vergoeding. Uit onderzoek van PricewaterhouseCoopers (2013b) blijkt dat het gemiddelde brutoschadebedrag per slachtoffer van 2007 tot 2011 rond de 1500 euro en in 2012 op 600 euro lag. Omgerekend zou dit in 2012 optellen tot een totaal schadebedrag van 355 miljoen euro.[15] Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2013) heeft cijfers gepubliceerd over de schade van skimming en schade in de bankensector, op basis van officiële registraties van de bankensector voor het jaar 2012. Dit bedroeg 28,9 miljoen euro voor skimming en 34,8 miljoen euro voor fraude met internetbankieren. In totaal is er in 2012 daarom in de bankensector voor ruim 60 miljoen schade geleden als gevolg van identiteitsfraude. Ten opzichte van de vorige jaren is dit gedaald, met name door de afname van skimming (onder andere door de invoering van de EMV-chip).

15 Over het maatschappelijk geleden schadebedrag bestaat tussen PwC en de Nederlandse Vereniging van Banken een verschil van inzicht. De NVB concludeert op basis van haar cijfers dat het maatschappelijk schadebedrag door PwC te hoog is geschat. Deze discrepantie zou meerdere redenen kunnen hebben, zoals een verschil in operationalisatie van identiteitsfraude.

Hoewel uit de literatuurstudie is gebleken dat het overgrote merendeel van de slachtoffers het schadebedrag vergoed krijgt, is er sinds januari 2013 een andere trend aan het inzetten (NOS, 2013). De Consumentenbond stelt dat banken steeds minder coulant zijn bij het vergoeden van schade als gevolg van pinpasfraude of phishing. Consumenten zullen dus in de toekomst meer financieel risico gaan lopen. Van der Meulen (2012) bevestigt deze verschuiving en geeft aan dat het eigen risico van de consument groter wordt, omdat banken naar eigen zeggen voldoende hebben gewaarschuwd voor bijvoorbeeld phishing-technieken. Er is dan ook al een aantal zaken bekend (zowel in Nederland als internationaal), waarbij de consument, door volgens de bank aantoonbare nalatigheid, niet schadeloos is gesteld. Toekomstig onderzoek zal moeten uitwijzen of deze ontwikkeling invloed heeft op de nettoschade van burgers.

4.2 *Analyse van internationale literatuur*

Naast cijfers uit de Nederlandse literatuur, zijn ook cijfers bekend over de situatie in de Verenigde Staten, het Verenigd Koninkrijk, Australië en Canada. Uit de representatieve slachtofferenquête van Harrell en Langton (2013) in de Verenigde Staten is gebleken dat het maatschappelijk geleden schadebedrag in 2012 lag op 24,7 miljard dollar. Op individueel niveau is, op basis van de literatuur, een afname waarneembaar. In 2005 leed 40 procent van de slachtoffers nettoschade met een gemiddeld schadebedrag van 500 dollar, waarvan 10 procent meer dan 1200 dollar kwijt was (Anderson e.a., 2008). In 2012 leed nog maar 14 procent nettoschade, waarvan 50 procent niet meer dan 100 dollar kwijt was (Harrell & Langton, 2013). Uit Engels onderzoek blijkt dat de schade die burgers in 2011-2012 moesten dragen op 1,2 miljard pond lag (UK National Fraud Authority, 2012). Uitgaande van dit schadebedrag, komt dat neer op een gemiddeld schadebedrag van 481 pond per slachtoffer. Verder is uit de Australische studie van Smith en Hutchings (2014) gebleken dat 45,7 procent van de slachtoffers geen nettoschade heeft geleden. Onder de slachtoffers die wel nettoschade leden, bleef de schade bij 50 procent beperkt tot 250 dollar of minder, maar waren er in enkele gevallen ook schadegevallen van duizenden dollars. De resultaten voor Canada zijn gebaseerd op één studie (Sproule & Archer, 2008). Uit dit onderzoek is gebleken dat de winst voor daders van identiteitsfraude ongeveer 3 miljard dollar per jaar is. De kosten voor de slachtoffers liggen elk jaar rond 164 miljoen dollar. In 50 procent van de gevallen lijden de slachtoffers helemaal geen nettoschade (2003 tot 2008).

4.3 Analyse LISS-paneldata

Naast literatuuronderzoek zijn ook verschillende analyses op de LISS-paneldata uitgevoerd om een beeld te krijgen van de geleden schade in Nederland van 2008 tot 2012. Voor de fraudevorm onrechtmatige bankafschrijving is gekeken naar de bruto en netto financiële schade die de slachtoffers hebben opgelopen. Naast de bruto- en nettoschade is ook gekeken of de slachtoffers de schade vergoed hebben gekregen. Ten slotte is een schatting gemaakt van de schade van bankfraude op maatschappelijk niveau, door de gemiddelde schade per slachtoffer te extrapoleren naar de Nederlandse bevolking.[16]

Ten eerste is gekeken naar de bruto- en nettoschade van onrechtmatige bankafschrijvingen in de perioden 2008 tot 2010 en 2010 tot 2012. In tabel 4.1 zijn onder meer de gemiddelden en de mediaan van de bruto- en nettoschade weergegeven.[17] In tabel 4.2 wordt getoond hoeveel respondenten in welke schadecategorie vallen. Uit deze resultaten is gebleken dat in 2010 de 161 slachtoffers (slachtoffers die hebben ingevuld hoeveel schade ze hebben geleden), gemiddeld 407 euro brutoschade hebben geleden. De mediaan is minder gevoelig voor uitschieters en ligt met 75 euro een stuk lager. Voor de brutoschade in 2012 geldt dat 150 slachtoffers gemiddeld 382 euro schade hebben geleden. Ook hier ligt de mediaan lager, op 100 euro. Verder is ook gekeken of slachtoffers hun geld vergoed hebben gekregen. In 2010 en 2012 is er voor ruim 80 procent van de slachtoffers sprake van volledige schadevergoeding (2010: 82,4%; 2012: 83,1%). Circa 15 procent kreeg het in beide perioden in het geheel niet vergoed (resp. 14,8% en 14,6%), het resterende deel kreeg de schade deels vergoed. Deze tendens is ook terug te vinden in andere empirische studies (Anderson e.a., 2008; Van Wilsem e.a., 2010; Harrel & Langton, 2013). Door het hoge percentage slachtoffers dat de brutoschade vergoed heeft gekregen, is de nettoschade voor veel slachtoffers afwezig of beperkt. Niettemin is er in een aantal individuele gevallen wel degelijk sprake van een ernstige schadepost.

16 Over de schade die de slachtoffers hebben opgelopen door misbruik van een creditcard is niets bekend. Voor de fraudevorm misbruik van persoonlijke informatie is ook gekeken naar hoeveel geld de slachtoffers kwijt waren aan het rechtzetten van de fraude. De groep respondenten die een overige fraudevorm hebben meegemaakt, is echter zo klein dat hier geen concrete uitspraken over gedaan kunnen worden.

17 Omdat er voor beide perioden een klein aantal gevallen is met een zeer hoge schade (oplopend tot een maximum van 30.000 euro), hebben deze veel invloed op het gemiddelde en op de schatting van de maatschappelijke schade. Om de invloed van deze uitschieters te beperken hebben we een maximumwaarde voor de financiële schade ingesteld van 2500 euro per slachtoffer. In 2010 zijn daarmee de schadebedragen van 5 slachtoffers naar beneden bijgesteld en in 2012 van 7 slachtoffers.

Tabel 4.1: Bruto- en nettoschade bankfraude in 2010 en 2012, in euro's[18]

	Brutoschade		Nettoschade	
	2010	2012	2010	2012
Gemiddelde	407	382	25	45
Mediaan	75	100	0	0
Std. dev.	669	616	127	279
Minimum	0	1	0	0
Maximum	2500	2500	1250	2500
N	161	150	175	176

Tabel 4.2: Bruto- en nettoschade bankfraude in categorieën in 2010 en 2012, in procenten

	Brutoschade		Nettoschade	
	2010	2012	2010	2012
< €50	32,9	33,6	82,9	84,1
€50 - €100	24,2	16,4	10,3	8,5
€100 - €250	13,7	16,4	2,3	4,0
€250 - €1000	12,4	21,9	3,4	1,7
> €1000	16,8	11,6	0,6	0,0
Totaal	100	100	100	100
N	161	150	175	176

Hoewel de meeste individuele slachtoffers schadeloos zijn gesteld, is er wel sprake van een aanzienlijke maatschappelijke schadepost van bankfraude die voor rekening van een bank en uiteindelijk diens klanten komt (Van Wilsem e.a., 2013). De resultaten van onrechtmatige bankafschrijving zijn voor de schatting geëxtrapoleerd naar het bevolkingsaantal (CBS – leeftijd vanaf 15 jaar en ouder) in de twee perioden.[19] Deze schatting geeft aan de hand van een 95-procentbetrouwbaarheidsinterval een bereik aan waarbinnen de schade zich, op basis van deze gegevens, waarschijnlijk bevindt. Voor de periode 2008 tot 2010 ligt de geschatte maatschappelijke schade, gezien de prevalentie van 3,6 procent slachtofferschap, tussen de 147 en 248 miljoen euro. Voor 2010 tot 2012 komt de schatting uit op een bedrag tussen de 134 en 228 miljoen euro.

Tot slot is het opmerkelijk dat de schadebedragen zeer verschillend zijn voor

18 Enkele uitschieters per periode gehercodeerd tot maximumwaarde van 2500.

19 Nederland had in 2008 en 2009 gemiddeld 13.316.085 inwoners van 15 jaar en ouder en in 2010 en 2011 gemiddeld 13.508.360.

de groep die de identiteitsfraude bij de politie meldt en degenen die dat niet doen. De kleine groep slachtoffers die in de periode 2008-2010 zegt aangifte van het incident te hebben gedaan (10% van alle slachtoffers, N=18) heeft gemiddeld genomen een aanzienlijk hoger schadebedrag dan de niet-aangevers: ruim 1200 euro versus circa 300 euro.[20] Voor de periode 2010-2012 zien we dezelfde verschillen, zij het nog iets groter (gemiddelde schadebedragen circa 1300 versus 250 euro). Dit duidt erop dat het werkaanbod identiteitsfraude dat de politie via aangiftes van slachtoffers ontvangt selectief is en zich concentreert rond de ernstiger gevallen met relatief veel schade.

4.4 Samengevat

- Het gemiddeld afgeschreven bedrag bij bankfraude bedraagt circa 400 euro.
- Wel blijft bij een vrij groot aantal slachtoffers de oorspronkelijke (bruto)-schade beperkt: 50 procent van de slachtoffers heeft een afgeschreven bedrag van minder dan 75 euro (2010) of 100 euro (2012).
- Slachtoffers die het delict aangeven bij de politie (circa 10% van het totaal) hebben gemiddeld te maken met veel hogere afgeschreven bedragen: circa 1200 à 1300 euro. Zij vormen dus een groep van mensen die vaak een relatief ernstiger geval van identiteitsfraude hebben meegemaakt.
- Ruim 80 procent van de slachtoffers krijgt het ten onrechte afgeschreven bedrag in de periode 2008-2012 vergoed en lijdt dus persoonlijk uiteindelijk geen financiële schade.
- De maatschappelijke schadepost is wel aanzienlijk en bedraagt naar schatting tussen de 147 en 248 miljoen euro in de periode 2008-2010. Voor 2010 tot 2012 komt de schatting uit op een bedrag tussen de 134 en 228 miljoen euro.

20 Medianen: 1250 euro versus 65 euro.

5

Risicogroepen en -gedragingen

In hoeverre zijn er sociale groepen aan te wijzen die een verhoogd risico lopen op de onderscheiden fraudevormen, in termen van geslacht, leeftijd, opleidingsniveau en inkomenspositie?

In welke mate dragen bepaalde gedragingen of kenmerken van mensen bij aan een verhoogd risico op slachtofferschap van identiteitsfraude, zoals riskante internetgedragingen en lage zelfcontrole?

5.1 *Literatuuranalyse*

De kans om in aanraking te komen met identiteitsfraude hangt mogelijk samen met gedragingen van het slachtoffer, voor zover die van invloed zijn in de overwegingen van daders bij het selecteren van slachtoffers. Analoog aan de gelegenheidstheorie kan daarbij worden gedacht aan factoren als blootstelling, waarde en genoten bescherming (Cohen & Felson, 1979; zie Reyns, 2013), voor een toepassing van dit uitgangspunt op identiteitsfraude). In de literatuur wordt veel aandacht besteed aan achtergrondkenmerken die samenhangen met slachtofferschap van identiteitsfraude, zoals geslacht, leeftijd en inkomen, mogelijk vanwege de relatie van deze kenmerken met bovengenoemde gelegenheidsfactoren.

Verschillende studies hebben de samenhang van *geslacht* met slachtofferschap van identiteitsfraude onderzocht. Uit de meeste onderzoeken is gebleken dat mannen significant vaker slachtoffer worden van identiteitsfraude dan vrouwen (Allisson,e.a. 2005; Newman & McNally, 2005; PwC, 2013b; Reyns, 2013). Daarnaast stellen twee studies dat juist vrouwen vaker slachtoffer worden van identiteitsfraude (Anderson, 2006; Copes e.a., 2010). Voor Nederland heeft PricewaterhouseCoopers (2013a) naar de man-vrouwverdeling gekeken in meldingen van identiteitsfraude en die bleek min of meer gelijk. Volgens een aantal studies hangt ook *leeftijd* samen met slachtofferschap van identiteitsfraude, maar zij tonen wel een uiteenlopend beeld. Nederlands onderzoek van Price-

waterhouseCoopers (2013b) laat zien dat jongeren vaker slachtoffer worden van identiteitsfraude dan ouderen, terwijl het onderzoek op Engelse gegevens van Reyns (2013) het tegenovergestelde aantoont. Drie onderzoeken merken juist een bepaalde leeftijdscategorie aan als risicovol. Newman en McNally (2005) stellen op basis van een uitgebreide literatuurreview dat de meeste slachtoffers tussen de 30 en 39 jaar oud zijn. Uit onderzoek van Anderson (2006) is gebleken dat personen tussen de 25 en 43 jaar de meeste kans lopen om slachtoffer te worden van identiteitsfraude. Ten slotte rapporteren Copes en anderen (2010) dat de meeste slachtoffers vallen in de leeftijdscategorieën tussen de 35 en 44 jaar en boven de 55 jaar.

Over de relatie van *opleiding* en slachtofferschap is er in de meeste studies meer overeenstemming. Twee studies laten zien dat slachtofferschap onder hoogopgeleiden vaker voorkomt dan onder laagopgeleiden (Copes e.a., 2010; PwC, 2013b). Anderson (2006) vond geen invloed van opleidingsniveau op slachtofferschap. Een verband dat in alle studies wordt gevonden, is het verband tussen het *inkomen* en slachtofferschap van identiteitsfraude. Uit de resultaten is gebleken dat hogere inkomens vaker doelwit zijn van daders van identiteitsfraude (Anderson, 2006; Copes e.a., 2010; Harrell & Langton, 2013; Van Wilsem, 2012; Reyns, 2013).

Naast deze veel onderzochte kenmerken, is er nog een aantal kenmerken dat maar in één studie wordt onderzocht. Uit onderzoek van Anderson (2006) is gebleken dat alleenstaanden meer kans lopen op slachtofferschap van identiteitsfraude. Ten slotte concludeerden Newman en McNally (2005) uit hun literatuurreview dat stedelijkheid van de woonplaats gerelateerd is aan slachtofferschap van identiteitsfraude. Identiteitsfraude komt volgens hen het meest voor in stedelijke en toeristische gebieden.

Naast achtergrondkenmerken is in een klein aantal studies ook gekeken naar welke *gedragingen* en *online activiteiten* samenhangen met slachtofferschap van identiteitsfraude. Zoals ook gold voor de achtergrondkenmerken, worden in de literatuur telkens verschillende gedragingen, kenmerken en activiteiten van respondenten onderzocht. Het is dus op basis van de literatuur lastig te concluderen welke activiteiten of kenmerken consistent verband houden met identiteitsfraude. Nu het gebruik van sociale media aan het toenemen is, wordt dit ook steeds vaker onderzocht in verband met identiteitsfraude. Onderzoek van Van Wilsem en anderen (2010) heeft bijvoorbeeld aangetoond dat scholieren en studenten met een of meer profielen op internet, tweemaal vaker slachtoffer worden dan scholieren en studenten zonder profiel. Deze kans neemt toe, wanneer personen hun achternaam en telefoonnummer vermelden op die profie-

len. PricewaterhouseCoopers (2013b) stelt echter dat mensen met uiteenlopend gebruik van sociale media, niet verschillen in hun slachtofferrisico. Andere riskante gedragingen die terugkomen in de literatuur, zijn het bezoeken van internetwinkels, internetbankieren en internetgebruik in het algemeen. PricewaterhouseCoopers (2013b) concludeert dat 24 procent van de fraude plaatsvindt in internetwinkels. De kans op slachtofferschap van identiteitsfraude neemt volgens Reyns (2013) met 30 procent toe wanneer iemand internetwinkels bezoekt. Internetbankieren is volgens dezelfde studie nog riskanter. De kans op slachtofferschap neemt met 50 procent toe wanneer iemand online zijn of haar bankzaken regelt. In het onderzoek van Reyns (2013) komt ten slotte nog naar voren dat mensen die veel e-mailen, chatten en downloaden, meer kans lopen om slachtoffer te worden van identiteitsfraude. Naast deze risicovolle gedragingen op internet, is in de literatuur ook aandacht besteed aan beschermende factoren. Individuen die hun computer beschermen door middel van het updaten van hun antivirussoftware, antispy-software en ad-blocker-software,[21] zijn volgens de resultaten van Holt en Turner (2012) beter beschermd tegen identiteitsfraude dan individuen die dit niet doen. Ten slotte is ook aandacht besteed aan de invloed van het niveau van zelfcontrole van een persoon op slachtofferschap van identiteitsfraude; mogelijk komen impulsieve mensen sneller in aanraking hiermee. De twee onderzoeken die hier op ingaan hebben echter geen samenhang gevonden (Bossler & Holt, 2010; Ngo & Paternoster, 2011).

5.2 *Analyse LISS-paneldata*

5.2.1 *Achtergrondkenmerken en slachtofferschap*

Om de onderzoeksvragen omtrent risicogroepen te beantwoorden, is ten eerste middels een Spearman rangcorrelatietoets[22] gekeken welke achtergrondken-

21 Antispy- en ad-blocker-software detecteren malware, spyware en dergelijke.

22 De Spearman rangcorrelatiecoëfficiënt is een maat voor samenhang voor bepaalde variabelen. De uitkomsten liggen altijd tussen de -1 en +1 (negatief en positief verband). Hoe dichter een score bij de waarde 0 ligt, des te zwakker het verband; en dus hoe verder ervan verwijderd, des te sterker het verband. Een waarde van 0 betekent dat er geen samenhang is tussen de variabelen. Daarnaast is in de tabel het significantieniveau aangegeven met * of **. Wanneer dit teken achter de coëfficiënt staat, betekent dit dat het verband waarschijnlijk niet alleen in de steekproef is gevonden, maar zich ook voordoet in de populatie (i.e. de Nederlandse bevolking van 15 jaar en ouder). Bij * (p<.05) is de kans op een 'toevalsbevinding' kleiner dan 5 procent, bij ** (p<.01) is die kleiner dan 1 procent.

merken samenhangen met slachtofferschap van de verschillende vormen van identiteitsfraude. De achtergrondkenmerken die hieraan zijn gerelateerd zijn: geslacht, leeftijd, opleiding, nettomaandinkomen, stedelijkheid en alleenstaand zijn. Deze analyse is uitgevoerd voor slachtofferschap van bankfraude, creditcardfraude en overige fraude in beide perioden. De resultaten zijn weergegeven in tabel 5.1.

Tabel 5.1: Correlaties tussen achtergrondkenmerken en slachtofferschap van bankfraude, creditcardfraude en overige fraude, 2008-2010 en 2010-2012

	Bankfraude		Creditcardfraude		Overige fraude	
	2010	2012	2010	2012	2010	2012
Vrouw	ns	ns	-0.043 **	-0.035 **	ns	-0.032 *
Leeftijd	ns	ns	ns	ns	-0.034 *	0.037 **
Opleiding	0.037 **	0.036 **	0.047 **	0.062 **	ns	ns
Netto-inkomen	ns	ns	ns	ns	0.037 **	ns
Stedelijkheid woonplaats	0.042 **	ns	ns	ns	ns	ns
Alleenstaand	0.026 *	ns	ns	ns	ns	ns
N	5764	5709	5764	5709	5764	5709

ns = niet significant

* = p < .05; ** = p < .01

Een algemeen beeld uit deze tabel, is dat de meeste sociale categorieën niet gerelateerd zijn aan slachtofferschap identiteitsfraude – en voor zover dat wel zo is, is het verband zwak. Meer specifiek is in de tabel te zien dat wanneer gekeken wordt naar *bankfraude*, alleen het opleidingsniveau in beide perioden significant samenhangt met slachtofferschap. Hoogopgeleiden lopen meer risico om slachtoffer te worden van bankfraude. In 2010 is verder nog te zien dat ook de stedelijkheid van de woonplaats en alleenstaand zijn, samenhangen met slachtofferschap van bankfraude. Dit wil zeggen dat mensen die in een stedelijk gebied wonen en alleenstaanden, meer kans liepen op slachtofferschap van bankfraude in de periode 2008 tot 2010. Voor *creditcardfraude* geldt ook dat voor beide perioden het opleidingsniveau van belang is. Hoogopgeleiden lopen meer kans om slachtoffer te worden van creditcardfraude. Verder lopen mannen meer kans om slachtoffer te worden van creditcardmisbruik. Voor *overige fraude*, een zeldzame gebeurtenis in deze gegevens, komt een wisselend beeld naar voren. Leeftijd hangt voor de twee perioden op uiteenlopende wijze samen met slachtofferschap. In 2010 zijn jongeren vaker slachtoffer, in 2012 juist ouderen.

In 2010 hebben mensen met hogere inkomens een hoger risico, maar in 2012 niet. Mannen worden in 2012 vaker slachtoffer dan vrouwen, maar dat gold niet voor 2010.

Met dezelfde achtergrondkenmerken als in tabel 5.1 is ook een logistische regressieanalyse[23] uitgevoerd. Dit stelt ons beter in staat om de relatie tussen de kenmerken en slachtofferschap vast te stellen. Sommige achtergrondkenmerken overlappen namelijk – hoger opgeleiden wonen bijvoorbeeld vaker in grote steden –, waardoor uit de correlaties niet optimaal is af te leiden welk kenmerk nu risicoverhogend is. In de logistische regressieanalyse wordt gezocht naar de unieke bijdrage van ieder kenmerk aan de voorspelling van slachtofferschap van identiteitsfraude. In tabel 5.2 zijn de resultaten van deze regressieanalyse weergegeven. De resultaten hebben betrekking op slachtofferschap van bankfraude

Tabel 5.2: Logistische regressieanalyse van slachtofferschap bankfraude en creditcardfraude in 2010 en 2012 op achtergrondkenmerken

	Bankfraude				Creditcardfraude			
	2010		2012		2010		2012	
	B	s.e.	B	s.e.	B	s.e.	B	s.e.
Constante	-2.268 **	0.460	-3.022	0.480	-3.396 **	0.876	-4.340 **	0.901
Vrouw	-0.250	0.248	-0.038	0.149	-0.930 **	0.305	-0.652 *	0.285
Leeftijd	-0.062	0.046	-0.051	0.047	-0.149	0.090	-0.127	0.087
Opleiding	0.111 *	0.024	0.123 *	0.051	0.295 **	0.100	0.465 **	0.107
Inkomen	-0.047	0.048	-0.024	0.045	0.077	0.078	-0.165	0.106
Stedelijkheid	0.160 **	0.060	0.092	0.060	-0.110	0.114	0.093	0.108
Alleenstaand	-0.229	0.186	-0.128	0.196	-0.471	0.349	-0.302	0.347
Nagelkerke R^2		0.017		0.009		0.050		0.057
N		5614		5563		5572		5549

* = $p < .05$; ** = $p < .01$

23 Een logistische regressieanalyse gaat na of meerdere onafhankelijke variabelen (bijvoorbeeld leeftijd en opleiding) invloed hebben op de afhankelijke variabele (bijvoorbeeld slachtofferschap bankfraude). In tegenstelling tot in een correlatieanalyse, worden de variabelen controlerend voor elkaar gemeten. Hierbij wordt dus ook rekening gehouden met de correlatie (samenhang) van de onafhankelijke variabelen onderling. In de kolom aangeduid met **B,** wordt de coëfficiënt weergegeven die de sterkte van het verband aangeeft. Hoe hoger het getal, hoe sterker het verband (deze verbanden kunnen positief of negatief zijn). De **s.e**. is de standaardafwijking van deze coëfficiënt. Regressiecoëfficiënten die ten minste 1,96 keer groter zijn dan hun bijhorende standaardfout, worden als significant aangemerkt. De Nagelkerke R^2 geeft in zekere zin aan wat het percentage verklaarde variantie van het model is. Dit cijfer geeft aan hoeveel procent de variabelen in het model, in dit geval, slachtofferschap verklaren.

en creditcardfraude in beide perioden. Overige fraude is vanwege het lage aantal slachtoffers (10 in 2010 en 11 in 2012) niet geschikt voor deze analyse.

Uit de resultaten blijkt dat alleen opleidingsniveau een consistent en significant verband laat zien met slachtofferschap van *bankfraude* in beide perioden. Dat wil zeggen dat hoe hoger het opleidingsniveau, des te groter de kans dat iemand slachtoffer wordt van bankfraude (zie voor vergelijkbare internationale bevindingen: Anderson, 2006; Harrell & Langton, 2013). Daarnaast is te zien dat stedelijkheid significant samenhangt met bankfraude in de periode 2008 tot 2010: meer slachtoffers in grote steden. De Nagelkerke R^2 representeert hoeveel procent de variabelen in dit model slachtofferschap van bankfraude verklaren en die is voor bankfraude in beide perioden zeer laag, respectievelijk 1,7 en 0,9 procent. Dit wil zeggen dat de achtergrondkenmerken slachtofferschap van bankfraude in beide perioden niet goed voorspellen. Uit de resultaten voor *creditcardfraude* is gebleken dat opleidingsniveau opnieuw in beide perioden invloed uitoefent op slachtofferschap van creditcardfraude, met hogere risico's voor hoogopgeleiden. Daarnaast zien we dat mannen vaker slachtoffer worden van creditcardfraude dan vrouwen, eveneens voor beide perioden, een bevinding die overeenkomt met resultaten uit eerdere studies in Nederland en het buitenland (Allisson e.a., 2005; PwC, 2013b; Reyns, 2013). De overige achtergrondkenmerken zijn niet gerelateerd aan slachtofferschap. Deze resultaten komen overeen met de eerder genoemde resultaten uit de rangcorrelaties. De beide Nagelkerke R^2's zijn in dit model weliswaar wat hoger dan in de beide modellen van bankfraude, maar blijven ook hier beperkt, met respectievelijk 5 en 5,7 procent verklaarde variantie.

5.2.2 Persoonskenmerken, internetgedragingen en slachtofferschap

Een uniek kenmerk van de LISS-paneldata – in vergelijking met eerdere studies op het gebied van identiteitsfraude – is dat het naast achtergrondkenmerken ook veel gedetailleerde informatie bevat over aanvullende persoonskenmerken en gedragingen, zoals zelfcontrole, tijdsbesteding op internet en preventie-activiteiten. Omdat deze informatie zowel is verzameld onder slachtoffers als niet-slachtoffers, zijn we daarmee in staat na te gaan in hoeverre we tussen beide groepen verschillen aantreffen in deze kenmerken. Dat geeft op zijn beurt weer meer inzicht in waar de risico's op identiteitsfraude mee samenhangen. We bespreken de resultaten van een aantal analyses op deze gegevens en bouwen die als volgt op. Analoog aan de zojuist getoonde analyse waarin we achter-

grondkenmerken relateerden aan identiteitsfraude, bespreken we eerst correlaties tussen gedragingen en slachtofferschap en vervolgens de resultaten van logistische regressieanalyses, die ons beter in staat stellen te beoordelen welke aspecten nu daadwerkelijk risicoverhogend zijn.[24] De resultaten van de correlaties tussen internetgedragingen en slachtofferschap van identiteitsfraude zijn vanwege het grote aantal variabelen te vinden in bijlage 3 (tabel B.3.1). Alleen de belangrijkste resultaten zullen hier worden besproken.

Als eerste blijkt uit de correlaties dat *zelfcontrole* alleen samenhangt met bankfraude in 2010 en overige fraude in 2012: mensen met lage zelfcontrole lopen meer risico op slachtofferschap van deze vormen in deze perioden. Studies van Bossler en Holt (2010) en Ngo en Paternoster (2011) toonden geen verband met het niveau van zelfcontrole.

Wanneer gekeken wordt naar bepaalde online activiteiten, blijkt dat het *invullen van internetenquêtes* samenhangt met een hoger risico op bankfraude in beide perioden en met creditcardfraude in 2012. Daarnaast hangen het *gebruik van een webcam*, *het bezit van een virusscanner* en *creditcardgebruik* allen samen met een vergrote kans op slachtofferschap van creditcardfraude in beide perioden. Daarnaast blijkt dat *het aantal sociale-netwerksites* en *de informatie die iemand daarop zet* samenhangt met verhoogde slachtofferrisico's van bankfraude in 2010. Opvallend is dat deze samenhang in 2012 is weggevallen. Deze tendens is ook te zien bij slachtofferschap van creditcardfraude. De kans op slachtofferschap van creditcardfraude in 2010 is groter bij meer sociale netwerken en het plaatsen op die sites van de achternaam, de leeftijd, het e-mailadres en foto's. Ook deze samenhang is niet terug te zien voor 2012. De samenhang met deze variabelen en overige fraude is niet significant. Alleen het aantal sociale-netwerksites hangt daar positief mee samen. Het nemen van preventieve maatregelen op de computer is ook gerelateerd aan slachtofferschap. Voor beide perioden geldt dat alle maatregelen (behalve het gebruik van een trojanscanner) *positief* samenhangen met slachtofferschap van

24 De volgende variabelen zijn zowel in de correlatie- als in de regressieanalyses meegenomen: zelfcontrole, invullen van internetenquêtes, webcamgebruik, controle van virussen en creditcardgebruik. Aantal uren per week besteding aan: e-mailen, informatie zoeken op internet, producten vergelijken op het internet, producten kopen op het internet, korte films kijken, tv of films kijken, downloaden, gokken, internetbankieren, gamen, lezen van nieuwssites, bezoeken van nieuwsgroepen, chatten, bezoeken van fora en overige bezigheden. Voor de survey uit 2012 zijn daar nog de volgende activiteiten aan toegevoegd: sociale media, bloggen, Skypen, Twitter en datingsites. Ten slotte zijn de volgende variabelen meegenomen in de analyses: aantal sociale-netwerksites, vermelding achternaam, vermelding leeftijd, vermelding adres, vermelding telefoonnummer, vermelding e-mailadres, plaatsen van foto's, gebruik firewall, virusscanner, antispy-software, trojanscanner, spamfilter, beveiliging van de wifi en computeronwetendheid.

bankfraude en creditcardfraude. Dit wil, paradoxaal genoeg, zeggen dat wanneer iemand deze preventieve maatregelen heeft geïnstalleerd, diegene meer kans loopt om slachtoffer te worden van bankfraude en creditcardfraude. Voor overige fraude is deze samenhang niet aangetoond. Mogelijk komt dit onverwachte resultaat tot stand doordat mensen die preventiemaatregelen nemen, op andere aspecten juist risicovoller scoren, zoals meer internetgedrag. De logistische regressieanalyses, waarvan we de resultaten aansluitend presenteren, kunnen hier meer licht op werpen. Ten slotte hangt een geringe kennis van computers samen met slachtofferschap van bankfraude en creditcardfraude in beide perioden. Hoe minder verstand iemand heeft van computers, des te kleiner de kans is dat iemand slachtoffer wordt van bankfraude en creditcardfraude.

Naast correlaties zijn met dezelfde variabelen logistische regressieanalyses uitgevoerd. Dit is gedaan voor bankfraude en creditcardfraude in 2010 en 2012. Door het lage aantal personen dat slachtoffer is geworden van overige fraude, is deze analyse niet uitgevoerd voor deze fraudevorm. De resultaten zijn te vinden in bijlage 3 in tabellen B3.2. tot en met B3.5. In deze analyse zijn ook de achtergrondkenmerken meegenomen, om een zo compleet mogelijk beeld te schetsen van factoren die invloed uitoefenen op slachtofferschap. Uit de resultaten voor *bankfraude* is gebleken dat wanneer alle variabelen in de analyse worden meegenomen, in 2010 stedelijkheid van de woonplaats, het vermelden van het woonadres op een sociale-netwerksite en het aantal uren dat iemand internetbankiert, invloed hebben op slachtofferschap. Een stedelijker woonplaats, meer uren internetbankieren en het vermelden van een woonadres op sociale media vergroot de kans op slachtofferschap in de periode 2008 tot 2010. In model 1 (alleen de achtergrondkenmerken meegenomen) was ook de variabele opleidingsniveau aan te merken als significant, maar dat verband is na toevoeging van internetbankieren weggevallen. Dit zou verklaard kunnen worden door het feit dat hoogopgeleiden meer internetbankieren. Wanneer gekeken wordt naar bankfraude in de periode 2010 tot 2012, is gebleken dat hoe meer enquêtes iemand invult op internet, hoe groter de kans is op slachtofferschap van bankfraude. Ook in deze periode is het gebruik van internetbankieren van belang. Mensen die internetbankieren, lopen meer kans om slachtoffer te worden dan mensen die dit niet doen (zie ook Reyns, 2013, voor een vergelijkbare bevinding). Wanneer 2010 en 2012 worden vergeleken, is te zien dat internetbankieren in beide perioden een significant effect heeft op slachtofferschap. Verder geldt voor bankfraude ook in beide perioden dat getroffen preventiemaatregelen niet van invloed zijn. Het feit dat de positieve correlatie in de logistische regressieanalyse is weggevallen, duidt erop dat goed beveiligde

mensen meer risicoactiviteiten ondernemen, zoals internetbankieren. Indien daar rekening mee wordt gehouden, zien we niet langer een positieve samenhang tussen computerbeveiliging en slachtofferschap. Opvallend is dat ondanks het gebruik van een zeer uitgebreid voorspellingsmodel het percentage verklaarde variantie (Nagelkerke R^2) laag blijft: rond de vijf procent. Slachtofferschap van bankfraude is dus in belangrijke mate afhankelijk van andere mechanismen dan die in het model zijn opgenomen.

Uit de resultaten voor *creditcardfraude* in de periode 2008 tot 2010 is gebleken dat geslacht en het gebruik van een creditcard invloed hebben op slachtofferschap van creditcardfraude. In model 1 is ook opleidingsniveau als significant aan te merken, maar door toevoeging van de variabele creditcardgebruik valt dit verband weg: hogeropgeleiden gebruiken vaker een creditcard. Voor de periode 2010 tot 2012 zijn meer significante verbanden gevonden. Wanneer alle variabelen mee worden genomen in de analyse, zijn de volgende kenmerken van invloed op slachtofferschap van creditcardfraude in 2012: opleidingsniveau, zelfcontrole, invullen van online enquêtes, het bezit van een virusscanner, creditcardgebruik en het aantal uur per week kijken naar korte online video's. Dit wil zeggen dat mensen die hoog zijn opgeleid, weinig zelfcontrole hebben, online enquêtes invullen, een virusscanner hebben, vaak een creditcard gebruiken en tijd besteden aan het kijken van korte online video's, meer kans lopen op slachtofferschap van creditcardfraude in de periode 2010 tot 2012. Verder geldt ook voor creditcardfraude dat we geen preventieve effecten vinden van beschermingsmaatregelen op de thuiscomputer. Tot slot zien we voor creditcardfraude dat het percentage verklaarde variantie in deze voorspellingsmodellen hoger is dan voor bankfraude (vergelijk het meest uitgebreide model 5: circa 19% versus 6%), maar veel van die extra verklaringskracht heeft te maken met een voor de hand liggende voorspeller: gebruik van een creditcard. De overige significante factoren dragen weliswaar iets bij aan de voorspelling, maar ook hier geldt dat er nog een groot onverklaard deel overblijft in het beantwoorden van de vraag wie er slachtoffer wordt en wie niet.

5.3 Samengevat

- Slachtofferschap van diverse vormen van identiteitsfraude komt wat vaker voor onder hoogopgeleiden, maar de verschillen zijn niet erg groot.
- Creditcardfraude komt wat vaker voor bij mannen dan bij vrouwen, maar opnieuw zijn de verschillen niet groot.

- Bankfraude komt vaker voor naarmate men meer aan internetbankieren doet en online transacties via iDEAL verricht.
- Creditcardfraude komt meer voor onder frequente creditcardgebruikers en (in 2012) onder mensen met weinig zelfcontrole.
- Beschermingsmaatregelen op de pc hebben geen beschermende werking tegen slachtofferschap van bank- of creditcardfraude.
- Zowel slachtofferschap van bank- als creditcardfraude laten zich niet goed voorspellen aan de hand van het zeer uitgebreide voorspellingsmodel.

6 Modus operandi

Welke modus operandi hanteren daders van identiteitsfraude en in hoeverre is op dit gebied door de tijd heen een verschuiving in werkwijzen te constateren?

6.1 Literatuuranalyse

Het delict identiteitsfraude is, algemeen gezegd, verdeeld in twee fasen. Een dader zal eerst persoonlijke informatie moeten *stelen* of *de gestolen informatie kopen* en vervolgens zal hij met die persoonlijke informatie *frauderen*. Het stelen van informatie kan een dader op veel verschillende manieren bewerkstelligen. Het scala aan modus operandi is uitgebreid, variërend van eenvoudige, fysieke manieren, zoals het hengelen van post uit brievenbussen, tot complexe methoden waarbij digitale persoonsinformatie (die bijvoorbeeld door bedrijven wordt opgeslagen) via hacking wordt ontvreemd (Koops e.a., 2009). In het volgende overzicht worden de modus operandi uiteengezet die in de literatuur het meest voorkomen. De aard van deze beschrijving vereist geen of weinig voorkennis van cybercrime en wordt daarmee op inleidend niveau besproken.

Fysieke diefstal

Portemonnees, tassen, computers en telefoons zijn voor daders van identiteitsfraude interessante objecten. Deze kunnen door daders vaak relatief makkelijk gestolen worden, maar slachtoffers kunnen ze zelf ook verliezen. Een tweede manier om op een fysieke manier aan informatie te komen, is *dumpster diving*. De daders gaan in het afval van bijvoorbeeld huishoudens op zoek naar informatie die bruikbaar is om identiteitsfraude mee te plegen. Bruikbare informatie kan zijn: rekeningnummers, adresgegevens, accountinformatie (bijvoorbeeld van een telefoonabonnement) en overheidsgegevens (bijvoorbeeld burgerservicenummers). Behalve zoeken in afval, zoeken daders ook naar post in brievenbussen, postbussen en recycling-afvalbakken op straat (Newman & McNally, 2005).

Een andere eenvoudige manier om aan persoonlijke informatie te komen, die iets meer moeite kost, is het laten doorsturen van de post van het slachtoffer naar een ander adres. Dit doen daders om twee redenen. Ten eerste is post rijk aan bruikbare persoonlijke informatie en ten tweede duurt het enige tijd voordat het slachtoffer ontdekt dat niet alle post op het goede adres aankomt (CIPPIC, 2007). Naast deze manier, kiezen daders er soms voor om persoonlijke informatie van overledenen te gebruiken. Deze informatie kan bijvoorbeeld gehaald worden uit het overlijdensbericht in de krant. Het komt ook voor dat een dader zich voordoet als een nabestaande en contact opneemt met bijvoorbeeld het mortuarium (CIPPIC, 2007).

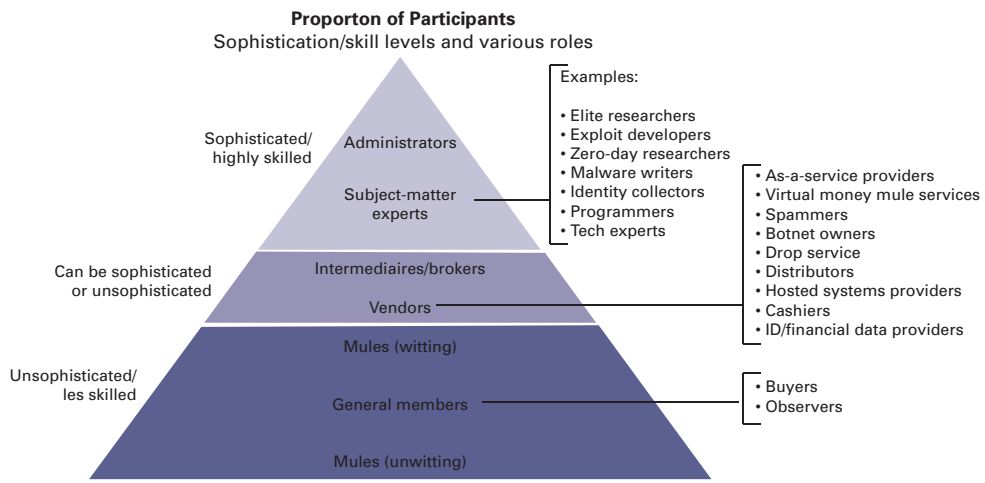
Hoewel er weinig onderzoek naar is gedaan, stelt een Amerikaanse studie van Collins en Hoffman (2004) dat werknemers van organisaties regelmatig betrokken zijn bij het plegen van identiteitsdiefstal. Het onderzoek toont aan dat 70 procent van de diefstal van persoonlijke informatie van organisaties, gepleegd wordt door interne medewerkers. Werknemers hebben toegang tot informatie over veel personen en sommige zijn bereid dit te verspreiden of te verkopen. De studie van Collins en Hoffman (2004) is echter gedateerd en hoe de situatie nu is, is niet duidelijk. Het NCSC (2014) stelt nog wel dat medewerkers de beveiligingsketen kunnen maken of breken en dat misbruik van en door interne medewerkers of ondernemers een zeer reële dreiging is geworden.
Ten slotte komt het gebruiken van een kopie van een identiteitsbewijs voor (CIPPIC, 2007). Deze kopieën kunnen op allerlei manieren worden ontvreemd, bijvoorbeeld omdat organisaties (zoals hotels en autoverhuurbedrijven) – al dan niet terecht – om kopieën van identiteitsbewijzen vragen en deze onvoldoende beveiligd bewaren. Om te voorkomen dat ieder zomaar een kopie laat maken van paspoort of rijbewijs, is de overheid in 2013 een *awareness* campagne begonnen ('Laat u niet zomaar kopiëren').

Kopen van informatie

Hoewel daders zelf op verschillende manieren informatie kunnen stelen, zijn er ook daders die deze informatie kopen. Uit onderzoek van Copes en Vieraitis (2009) is gebleken dat de meest voorkomende methode om een identiteit van een ander te gebruiken, het kopen van een identiteit was. Voor het onderzoek interviewden de onderzoekers 59 daders van identiteitsfraude in gevangenschap. Zij vertelden dat ze de informatie meestal kochten van een medewerker van een organisatie. Ook online is het mogelijk om de persoonsgegevens van een slacht-

offer van identiteitsdiefstal aan te schaffen. Onderzoek van Soudijn en Monsma (2012) laat zien dat er virtuele ontmoetingsruimtes bestaan waar daders samenkomen. Deze worden ook wel *carding forums* of *carder networks* genoemd. Carding is een term die verwijst naar alle technieken waarmee persoonlijke financiële gegevens verkregen, verhandeld en misbruikt worden (Soudijn & Monsma, 2012). In feite faciliteren deze netwerken onder andere vraag en aanbod van gestolen persoonsgegevens. Uit onderzoek van Holt (2013) blijkt dat criminelen elkaar ook beoordelen op betrouwbaarheid wanneer ze met elkaar handelen. Kopers en verkopers krijgen een bepaalde rating, zodat ze tot op zekere hoogte weten met wie ze zaken doen. Het onderzoek van Holt (2013) is gebaseerd op een uitgebreide analyse van vier fora waar criminelen en hackers gegevens kopen, verkopen en verhandelen. Het NCSC (2014) bevestigt het bestaan van dergelijke zwarte markten die worden opgezet om cybercrime te faciliteren en stellen dat het een wereldwijd verschijnsel is geworden. Wat deze markten ook faciliteren, zijn mogelijkheden om in contact te komen met anderen en samenwerkingsverbanden te starten. Volgens het NCSC (2014) worden de samenwerkingsverbanden en daarmee de gepleegde delicten, steeds beter georganiseerd en vindt georganiseerde criminaliteit nu ook op digitaal niveau plaats. De studie van Ablon en anderen (2014) stelt dat er sprake is van een hiërarchisch piramidemodel (zie figuur 6.1).

Figuur 6.1: Samenwerkingsverbanden bij identiteitsfraude (bron: Ablon e.a., 2014)



Aan de top van de piramide staat de beheerder van de organisatie. Deze wordt gevolgd door experts op bepaalde gebieden (bijvoorbeeld hackers en technische experts). Hierna volgen de tussenpersonen, leveranciers en overige leden. Voor het innen van de winst worden zogenaamde *money mules* ingezet, zij staan onderaan in de hiërarchie. Aan de money mules wordt gevraagd hun pinpas tijdelijk ter beschikking te stellen om crimineel geld op te storten. Zodra dit geld is gestort, kan met de pinpas van de money mule het geld worden opgenomen, zodat het geld contant beschikbaar komt.

Skimming

Een bekende manier om succesvol met andermans gegevens te frauderen, was het proces van skimming. De dader heeft hiervoor skimapparatuur aangeschaft of gemaakt, die kopieën kan maken van de magneetstrip van een betaalkaart. Daders installeren de apparaatjes veelal in bestaande pinautomaten. Om de pincode te achterhalen, wordt er veelal een kleine camera bij geplaatst. Of daders gaan achter de pinnende klant staan en kijken mee over de schouder, dit wordt ook wel *shoulder surfing* genoemd (CIPPIC, 2007). In andere gevallen komt het ook voor dat de dader werkt in een restaurant, winkel of hotel en de betaalpas kopieert bij de betaling. Het maken van een kopie is in een aantal seconden gebeurd en het slachtoffer merkt niet dat de betaalpas gekopieerd is. Dit wordt vaak pas opgemerkt wanneer er geld wordt afgeschreven van de bankrekening (CIPPIC, 2007). Uit twee Nederlandse studies (Domenie e.a., 2013; PwC, 2013b) is gebleken dat skimming volgens de slachtoffers zelf de meest gebruikte methode is om identiteitsfraude te plegen. De percentages die in deze twee studies zijn gevonden, liggen beide tussen 30 en 40 procent. Hoewel deze twee studies een indicatie geven dat skimming een veelgebruikte methode is, stelt een meer recente studie van het ministerie van BZK (2013) dat skimming snel afneemt door geo-blocking,[25] afschaffing van de magneetstrip in 2012 en de invoering van de EMV-chip op betaalpassen.

25 Bij geo-blocking van de betaalpas, is een betaalpas standaard onbruikbaar gemaakt voor gebruik buiten Europa. Om buiten Europa te kunnen pinnen, moet de consument zijn of haar pas tijdelijk activeren.

Phishing

Phishing wordt ook wel een hybride techniek genoemd, omdat een dader gebruikmaakt van technische methoden, maar ook van *social engineering* (CIPPIC, 2007). Social engineering wordt ingezet om het vertrouwen van het slachtoffer te winnen en hem te laten geloven dat hij te maken heeft met een betrouwbare organisatie. Om dit te bereiken, krijgt het slachtoffer een mail van de dader die er betrouwbaar en echt uitziet. Vaak wordt gebruikgemaakt van de kleuren en het logo van de organisatie (*spoofing*). De daders doen zich vaak voor als financiële organisaties, en dan voornamelijk als banken (CIPPIC, 2007). Volgens Symantec Corporation (2014) wordt bij ruim 70 procent van de phishing mails voorgewend dat deze afkomstig zijn van een financiële organisatie. Wanneer het slachtoffer op de e-mail ingaat, wordt hij of zij gevraagd persoonlijke informatie en accountinformatie in te vullen. Het onderzoek van PricewaterhouseCoopers (2013b) stelt wel dat phishing tussen 2011 en 2012 is afgenomen als methode om identiteitsfraude mee te plegen. Bij phishing worden vaak mails verstuurd naar grote groepen mensen die de dader niet kent. In een korte tijd kunnen miljoenen e-mails tegelijk worden verstuurd (Gercke, 2007) en ook bij een relatief klein succespercentage – vanuit het perspectief van de dader – kan het dan toch om een substantieel aantal slachtoffers gaan. Wanneer de dader zich met phishing richt op een specifiek persoon, wordt het ook wel *spear-phishing* genoemd (Brody e.a., 2007).

Pharming

Pharming staat ook wel bekend als *domain spoofing* (CIPPIC, 2007). Pharmers zorgen ervoor dat bezoekers van een website naar een andere website worden geleid dan waar ze denken heen te gaan (zoals hun bank). Op deze website vullen slachtoffers dan identificatiegegevens in, zoals gebruikersnaam en wachtwoord (Brody e.a., 2007). Pharming kan op meerdere manieren plaatsvinden. Een eerste manier om pharming te bewerkstelligen is *Domain Name System (DNS) poisoning*. Een DNS poisoning zorgt ervoor dat wanneer iemand een webadres in de adresbalk intypt, hij of zij op een andere pagina uitkomt. Een tweede manier van pharming is *Domain Name System (DNS) cache poisoning* (Brody e.a., 2007). Een computer heeft veelal een DNS server aangewezen gekregen en deze server houdt voor een bepaald aantal uur een domein in zijn cache (tijdelijk geheugen) vast. Wanneer een domein in een cache staat hoeft de server niet telkens

het internet op om domeinen op te vragen, en dit scheelt dus tijd. Pharmers kunnen deze cache vervuilen en bij vervuiling zal die DNS server gedurende de tijd dat het domein in de cache is opgeslagen een 'verkeerd antwoord' geven en het slachtoffer naar de verkeerde website sturen.

Malware

Malware is kwaadaardige (*malicious*) software en kan op verschillende manieren worden ingezet en op iemands computer belanden (CIPPIC, 2007). Een doel van malware kan zijn om van een organisatie grote hoeveelheden informatie te stelen, maar malware kan ook op individueel niveau worden toegepast. Hoewel het gebruik van malware geen nieuwe trend is (het wordt al ruim tien jaar toegepast), worden de methoden steeds inventiever en moeilijker te detecteren (Symantec Corporation, 2014). Malware loopt vaak voor op de beveiligingstechnieken van computers, wat detectie lastig maakt. Mensen die denken dat ze goed beveiligd zijn, openen bepaalde links die ze vertrouwen en kunnen desondanks geïnfecteerd raken (Marshall & Tompsett, 2005). Malware kan zich op verschillende manieren verspreiden en in verschillende vormen voorkomen. Een voorbeeld van een verspreidingsmanier, is via een *watering-hole attack* (Symantec Corporation, 2014). Bij een watering-hole attack infiltreert de aanvaller een legitieme site, die bezocht wordt door de persoon of personen die hij wil aanvallen (Symantec Corporation, 2014). De term is afgeleid van het dierenrijk en refereert aan leeuwen die bij een waterplas liggen te wachten op hun prooi. De daders planten een kwaadaardige code en wachten tot hun doelwit de site bezoekt. Door een scan uit te voeren die kwetsbaarheden in sites laat zien, kan de aanvaller kijken welke site makkelijk te infiltreren is. Het onderzoek van Symantec Corporation (2014) laat zien dat een op de acht websites makkelijk toegankelijk is voor hackers. Wanneer ze een site hebben geïnfiltreerd, kunnen ze in de logs (door middel van IP-adressen) zien wie de site bezoekt en wachten op hun doelwit. Wanneer het doelwit dan de site bezoekt (onwetend, omdat hij de site vertrouwt), wordt de gebruiker geïnfecteerd met malware. Op deze manier kan de aanvaller aan belangrijke informatie en persoonlijke gegevens komen. Organisaties zijn vaak het doelwit, omdat daar veel belangrijke en persoonlijke informatie te krijgen is. Watering-holes maken vaak gebruik van *zero-day vulnerabilities* (Symantec Corporation, 2014). Dit zijn beveiligingslekken in nieuwe browsers die worden ontdekt op het moment dat ze worden uitgerold. Ze heten zero-days omdat alle virusscanners en de software-ontwikke-

laars van die browsers, minstens twee dagen nodig hebben om de update uitgerold en gedistribueerd te krijgen. Hackers moeten hem dus echt op de zero-day ontdekken om hem te kunnen uitbuiten, want zodra het lek gedicht is – dit duurt tussen de twee en tien dagen – kunnen zij er niets meer mee.[26] Van 2012 tot 2013 is het aantal zero-day vulnerabilities gestegen met 61 procent (Symantec Corporation, 2014). Watering-hole attacks en zero-day vulnerabilities zijn daarnaast populair, omdat ze niet gebaseerd zijn op social engineering technieken – en dus niet afhankelijk zijn van de bereidwilligheid van slachtoffers om 'mee te werken' – en omdat ze bovendien bestand zijn tegen antiphishing software. Wanneer door daders netwerken van (met malware) geïnfecteerde computers worden gecreëerd, spreken we van *botnets*. Dit netwerk van computers wordt gestuurd door de dader en hij kan het botnet voor meerdere doeleinden gebruiken. Voorbeelden hiervan zijn het verspreiden van virussen, massale spamverzending en het uitvoeren van DDoS-aanvallen.[27] Ook het stelen van persoonlijke informatie is een van de doelen die daders hebben wanneer ze een botnet opzetten (Symantec Corporation, 2014).

Spyware is een subcategorie van malware. Spyware staat bekend om het laten crashen of vertragen van systemen en het laten verschijnen van ongewenste reclame en pop-upberichten (CIPPIC, 2007). Spyware kan echter ook leiden tot identiteitsfraude. Bepaalde vormen van spyware maken het mogelijk om bepaalde activiteiten op de computer te volgen en toegang te krijgen tot de harde schijf van het slachtoffer.

Hacking

Hacking is het uitbuiten van de beveiligingskwetsbaarheden van computersystemen. Uit onderzoek van Symantec Corporation (2014) is gebleken dat hacking de belangrijkste oorzaak is voor grootschalige datalekken waar veel persoonlijke informatie bij wordt gewonnen (34% van de datalekken in 2013 was een gevolg van hacking). Bij hacking worden corrupte data gestuurd naar de software die draait op een bepaalde computer. De corrupte data verwarren de

26 Deze toelichting op de zero-day vulnerabilities komt voort uit persoonlijke communicatie met de respondent van Business Forensics.

27 Een Distributed Denial of Service aanval (DDoS) is een poging een computernetwerk of dienst onbereikbaar en onbruikbaar te maken voor de gebruiker van dat netwerk of die dienst. Voor een DDoS-aanval wordt vaak een botnet gebruikt.

software en de software gaat instructies uitvoeren, gestuurd door de hacker. Het doel is veelal het installeren van een *trojan horse* om een 'achterdeur' in het systeem te openen. De achterdeur maakt het mogelijk gebruik te maken van de computer zonder dat de eigenaar of de organisatie iets in de gaten heeft. Op deze manier kan veel informatie worden gekopieerd en weggesluisd. Trojan horses die gericht zijn op het verkrijgen van financiële gegevens zijn *banking trojans*. Ze kunnen het proces van internetbankieren aanpassen en bankdetails stelen. Sinds 2012 is het aantal banking trojans verdriedubbeld (Symantec Corporation, 2014).

Gebruik van sociale media

Door het toenemende aantal sociale-netwerksites en het toenemende aantal gebruikers, zijn sociale netwerken voor daders van identiteitsfraude een aantrekkelijk doelwit. Op verschillende manieren kunnen daders via sociale-netwerksites iemands identiteit overnemen of veel belangrijke persoonlijke informatie verzamelen. Ten eerste is het eenvoudig voor elke computergebruiker om aan zogenaamde *vrije gegevens* van de gebruikers te komen, wanneer deze hun profiel niet goed hebben afgeschermd. Gegevens zoals naam, geboortedatum en woonplaats zijn regelmatig vrij beschikbaar op het internet. Volgens de resultaten van het onderzoek van PricewaterhouseCoopers (2013b), is identiteitsfraude door middel van het gebruik van openbaar beschikbare gegevens sterk toegenomen. Onderzoek onder studenten van Van Wilsem en anderen (2010) laat zien dat personen met een of meer persoonlijke profielen op sociale-netwerksites, twee keer meer kans lopen op slachtofferschap van identiteitsfraude. Deze kans neemt vooral toe wanneer achternaam en telefoonnummer op deze profielen zijn vermeld. Daarnaast verplaatsen technieken zoals spam en phishing zich steeds meer richting de sociale netwerken (Symantec Corporation, 2014; NCSC, 2014). Op deze manier kunnen daders weer aan persoonlijke informatie komen wanneer slachtoffers op de phishing-links klikken en hun persoonlijke informatie invullen. Voor daders is deze wereld interessant. De marges zijn weliswaar smaller dan bijvoorbeeld bij phishing mails vanuit 'banken', maar de kans op ontdekking is veel kleiner. In het onderzoek van Bilge en anderen (2009) worden twee technieken getoond die laten zien dat het kopiëren van profielen en het verzamelen van persoonlijke informatie eenvoudig gaat. De eerste techniek die zij hebben gebruikt in hun onderzoek is *profile cloning*. Bij deze techniek wordt misbruik gemaakt van vriendschapsverzoeken. De dader maakt een account aan dat exact

lijkt op het account van iemand in de vriendenlijst van het slachtoffer. Vervolgens stuurt de dader het slachtoffer een vriendschapsverzoek. Wanneer het slachtoffer het vriendschapsverzoek heeft geaccepteerd, kan de dader alle persoonlijke informatie bekijken en kopiëren. De andere techniek die ze hebben gebruikt, is *cross-site profile cloning*. Bij deze methode wordt een profiel gekloond tussen verschillende sociale netwerken in plaats van binnen één sociaal netwerk, zoals bij profile cloning. Het doel van de aanval is het identificeren van slachtoffers die lid zijn van een bepaald sociaal netwerk, maar nog niet van een ander sociaal netwerk. De dader wil de identiteit van het slachtoffer ontvreemden en met die identiteit profielen aanmaken op andere sociale netwerken. De tweede stap is dan om te identificeren of vrienden van het slachtoffer op de sociale-netwerksite, ook lid zijn van de sociale-netwerksite waar de dader het profiel op gaat klonen. Wanneer bekend is welke vrienden ook lid zijn van het netwerk waarop de dader een profiel wil plaatsen, worden vriendschapsverzoeken verstuurd. De meeste vrienden zullen deze accepteren, omdat het van een bekend persoon komt die ze nog niet in hun lijst hebben staan. Wanneer het verzoek is geaccepteerd, kan de dader op verschillende manieren frauderen met de persoonlijke informatie van de slachtoffers.

Overige methoden

Aangezien het bovenstaande overzicht niet uitputtend is, zullen hier kort een aantal andere methoden worden gesproken. Ten eerste kunnen daders ook via onbeschermde wifi- netwerken aan persoonlijke informatie komen. Met een apparaatje kunnen daders snel zien welke apparaten zijn ingelogd op het lokale wifi-netwerk. Via een paar stappen is dan de informatie te achterhalen (Martijn, 2014). Aangezien steeds meer restaurants, hotels en winkels gratis wifi aanbieden, maken steeds meer mensen gebruik van deze letterlijke 'hot spots'. Een andere manier om aan informatie te komen, is via de mobiele telefoon van slachtoffers (Symantec Corporation, 2014). Met opkomst van smartphones richten de daders van identiteitsfraude zich steeds meer op deze apparatuur. Veel mensen zijn zich niet bewust van het feit dat ook hun mobiele telefoon gehackt kan worden en dat er beveiliging nodig is om dit te voorkomen. Ook phishing aanvallen zijn inmiddels uitgevoerd op telefoons. Daarnaast creëren daders ook geloofwaardige applicaties (apps) die slachtoffers installeren op hun telefoon. Via deze applicaties kunnen ze dan weer informatie op de telefoon buitmaken (Symantec Corporation, 2014).

Hoewel social engineering al kort is besproken in relatie tot phishing, is het ook een aparte techniek om persoonlijke informatie te achterhalen. De sleutel tot succes is het winnen van het vertrouwen van het slachtoffer of andere partijen om zo informatie los te krijgen. Wanneer de dader een derde partij inschakelt, gaat dat vaak om organisaties waarbij het slachtoffer aangesloten is. Hij neemt contact op met die organisatie en doet zich voor als een werknemer van de organisatie zelf, of als iemand van een andere organisatie die ook een relatie heeft met het slachtoffer. De dader vraagt dan om gegevens van het slachtoffer. Wanneer hij het slachtoffer zelf direct benadert, doet hij zich bijvoorbeeld voor als telemarketeer of zegt hij dat hij van een 'niet-bellen-register' is (CIPPIC, 2007).

6.2 Schema modus operandi

Op basis van bovenstaande literatuur is een schema gemaakt dat tijdens de interviews aan de respondenten is getoond. Dit schema is te vinden in bijlage 2, figuur B2.1. Het opgestelde schema weerspiegelt de methoden die het meest in de literatuur naar voren kwamen. Het is daarmee dan ook geen uitputtend overzicht van alle modus operandi gebruikt voor identiteitsfraude. Daarnaast is vooral aandacht besteed aan modus operandi met een digitale component, omdat hier in de literatuur ook het meeste onderzoek naar is gedaan. Het schema is onderverdeeld in drie hoofdcategorieën. De eerste categorie is fysieke diefstal, die de eenvoudige manieren van identiteitsfraude betreft. Voorbeelden bij deze categorie, zijn dumpster diving en het stelen van post. De tweede hoofdcategorie bevat de technische methoden, die weer in drie subcategorieën uiteenvallen. Deze categorieën zijn 'eenvoudige manieren', 'complexere methoden' en 'technische hoogstandjes' die een gedegen inzicht vereisen in het hacken en overnemen van computers. De categorie eenvoudige manieren, bevat onder andere het surfen op internet naar informatie en het gebruiken van sociale media. De complexere methoden vallen uiteen in phishing, pharming en skimming, en de technische hoogstandjes bevatten de watering-hole attacks, zero-day vulnerabilities, DNS server poisoning en malware en spyware. Aan de respondenten is gevraagd of het schema overeenkwam met hun ervaringen in de praktijk. In de volgende paragraaf zullen de resultaten van de interviews worden besproken.

6.3 *Analyse interview data*

Definitie en verschijningsvormen identiteitsfraude

In hoofdstuk 2 hebben we uiteengezet welke experts op het gebied van identiteitsfraude voor dit onderzoek zijn geïnterviewd (zie hoofdstuk 2.3). Na een inleidend gesprek over dit onderzoek, de functie van de respondent en de achtergrond van de respondent, is aan de respondenten gevraagd of er bepaalde definities binnen hun organisatie worden gebruikt om identiteitsfraude in te kaderen. De meeste organisaties doen dit niet. De twee organisaties die dit wel doen, zijn het CMI en het ECID. Wanneer zij een definitie gebruiken, hanteren zij die van De Vries en anderen (2007).[28] De respondent van het ECID geeft echter aan dat deze definitie niet leidend is. De overige organisaties hebben allen eenzelfde visie op het probleem identiteitsfraude. De meest algemene, overlappende opvatting is dat het gaat om *misbruik van iemands persoonlijke informatie om een wederrechtelijke gedraging te begaan*. Meestal is financiële winst het ultieme doel voor de daders. Aangezien deze studie gebaseerd is op slachtoffers van bankfraude, creditcardfraude en overige vormen van fraude, is de respondenten gevraagd welke vormen van identiteitsfraude zij tegenkomen in hun werk. Uit de antwoorden van de respondenten is gebleken dat dit zeer afhankelijk is van de aard van de organisatie en de manier waarop ze met identiteitsfraude te maken krijgen. De meeste organisaties krijgen vooral te maken met financiële identiteitsfraude en noemen daarbij fraude met de bankpas, fraude met de creditcard en fraude met internetbankieren. Het CMI en de Fraudehelpdesk krijgen te maken met meer diverse vormen, aangezien zij een steunpunt zijn voor burgers die in aanraking zijn gekomen met de meest uiteenlopende vormen van identiteitsfraude. Voorbeelden zijn contractvervalsing, internetbestellingen zonder te betalen, rekening openen op naam van een ander en fraude op Marktplaats. Documentfraude is een vorm van identiteitsfraude waar de meeste organisaties zich niet mee bezig houden. Uitzonderingen hierop zijn het ECID (van de Koninklijke Marechaussee) en Team Identiteitsfraude (TIF) van de gemeente Amsterdam. Onder documentfraude valt onder andere het maken van een vals document, het vervalsen van een document of een document creëren dat niet

28 Definitie identiteitsfraude De Vries en anderen (2007): 'Identiteitsfraude is het opzettelijk en wederrechtelijk of zonder toestemming verkrijgen, toe-eigenen, bezitten of creëren van valse identificatiemiddelen en daarmee begaan van een wederrechtelijke gedraging of met de intentie om een wederrechtelijke gedraging te begaan.'

bestaat. Wat het ECID en TIF veel tegenkomen in de praktijk, is *lookalike* fraude. Hierbij gebruikt iemand een paspoort of ander identiteitsbewijs van een persoon die erg op hem lijkt. Hoewel door de meeste organisaties weinig aandacht wordt besteed aan documentfraude, is het echter wel zo dat criminelen vaak valse of vervalste documenten gebruiken om bijvoorbeeld een bankrekening te openen. Documentfraude zal daarom zeker bij andere vormen van identiteitsfraude een rol spelen.

Methoden identiteitsfraude

Zoals eerder genoemd, is de respondenten een schema getoond en gevraagd of ze de indeling van het schema ook terugzagen in de praktijk (zie bijlage 2, figuur B2.1). De respondenten vonden het schema op zichzelf een goede weerspiegeling van de werkelijkheid, maar tegelijkertijd wel te abstract weergegeven. In de praktijk is er vaak sprake van verschillende combinaties van modus operandi. De combinatie die het meest voorkomt, is social engineering samen met een andere modus operandi, bijvoorbeeld phishing. Aan de respondenten is ook gevraagd of bepaalde modus operandi in het schema ontbraken. De volgende methoden zijn toen genoemd: *man-in-the-middle*-scenario,[29] fraude met gegevens van de Kamer van Koophandel (dus op bedrijfsniveau), vhishing (phishing via voice, bijvoorbeeld via de telefoon) en smishing (phishing via SMS of een soortgelijke dienst), en corrupte medewerkers. Daarnaast heeft fraude met documenten geen plaats in het schema, terwijl het volgens het ECID en TIF veel voorkomt. Aangezien documentfraude geen plaats had in het schema, was het voor deze respondenten vaak niet mogelijk de vragen over de digitale vormen van modus operandi te beantwoorden. Aan hen zijn deze vragen dan ook niet gesteld en zij worden dus ook niet meegenomen in de beantwoording van die vragen in de onderstaande tekst.

Wanneer de respondenten werd gevraagd naar de *populairste methode* om op dit moment identiteitsfraude te plegen, zei de meerderheid te denken dat dit phishing was (NVB, Skimmingpoint, ECTF (beide respondenten), Business Forensics en de Fraudehelpdesk). Er werd echter wel door een aantal organisaties de

29 Het *man-in-the-middle*-scenario betreft het door de dader online onderscheppen van bijvoorbeeld een financiële transactie. De dader zorgt ervoor dat die transactie ergens ander naartoe gaat dan bedoeld door het slachtoffer. Het slachtoffer ziet na de aanval de bedoelde transactie op zijn scherm en heeft niet door dat de betaling is afgebogen.

kanttekening geplaatst dat door goede preventieve maatregelen de technische methoden voor de dader steeds lastiger te gebruiken worden als modus operandi. Als gevolg daarvan, vallen ze weer terug op de meer fysieke methoden, zoals het stelen van post, vaak in combinatie met social engineering. Ten slotte stelde een strategisch analist van Europol dat grootschalige datahacks het meest populair zijn in die zin, dat op die manier de meeste persoonlijke informatie wordt verkregen. Deze winst kan bijna niet door andere methoden geëvenaard worden. De precieze prevalentie van de meeste populaire methoden (meestal phishing) in tegenstelling tot andere methoden, konden de respondenten niet melden. De respondent van de Nederlandse Vereniging van Banken (NVB) stelde wel dat phishing met 76 procent was gedaald (in 2013 in vergelijking met 2012), maar nog wel (in vergelijking met malware) de meeste schade oplevert. Malware was met 72 procent gedaald (in 2013 in vergelijking met 2012) (Nederlandse Vereniging van Banken, 2014). Beide respondenten van de Electronic Crimes Taskforce (ECTF) bevestigden dat de schade van phishing en malware aan het afnemen is. Onduidelijk is echter of de schade door andere modus operandi juist toeneemt. Ten slotte kon het CMI melden dat de meldingen van identiteitsfraude alleen maar blijven stijgen en dat 30 procent van de meldingen fraude met een kopie van een identiteitsbewijs betreft (CMI: persoonlijke communicatie).

Naast de populairste methode, is de respondenten ook gevraagd of bepaalde methoden aan het *verdwijnen* zijn en welke dat zijn. Uit de interviews is gebleken dat alle respondenten het erover eens zijn dat skimming als methode aan het verdwijnen is. Dit is te danken aan de invoering van de EVM-chip en geo-blocking van de betaalpas. Volgens de respondent van Skimmingpoint hebben de dadergroeperingen zich, als reactie op deze preventieve maatregelen, verplaatst naar landen buiten West-Europa. De NVB meldde daarnaast dat ook fraude in het betalingsverkeer spectaculair aan het dalen is en dat we ons, wat betreft aanvallen op het betalingsverkeer, in een rustperiode bevinden. In een dergelijke rustperiode vindt er dan een verplaatsing plaats naar het buitenland. Wanneer deze landen hun preventieve maatregelen ook op orde hebben, zullen – naar verwachting – identiteitsfraudeurs nieuwe methoden bedenken die ze weer in Nederland kunnen toepassen. Ten slotte stelde een analist van Europol dat spam via e-mail en spamming malware gericht op e-mail, aan het afnemen zijn. Spam heeft zich volgens de respondent verplaatst naar sociale media. Op de vraag of in de praktijk meer high-tech of low-tech methoden voorkomen, is geen eenduidig antwoord gegeven. Het CMI gaf aan dat het het meeste te maken krijgt met low-tech methoden en ook denkt dat deze het meest voorko-

men in de praktijk. De overige organisaties dachten dat ze beide én in combinatie voorkomen. Het antwoord van de organisaties op deze vraag, lijkt veel te maken te hebben met het werkveld waar zij zich in bevinden. Geen van de benaderde organisaties gaf aan een overzicht te hebben van alle identiteitsfraude gepleegd in Nederland.

Daders, samenwerking en carder networks

Naast vragen over de bovenstaande onderwerpen, is de respondenten ook gevraagd naar samenwerking tussen daders, taakverdeling tussen daders en de *carder networks*. Bij de vraag of daders die identiteitsfraude plegen, vaker alleen of in samenwerkingsverband werken, werd vaak geantwoord dat dit afhangt van hoe geavanceerd de identiteitsfraude is. De respondent van de Fraudehelpdesk gaf als voorbeeld dat een dader bestellingen op naam van een ander alleen zal doen, maar dat bij een meer complex delict zal worden samengewerkt. Bij sommige methoden, zoals phishing en skimming is het volgens de respondenten zelfs ondenkbaar dat er geen georganiseerd netwerk achter zit. De respondent van de NVB stelde dat achter de aanvallen op internetbankieren een hele organisatie zit, die werkt met een bepaalde gelaagdheid. De teamleider van Europol zei dat het netwerk achter identiteitsfraude gezien kan worden als een 'business model' waar ieder zijn rol heeft. Een van de respondenten van het ECTF gaf daarnaast ook aan dat elke zaak die ze hebben behandeld, het stempel 'georganiseerde criminaliteit' kan krijgen. Deze antwoorden komen overeen met het onderzoek uitgevoerd door Ablon en anderen (2014) en het eerder getoonde piramidefiguur (zie figuur 6.1).

Aan vijf van de respondenten (NVB, ECTF (beide respondenten), Fraudehelpdesk, Business Forensics) is verder de hypothese voorgelegd dat het verschillende personen zijn die stelen en frauderen. Zijn het bijvoorbeeld de hackers die stelen en anderen die frauderen? Deze hypothese is op basis van de kennis van de respondenten niet te bewijzen, maar het leek hun wel plausibel. Voor het stelen van veel gegevens is vaak technische kennis vereist die alleen hackers bezitten. Een respondent van het ECTF stelde dat hackers ingehuurd worden, of uit eigen beweging hacken en de gegevens verkopen. Ten slotte is over dit onderwerp aan vier organisaties (Business Forensics, ECTF, Fraudehelpdesk en Europol) doorgevraagd of er een bepaalde ontwikkeling te schetsen is op het gebied van samenwerking. Gebeurt dat nu meer dan een aantal jaar geleden? De vier respondenten dachten van wel. Door internet is het mogelijk

met meer mensen samen te werken en zijn er nieuwe *facilitators* ontstaan. Een van de respondenten van het ECTF antwoordde in deze context: 'De "nerds" waren bij wijze van spreken een paar jaar geleden niets waard. Die beheersen nu het kunstje dat interessant is. Deze mensen worden nu dus meer gebruikt.' Daarnaast merkte een analist van Europol op dat het aantal transacties en het aantal personen op de fora toeneemt. Europol verwacht dus ook dat daarmee de samenwerking toeneemt. Deze antwoorden zijn in lijn met het artikel van Soudijn en Monsma (2012). Zij stellen dat de virtuele fora het samenwerken tussen daders faciliteren en dat er zo nieuwe samenwerkingsverbanden ontstaan. Naast dat (bijna)[30] alle organisaties het erover eens zijn dat er sprake is van samenwerking, zijn alle respondenten het er ook over eens dat de carder networks op internet zeer belangrijk zijn voor plegers van identiteitsfraude.[31] Naast dat deze netwerken de gebruiker anoniem houden, zijn ze faciliterend in een aantal opzichten. Ten eerste zijn deze carder networks een koop- en verkooppunt voor allerlei persoonlijke informatie, maar ook voor bijvoorbeeld malware en spyware. De respondenten van Europol gaven tijdens het interview aan dat het er op deze sites zeer geautomatiseerd aan toe gaat. Net als bij Marktplaats, zet iemand zijn gekozen producten in zijn virtuele winkelwagen (bijvoorbeeld creditcardnummers) en rekent hij af. Daarnaast kunnen mensen op deze netwerken in de verschillende fora overleggen, kennis uitwisselen en elkaar ontmoeten. Op deze netwerken wordt ook gewerkt met een zogenaamde betrouwbaarheidsrating. De bezoekers van de sites kunnen zo zien wie er betrouwbaar zijn en met wie ze zaken willen doen. Deze uitspraak komt overeen met het onderzoek van Holt (2013) naar anonieme fora op het internet. Ten slotte worden deze netwerken volgens de respondent van Business Forensics ook gebruikt voor wervingsdoeleinden om 'vacatures' op te vullen. Door de groei van internet wordt steeds meer via deze weg gezocht naar partners om mee samen te werken. Het is zeer eenvoudig contact te leggen met personen die een bepaalde expertise bezitten die een ander mist. Wanneer bij een persoon technische kennis ontbreekt, kan hij op een dergelijk netwerk op zoek naar iemand die, in ruil voor een beloning, de technische kant van het delict op zich neemt. In de context van samenwerking en de carder networks, is aan de respondenten gevraagd of er een bepaalde taakverdeling bestaat tussen de daders die samen identiteitsfraude plegen. De respondenten die zicht op dit

30 Alleen het CMI zag geen duidelijke indicaties voor samenwerking in de gevallen waarmee het wordt geconfronteerd.

31 De respondent van Business Forensics zag de netwerken zelfs als cruciaal.

onderwerp hadden, gaven bij deze vraag aan dat de taakverdeling waarschijnlijk een erg amorf karakter heeft. (Het CMI en het TIF gaven aan geen zicht op dit onderwerp te hebben.) Samenwerking kan op allerlei manieren plaatsvinden – dit ligt aan het doel van de criminele organisatie, welke middelen ze nodig heeft om dat doel te bereiken en dus welke mensen ze moet inzetten.

Van skimming en phishing hebben twee respondenten (respectievelijk Skimmingpoint en het ECTF) uitgelegd hoe het proces en ook de taakverdeling in elkaar zitten. Aangezien skimming bijna niet meer voorkomt en phishing nog een groot probleem vormt, zal hier alleen het proces van phishing worden besproken. Om in één keer veel phishing e-mails te kunnen versturen, zullen de daders in het bezit moeten zijn van veel e-mailadressen. Stap één is om iemand een hack te laten plegen en zo een adressenbestand te stelen. Hij of iemand anders stuurt vervolgens een phishingmail naar de e-mailadressen en een deel van de ontvangers zal daar op reageren. Zij klikken op de link in de e-mail en worden geleid naar een phishingsite. Daar wordt hun meestal gevraagd hun wachtwoord en gebruikersnaam in te vullen. Wanneer ze dat hebben gedaan, worden ze gebeld om hun laatste benodigde gegevens te achterhalen. Dit kunnen bijvoorbeeld TAN-codes (wachtwoord voor internetbankieren) zijn. Degene die belt, is meestal iemand van Nederlandse afkomst (soms met callcentererervaring). Het doel van dit telefoongesprek is om meer gegevens te krijgen, maar ook om het vertrouwen te winnen van het slachtoffer (social engineering). Als de daders alle gegevens hebben, kunnen ze overschrijvingen doen naar rekeningen van de money mules. De money mules zullen, als het gestolen geld op hun rekening staat, dit zo snel mogelijk pinnen. Via verschillende wegen kan dit geld dan weer terugkomen bij de mensen hoger in de hiërarchie.

Ten slotte is met betrekking tot dit onderwerp aan de respondenten gevraagd of ze denken dat de samenstelling van samenwerkende groepen vluchtig of vast van aard is. De antwoorden op deze vraag waren zeer wisselend. Geen van de respondenten had hier zicht op, met als gevolg dat uitspraken over deze kwestie hypothetisch van aard zijn. De respondent van de NVB gaf aan dat het vaste groepen zijn, omdat men op elkaar ingespeeld moet zijn en dat er sprake is van het opbouwen van een vertrouwensband. Een van de respondenten van het ECTF is er juist van overtuigd dat de samenstelling heel vluchtig is, omdat criminelen in een organisatie telkens een andere expertise nodig hebben en opportunistisch zijn in hun keuze voor samenwerking. Anderen dachten dat hoe technischer de modus operandi, hoe vluchtiger de samenstellingen (Business Forensics). Er zijn echter ook respondenten die dachten dat juist de fysieke modus operandi een vluchtig samenwerkingskarakter hebben (Fraudehelpdesk).

Identiteitsfraude: een grensoverschrijdend delict

Een onderwerp waar alle respondenten hetzelfde over dachten, was het internationale karakter van identiteitsfraude. Dit internationale karakter maakt het voor de opsporingsdiensten en voor organisaties die zich met identiteitsfraude bezighouden, lastig goed zicht op de daders te krijgen. Uit de interviews is gebleken dat veel daders uit Oost-Europa lijken te komen. Wanneer daders succesvol criminaliteit willen plegen in Nederland, zullen ze echter ook faciliterende Nederlanders nodig hebben. Hierbij kan gedacht worden aan degene die na een phishingmail de slachtoffers belt, omdat daarvoor een goede beheersing van de Nederlandse taal vereist is. Verder voegde de respondent van Business Forensics nog toe dat Nederland een open en goed gefaciliteerd internetdistributieland is. Nederland is een rijk land en veel mensen maken gebruik van internetbankieren. Er is met andere woorden sprake van een goede gelegenheidsstructuur voor daders van identiteitsfraude en cybercrime in het algemeen.

Frauderen en winst maken

Wanneer de benodigde persoonlijke informatie is gestolen en ermee gefraudeerd is, wordt er uiteindelijk door de daders winst gemaakt. Aan de respondenten is de vraag gesteld hoe dit gebeurt. Uit de interviews is gebleken dat daders op allerlei manieren winst kunnen maken en dat dit ligt aan de modus operandi die de daders gebruiken. In de meeste gevallen is financieel gewin het doel en zal het criminele geld een plaats moeten krijgen in de bovenwereld. Dit kan op verschillende manieren plaatsvinden. Drie organisaties (NVB, ECTF (beide respondenten) en Europol) merkten Bitcoins aan als een belangrijke manier om het geld te investeren. De markt in Bitcoins is er een zonder controle en dat maakt het voor de daders aantrekkelijk. Naast Bitcoins, gaven drie andere organisaties aan dat luxe auto's en luxe goederen worden aangekocht. Hierbij valt te denken aan goud, kunst en sieraden. Ten slotte zijn money mules nog een manier om geld contant te krijgen. Volgens de respondent van de Fraudehelpdesk kunnen de money mules ook via de grenswisselkantoren geld opsturen naar het buitenland. In deze context is ook aan vijf respondenten (NVB, Business Forensics, ECTF, Fraudehelpdesks en Europol) de vraag gesteld hoe er wordt omgegaan met een grote hoeveelheid aan persoonlijke informatie (bijvoorbeeld honderden creditcardgegevens). Deze respondenten antwoordden allen dat die informatie verkocht wordt, binnen en buiten de carder networks.

Een hacker vergaart de persoonlijke gegevens en dat zal hij laten renderen via een volgende actie. Aangezien hackers over het algemeen niet automatisch ook bekwaam zijn in het uitvoeren van de vervolgdelicten, zal hij iemand in zijn netwerk benaderen die de gegevens van hem koopt.

Vergelijking literatuur en praktijk

Een deel van het interview bevatte vragen of cijfers gevonden in de literatuur, overeenkwamen met de praktijk. Alle respondenten konden de stelling van het ministerie van BZK (2013) bevestigen dat skimming aan het afnemen is. De tweede stelling betrof de uitspraak van PricewaterhouseCoopers (2013b), dat ook phishing als methode van identiteitsfraude aan het afnemen is. Vier respondenten konden hier geen uitspraken over doen (CMI, Skimmingpoint, ECID en TIF), één respondent dacht niet dat de methode aan het afnemen is, maar wel de bijbehorende schade (ECTF) en twee respondenten gaven aan dat het gebruik van phishing als methode aan het dalen is, dat de schade aan het dalen is, maar dat het nog wel een groot probleem blijft (NVB, ECTF). Een analist van Europol vond het een 'strong statement' gemaakt door PricewaterhouseCoopers. Hij stelde dat er geen manier is om erachter te komen of phishing daadwerkelijk aan het afnemen is.

Aangezien uit studies (Van Wilsem e.a., 2010; Symantec Corporation, 2014) is gebleken dat het gebruik van sociale media verband kan houden met slachtofferschap van identiteitsfraude, is de respondenten ook naar dit onderwerp gevraagd. Dit geldt ook voor het gebruik van onbeschermde wifi-netwerken. De meeste organisaties hadden geen antwoord op de vraag of sociale-netwerksites een belangrijke rol spelen. De respondenten van Europol en Business Forensics gaven echter wel aan dat sociale media belangrijk zijn. Een respondent van Europol stelde dat via sociale media, spam en phishing mails verstuurd kunnen worden en deze mails kunnen ook weer malware verspreiden. Daarnaast antwoordde de respondent van Business Forensics dat via een technische verbinding tussen sociale netwerken veel informatie over iemand en zijn netwerk te halen valt. Op die manier kan iemand aan veel gegevens komen en daarna zijn er veel mogelijkheden om die informatie te misbruiken. Op de vraag welke sociale-netwerksite het aantrekkelijkste doelwit is voor daders, antwoordde een respondent van Europol dat het voorkomt op alle sociale netwerken, maar dat Facebook de grootste is. De respondent van Business Forensics zei echter dat het niet gaat om de site met de meeste leden, maar om de snelst groeiende site. Sociale netwerken die snel groeien in gebruikers, zijn vooral gericht op het bijhouden van die groei en niet

op de beveiliging van de site. Zoals eerder genoemd, is ook gevraagd naar onbeschermde wifi-netwerken. De zes respondenten die antwoord hebben gegeven op deze vraag (CMI, ECTF (beide respondenten), Business Forensics, Europol en Fraudehelpdesk), antwoordde allen dat het een gebruikte modus operandi is, maar dat het geen efficiënte methode is om identiteitsfraude mee te plegen. De hoeveelheid persoonlijke informatie die je in één keer kunt winnen is gering. Volgens Europol zal deze methode echter wel toenemen, vanwege het toenemende aantal hotspots waar gratis wifi wordt aangeboden.

Grootschalige datahacks

Uit de analyse van LISS-paneldata is gebleken dat weinig kenmerken van potentiële doelwitten het uiteindelijke slachtofferschap goed kunnen voorspellen. Naar aanleiding van dit resultaat is een hypothese opgesteld om de oorzaak van slachtofferschap op een andere manier te verklaren. Aan de respondenten is de hypothese voorgelegd dat het doelwit van de daders aan het verschuiven is naar organisaties, omdat organisaties beheerders zijn van databases met persoonsgegevens van een groot aantal individuen, zoals klanten. Deze hypothese is ook gebaseerd op het toenemende aantal mediaberichten over grote datahacks en datalekken. De meeste respondenten vonden dit een logische hypothese, maar nog niet iedereen ziet de verschuiving van individu naar bedrijf terug in de praktijk. De respondenten stelden dat het logisch is voor een dader om een doelwit te kiezen waarbij met één aanval veel persoonlijke informatie gewonnen kan worden. Daarnaast antwoordde de respondent van de NVB dat onze persoonlijke informatie in veel databanken staat, terwijl dat niet toegestaan is. Deze databanken zijn vaak slecht beveiligd en dus een aantrekkelijk doelwit voor criminelen. Europol stelde dat het ligt aan de methode die een dader gebruikt (en waar hij dus bekwaam in is) en of die ook geschikt is om grote hacks mee te plegen. Daarnaast moet rekening gehouden worden met het feit dat grootschalige hacks en lekken sneller in het nieuws komen dan individuele aanvallen. Dit kan een vertekend beeld van de werkelijkheid opleveren.

Interne betrokkenheid

Ook de rol van medewerkers, dat wil zeggen van interne betrokkenheid bij identiteitsfraude is tijdens het interview aan bod gekomen. De respondenten hebben

het vermoeden dat betrokkenheid van medewerkers zeker voorkomt. Concrete cijfers zijn echter niet beschikbaar. Veel bedrijven willen niet dat interne betrokkenheid aan het licht komt en zullen een dergelijke situatie binnen het bedrijf proberen op te lossen. Interne betrokkenheid kan in meerdere sectoren voorkomen, maar het zijn vooral organisaties die veel persoonsinformatie in hun bezit hebben. Voorbeelden die de respondenten noemden zijn banken, postbedrijven, en de logistieke dienstverlening. Daarnaast kunnen de medewerkers verschillende rollen hebben en vrijwillig of niet vrijwillig (door middel van afpersing) meewerken aan identiteitsfraude. De respondent van Business Forensics gaf aan dat er een duidelijke trend bestaat waarbij criminele organisaties hun werknemers de opdracht geven bij een postbedrijf te gaan werken en in een bepaalde wijk terecht te komen. Zo kan die werknemer voor die wijk de post gaan afvangen. Hij stelde verder dat interne betrokkenheid bij banken meer facilitair is. Hij dacht dat bankmedewerkers in eerste instantie niet bij een bank gaan werken om te frauderen, maar dat ze, onder andere door de hoeveelheid aan gevoelige informatie, verleid kunnen worden tot fraude of afgeperst kunnen worden.

Nieuwe ontwikkelingen en de toekomst

De twee laatste vragen van het interview betroffen ontwikkelingen die in het interview niet behandeld waren en het perspectief van de respondenten op de toekomst. Europol en Business Forensics noemden beide nog ontwikkelingen die niet aan bod zijn gekomen tijdens het interview. Door Europol werd het gebruik en de stijgende dreiging van applicaties (apps) genoemd. Wanneer apps op een bepaald apparaat worden geïnstalleerd, geeft iemand veel persoonlijke informatie weg. Veel mensen zijn hier waarschijnlijk niet van op de hoogte. Een respondent van Europol vond het in deze context tevens opvallend dat mensen wel wantrouwend zijn wanneer de overheid persoonlijke informatie bewaart, maar dat ze hier bij private organisaties niet over nadenken. Deze opmerking komt overeen met de eerder genoemde privacyparadox van Bijlsma en anderen (2014). Zoals eerder benoemd, gaf Europol aan een verandering waar te nemen van phishing e-mails naar phishing op sociale media. Daarnaast zullen, volgens Europol, ook mobiele telefoons ook steeds interessanter worden voor daders. De smartphones hebben zich inmiddels ontwikkeld tot kleine computers, maar zijn nu nog minder goed beveiligd. Deze ontwikkeling wordt ook genoemd in de rapporten van Symantec Corporation (2014) en het NCSC (2014).

De respondent van Business Forensics noemde in de context van ontwikke-

lingen, de overmoedigheid van de Nederlandse burger. De Nederlandse burgers denken dat ze goed beveiligd zijn na installatie van een virusscanner en gaan zich dan juist risicovol gedragen. Hackers lopen altijd een stapje voor en zullen dus ondanks een virusscanner ook gegevens kunnen stelen of een computer kunnen binnendringen. Deze uitspraak komt overeen met de resultaten uit de uitgevoerde correlatieanalyse in deze studie. Mensen die zich beveiligen tegen identiteitsfraude door middel van preventieve maatregelen op de computer, worden eerder slachtoffer.

De antwoorden die de respondenten gaven op de vraag wat ze in de toekomst verwachten op het gebied van identiteitsfraude, kunnen als volgt worden samengevat: identiteitsfraude is een zorgelijk fenomeen. Het probleem zal door de huidige ontwikkelingen alleen maar groter worden. Alles wordt digitaal, de samenleving wordt anoniemer en meer mensen leggen (onder andere door het toenemende gebruik van sociale media) hun informatie in de handen van private organisaties. Doordat organisaties veel persoonlijke informatie opslaan, zal dit leiden tot meer gerichte aanvallen en dus ook meer datahacks. Voor de slachtoffers wordt het daarnaast steeds moeilijker te bewijzen dat zij onschuldig zijn en dat hun identiteit is misbruikt.

6.4 Samengevat

- Phishing lijkt de meest voorkomende manier te zijn waarop identiteitsfraude wordt gepleegd.
- Wel is er mogelijk een vlucht van daders die deze methode gebruiken naar het buitenland waar meer kansen liggen via deze modus operandi.
- Een andere populaire methode zijn grootschalige datahacks.
- Experts achten het plausibel dat achter dit soort hacks (tijdelijke) samenwerkingsverbanden zitten waarbij er een taakverdeling is tussen de betrokkenen.
- Carder networks vormen sites waarop niet alleen vraag en aanbod van verboden waar (zoals creditcardnummers) worden verhandeld, maar waar ook vraag en aanbod van expertise voor het plegen van identiteitsfraude worden afgestemd.
- Experts zijn het erover eens dat identiteitsfraude door de digitalisering van de samenleving alleen maar zal toenemen. Meer en meer mensen leggen (onder meer door het gebruik van sociale media) persoonsinformatie in de handen van private organisaties. Doordat organisaties die informatie opslaan, zal dit leiden tot meer gerichte aanvallen en dus ook meer datahacks.

7

Conclusie en discussie

7.1 Conclusie

Door de toegenomen digitalisering van de maatschappij zijn de mogelijkheden om identiteitsfraude te plegen toegenomen. Ten eerste zijn voor daders meer geavanceerde technologische methoden beschikbaar die ze kunnen gebruiken om andermans gegevens te misbruiken. Voorbeelden hiervan zijn phishing en het gebruik van malware. Ten tweede is door de digitalisering meer informatie online beschikbaar. Bedrijven en overheden slaan persoonlijke gegevens grootschalig op in diverse databases (Bijlsma e.a., 2014), die niet altijd even goed beveiligd zijn. Deze databases zijn voor plegers van identiteitsfraude dan ook een aantrekkelijk doelwit, omdat daders op deze manier in één keer meer gegevens kunnen ontvreemden, dan wanneer ze bijvoorbeeld de computer van één slachtoffer kraken. Niet alleen bedrijven en overheden zorgen voor de beschikbaarheid van persoonlijke gegevens, ook de consument zorgt op verschillende manieren dat zijn eigen identiteit wordt blootgelegd. Het gebruik van sociale media is erg populair en het dagelijks leven kan op allerlei manieren worden gedeeld, zoals via Facebook, LinkedIn en Instagram (Bijlsma e.a., 2014).

Uit de internationale literatuur is gebleken dat identiteitsfraude een groot probleem vormt. Het prevalentiecijfer in de Verenigde Staten lag in 2012 op 7 procent van de bevolking (Harrell & Langton, 2013) en in het Verenigd Koninkrijk en Australië op 9,4 procent (UK National Fraud Authority, 2012; Smith & Hutchings, 2014), wat duidt op miljoenen slachtoffers per jaar in die landen. In de Europese Unie (Dynamics/Fellowes, 2012) ligt het geschatte percentage dat *ooit* slachtoffer is geworden op 17 procent. Identiteitsfraude zorgt voor aanzienlijke financiële schade. Voor de Verenigde Staten werd dit voor 2012 geschat op 24,7 miljard dollar (Harrell & Langton, 2013) en in het Verenigd Koninkrijk lag dit bedrag voor de jaren 2011 en 2012 gezamenlijk op 73 miljard pond (UK National Fraud Authority, 2012). Ook in Nederland lijkt identiteitsfraude een flink maatschappelijk probleem te vormen. Uit een grootschalige slachtofferenquête van PricewaterhouseCoopers (2013b) is gebleken dat 4,5 procent van de Nederlandse burgers in 2012 slachtoffer is geworden van een vorm van identiteitsfraude, met een geschatte financiële schade van 355 miljoen euro.

Niet alleen het hoge prevalentiepercentage en de geleden schade zorgen voor een probleem, ook de opsporing en aanpak van identiteitsfraude blijken lastig. Ten eerste vergroot internet de anonimiteit van daders, wat het opsporingsproces kan bemoeilijken. Daarnaast bestaat – ondanks de grote inhaalslag van de afgelopen jaren – nog steeds het probleem dat politiemensen relatief weinig kennis hebben over cybercrime (Stol e.a., 2012) en ook specifiek over identiteitsfraude (Wall, 2013). De identiteitsdelicten die slachtoffers bij de politie melden wijken af van het standaardpatroon, zijn vaak complex en, voor de gemiddelde, niet in cybercrime gespecialiseerde politieman of -vrouw, moeilijk te doorgronden (Wall, 2013). Om de kennis over identiteitsfraude te vergroten, is onderzoek naar deze vorm van criminaliteit dan ook nodig, om zicht te kunnen bieden op de aard, omvang en pleegwijze van dit delict. Met deze studie wordt daaraan bijgedragen.

Hoewel er in Nederland al eerder grootschalige studies zijn uitgevoerd op het gebied van identiteitsfraude, verschillen deze van onderhavig onderzoek. De studie van PricewaterhouseCoopers (2013b) biedt een overzicht van de aard en omvang van slachtofferervaringen voor verschillende vormen van identiteitsfraude. Die studie is echter minder gedetailleerd op het gebied van risicogroepen en -gedragingen. De studie van Domenie e.a. (2013) geeft wel meer inzicht in deze kenmerken, maar is minder gedetailleerd met betrekking tot verschillende vormen van identiteitsfraude en de modus operandi van dit delict – juist omdat in dat rapport de focus uitging naar de volle breedte van cyberdelicten. De onderhavige studie biedt een combinatie van de sterke punten uit de bovengenoemde onderzoeken. Ten eerste wordt er onderscheid gemaakt tussen verschillende vormen van identiteitsfraude, namelijk onrechtmatige bankafschrijving, misbruik van een creditcard en misbruik van persoonlijke gegevens voor frauduleuze doeleinden. Daarnaast is gebruikgemaakt van een grote en representatieve steekproef, met gedetailleerde gegevens over slachtoffers en niet-slachtoffers, zodat nauwkeurig kan worden nagegaan waarin deze groepen verschillen. Ten slotte is er in deze studie ook aandacht voor de modus operandi gebruikt door daders. Niet alleen is in die pleegwijze de nodige dynamiek te constateren, ook biedt inzicht daarin beter begrip hoe slachtofferschap tot stand kan komen. De meerwaarde van een dergelijk overzicht is dat duidelijker wordt met wat voor verschijnsel de samenleving en de politie te maken hebben: hoe groot is het probleem en welke factoren hangen ermee samen?

Het doel van dit onderzoek is een overzicht te geven van slachtofferschap van identiteitsfraude in Nederland. Dit is gedaan middels het beantwoorden van een aantal onderzoeksvragen die ingaan op de omvang, aard, schade en risicofacto-

ren van deze vorm van slachtofferschap, voor de periode 2008 tot 2012. Daarnaast zijn we ingegaan op gesignaleerde modus operandi door daders van identiteitsfraude. Bij het beantwoorden van de onderzoeksvragen is gebruikgemaakt van verschillende methoden. Zo zijn er gedetailleerde, kwantitatieve gegevens geanalyseerd uit een grootschalige enquête die in 2010 en 2012 is afgenomen onder een representatief deel van de Nederlandse bevolking, het zogenoemde LISS-panel. Daarnaast zijn er semigestructureerde interviews afgenomen met experts op het gebied van identiteitsfraude en is de wetenschappelijke literatuur omtrent bovengenoemde onderwerpen op een rij gezet.

Uit de enquêtegegevens – waarin burgers is gevraagd naar hun slachtofferervaringen over de voorafgaande twee jaar – blijkt dat slachtofferschap van identiteitsfraude zowel in de periode 2008-2010 als 2010-2012 voorkwam onder 4,6 procent van de bevolking van 15 jaar en ouder. De gevonden percentages liggen lager dan de prevalentiecijfers van andere westerse landen, zoals de Verenigde Staten en het Verenigd Koninkrijk, waarbij wel moet worden aangetekend dat de vraagstelling in deze landen niet identiek was. Uit deze studie is daarnaast gebleken dat bankfraude als vorm van identiteitsfraude in beide perioden het meest prevalent is. Bankfraude – waarbij het slachtoffer constateert dat er ten onrechte geld van de rekening is afgeschreven – is, volgens dit onderzoek, met ongeveer 70 procent van het totaal de meest voorkomende vorm van slachtofferschap van identiteitsfraude in Nederland. Deze vorm wordt gevolgd door creditcardfraude en tot slot de (zeldzame) overige vormen van identiteitsfraude. Volgens het onderzoek van PricewaterhouseCoopers (2013b) komt financiële fraude het meest voor in Nederland, wat overeenkomt met de resultaten uit onze studie. Studies die de aard van identiteitsfraude in de Verenigde Staten betreffen, laten echter een ander beeld zien. Creditcardfraude is in de Verenigde Staten de meest prevalente vorm van identiteitsfraude (Anderson, 2006; Winterdyk & Thompson, 2008; Copes e.a., 2010). Naast omvang en aard is ook herhaald slachtofferschap bekeken. Uit de resultaten is gebleken dat voor alle vormen geldt dat de meeste slachtoffers eenmalig slachtoffer worden. Herhaald slachtofferschap komt weliswaar voor, maar niet op grote schaal.

Wanneer gekeken wordt naar de financiële schade (die met behulp van de LISS-paneldata alleen kon worden vastgesteld voor bankfraude), is gebleken dat in 2010 het gemiddeld afgeschreven bedrag per slachtoffer lag op 407 euro en in 2012 op 382 euro.[32] Opvallend daarbij is dat de slachtoffers die zich bij de

32 Zoals ook toegelicht in hoofdstuk 5, is hierbij aan enkele gevallen met zeer hoge schade een plafondwaarde ingesteld van 2500 euro, om de invloed van deze uitschieters op de gemiddelde schade te beperken.

politie melden om aangifte te doen niet alleen een kleine minderheid is (circa 10% van alle slachtoffers), maar ook bovengemiddeld veel schade hebben geleden. Het betreft dus vooral de ernstiger gevallen die zich bij de politie kenbaar maken. Meer dan 80 procent van alle slachtoffers krijgt de oorspronkelijk geleden schade volledig vergoed, zodat een minderheid van hen uiteindelijk daadwerkelijk financiële schade lijdt. Wel is er uiteraard een maatschappelijke schadepost voor banken en hun klanten, die voor de periode 2008-2010 naar schatting tussen de 147 en 248 miljoen euro bedroeg en in de periode 2010-2012 tussen de 134 en 228 miljoen euro. Wanneer de nationale en internationale literatuur erop nageslagen worden, blijkt dat meerdere studies rapporteren dat de (internationale) maatschappelijke schade daalt (Van der Meulen, 2006; Anderson e.a., 2008; Harrell & Langton, 2013). Ook het schadebedrag per persoon is volgens onderzoek aan het afnemen (Anderson, 2008; PwC, 2013b). Deze uitspraken zijn op basis van dit onderzoek echter voor Nederland niet te bevestigen.

Ten slotte is uit de resultaten gebleken dat slachtofferschap van alle vormen van identiteitsfraude nauwelijks samenhangt met individuele kenmerken of gedragingen van potentiële doelwitten. Dit was een onverwachte bevinding. Uit eerder onderzoek kwamen namelijk enkele risicogroepen naar voren: mannen, hoger opgeleiden en mensen met hoge inkomens (Allisson e.a., 2005; Anderson, 2006; Copes e.a., 2010; Harrell & Langton, 2013; PwC, 2013b; Reyns, 2013). Deze groepen komen echter niet eenduidig terug als risicogroepen in de door ons gebruikte (representatieve) LISS-panelgegevens. Zo lopen mannen meer kans op creditcardfraude dan vrouwen, maar er is geen verschil voor bankfraude. Voor inkomen vonden we zelfs geen relatie met slachtofferschap van deze twee vormen van identiteitsfraude. Wel zien we inderdaad dat hoger opgeleiden wat meer risico lopen op zowel bankfraude als creditcardfraude dan lager opgeleiden.

Wanneer andere risicokenmerken en -gedragingen worden gerelateerd aan de kans om in aanraking te komen met identiteitsfraude, is een tweetal zaken opvallend. Ten eerste houden het gebruik van sociale media en het plaatsen van gegevens op die media in de periode 2008-2010 verband met slachtofferschap van bankfraude en creditcardfraude: meer risico bij actiever gebruik. Deze verbanden vallen in de volgende periode (2010-2012) echter weg. Een ander opvallend resultaat is dat goede beveiliging op de computer samengaat met een hogere kans op slachtofferschap. De vraag is echter of goed beveiligde doelwitten specifieke kenmerken bezitten die hen blootstellen aan een hoger risico. In dat geval is er geen causale relatie tussen beveiliging en slachtofferschap. Een andere mogelijkheid zou kunnen zijn dat beveiliging zorgt voor een onterecht gevoel van veiligheid en daarmee onvoorzichtiger gedrag in de hand werkt.

Om meer duidelijk te krijgen over de wijze waarop verschillende factoren op elkaar ingrijpen en het risico op slachtofferschap van identiteitsfraude in de hand werken, zijn aanvullende analyses uitgevoerd met behulp van regressiemodellen. Hierin houden we rekening met zowel achtergrondkenmerken, internetgedragingen, beveiligingsmaatregelen en houding ten aanzien van het nemen van risico's (via een gevalideerde schaal omtrent zelfcontrole). Een dergelijk uitgebreid verklaringsmodel dat wordt toegepast op een representatieve steekproef van de bevolking vormt een unicum in het wetenschappelijk onderzoek naar identiteitsfraude, ook internationaal gezien. Op dat punt boeken we ten opzichte van eerdere studies dus duidelijke vooruitgang. Hoewel theoretisch gezien vanuit een gelegenheidsmodel (Cohen & Felson, 1979; Reyns, 2013) verwacht werd dat slachtofferschap afhangt van facetten die de blootstelling aan daders, bescherming tegen daders en aantrekkelijkheid voor daders bepalen, zien we in onze resultaten dat een uitgebreid palet aan internetactiviteiten (inclusief sociale-mediagebruik) en genomen preventiemaatregelen *niet* gerelateerd is aan bankfraude. Dat is – opnieuw – een onverwachte bevinding. Het meest consistent komt het vaak gebruiken van internetbankieren uit de analyses als risicoverhogend naar voren, maar het verband is zwak. Voor creditcardfraude zien we dat het model beter voorspelt, maar dat dit tegelijk veel te maken heeft met een voor de hand liggende voorspeller: het gebruik van een creditcard. Voor creditcardfraude speelt in 2012 daarnaast een aantal extra factoren mee: lage zelfcontrole, een hoog opleidingsniveau, het vaak controleren op virussen, het kijken van korte video's online en het invullen van online enquêtes. Maar ook voor creditcardfraude geldt dat de tijd die men aan allerlei andere internetactiviteiten besteedt, de hoeveelheid persoonlijke informatie die men op internet vermeldt en de genomen computerbeveiligingsmaatregelen niet meespelen in de voorspelling van het risico op slachtofferschap. De eerder gememoreerde opmerkelijke correlatie tussen betere preventie en hoger risico kon met behulp van dit model worden geduid: omdat het verband tussen computerbeveiligingsmaatregelen en slachtofferschap van identiteitsfraude wegviel in de regressiemodellen, duidt dit erop dat degenen die actief internetbankieren en een creditcard gebruiken ook degenen zijn die zich beter hebben beveiligd. Welke richting dit verband heeft is onduidelijk: mogelijk anticiperen degenen die actief internetbankieren op hun verhoogde risico met betere beveiliging, maar andersom kan het ook zijn dat betere beveiliging voor een gevoel van veiligheid zorgt en daarmee leidt tot meer actief internetbankieren. Het beperkte vermogen van het huidige model om patronen in slachtofferschap te voorspellen geeft aan dat er geen duidelijk risicoprofiel te schetsen is op basis

van de huidige gegevens. Mogelijk spelen de internetactiviteiten van doelwitten wel een rol in de totstandkoming van risico's op identiteitsfraude, maar op een andere manier dan via algemene blootstelling, zoals nu is verondersteld. Daarom moet in toekomstig onderzoek gevraagd worden naar bezoek van *specifieke*, door malware besmette, sites in plaats van naar algemeen internetgedrag: welke concrete sites heeft iemand bezocht? In hoeverre dat via alternatieve databronnen moet plaatsvinden (bijvoorbeeld via toestemming van providers om internetverkeer – geanonimiseerd – te analyseren) is een open vraag. Zodoende kan mogelijk duidelijker worden waarom de ene persoon getroffen wordt door identiteitsfraude en de ander niet.

Op basis van de interviews met twaalf experts omtrent de modus operandi bij identiteitsfraude kan worden gesteld dat zij het over bepaalde zaken en ontwikkelingen eens zijn. Ten eerste geven zij vrij eensgezind aan dat phishing op dit moment de populairste methode is om identiteitsfraude mee te plegen. Ook wordt de overtuiging gedeeld dat skimming door preventieve maatregelen – zoals invoering van de EMV-chip en geo-blocking – sterk is gedaald. Hoewel phishing populair is, neemt het volgens sommigen wel af in Nederland en zijn er twee verschuivingstendensen op te merken. Ten eerste lijken bepaalde modus operandi (zoals skimming en phishing) zich te verplaatsen naar het buitenland. Zeker buiten West-Europa zijn de preventieve maatregelen van onder andere de banken minder sterk ontwikkeld, waardoor deze landen nu aantrekkelijker zijn. De respondenten verwachten wel dat criminelen weer nieuwe, geavanceerdere methoden zullen bedenken die weer toegepast kunnen worden in Nederland. Nederland is namelijk wel een aantrekkelijk land voor identiteitsfraudeurs, vanwege de combinatie van een hoog niveau van welvaart en internetaansluiting. De tweede verschuiving die volgens een aantal experts plaats lijkt te vinden, is de verschuiving van phishing via *e-mail* naar phishing via *sociale media*. Deze verschuiving werd geconstateerd door zowel de respondenten van Europol, als in de literatuuranalyse (Symantec Corporation, 2014). Voor toekomstig onderzoek onder doelwitten is daarom de vraag van belang wie via phishing worden benaderd en wie daar vervolgens ook op ingaan en slachtoffer worden.

Daarnaast deelden veel van de geïnterviewde experts de visie dat identiteitsfraude vaak georganiseerde criminaliteit betreft en dat voor veel methoden samenwerking vereist is. Door middel van zogenaamde carder networks wordt deze samenwerking gefaciliteerd en versterkt (zie bijvoorbeeld Soudijn & Monsma, 2012). Carder networks bestaan niet alleen om samenwerking te faciliteren, maar ook om vraag en aanbod van bijvoorbeeld malware en gestolen creditcardgegevens te stroomlijnen. Hackers bieden zich daarnaast op deze

sites aan, om tegen een vergoeding software te ontwikkelen waarmee identiteitsgegevens kunnen worden buitgemaakt. Deze ontwikkeling brengt met zich mee dat ook 'niet-hackers' digitale criminaliteit kunnen plegen – zij kopen de door hackers ontwikkelde software.

Hoewel de experts het dus op een aantal punten met elkaar eens zijn, zijn er ook een aantal kennislacunes aan te merken. Zo is er weinig bekend over hoe vaak welke methoden worden ingezet door daders om criminaliteit te plegen, want harde cijfers op dit gebied ontbreken. Daarnaast hebben de experts, hoewel ze vermoedens hebben, weinig kennis over daders, hoe de netwerken precies in elkaar zitten en welke samenwerkingsverbanden bestaan. Ook uitspraken over wat er met de gestolen gegevens en het criminele geld gebeurt, blijven hypothetisch van aard. De experts zijn het er in ieder geval over eens dat het een groot, internationaal probleem is en zal blijven, zeker door verdere technologische ontwikkelingen. Ze pleiten dan ook voor een goede beveiliging van gegevens door bedrijven, overheden en consumenten (NCSC, 2014), voor privaat-publieke samenwerking (Stol e.a., 2012) en voor het laten toenemen van risicobewustzijn onder deze verschillende partijen (Bijlsma e.a., 2014).

7.2 Discussie

Ter besluit van dit rapport staan we stil bij een aantal mogelijkheden om toekomstig onderzoek op dit terrein verder vorm te geven. Ten eerste is het goed om te vermelden dat het gebruik van slachtofferenquêtegegevens, zoals in dit rapport met de LISS-paneldata, een aantal voor- en nadelen heeft. Ten opzichte van de officiële registraties die instanties bijhouden, bieden enquêtegegevens een aantal voordelen. Incidenten die niet geregistreerd zijn, maar wel hebben plaatsgevonden, kunnen via een enquête worden gemeten. Op die manier kan, in combinatie met een representatieve steekproef zoals bij de LISS-paneldata het geval is, een volledige schatting worden gegeven van de prevalentie van identiteitsfraude. Daarnaast kunnen de kenmerken van de slachtoffers worden vergeleken met niet-slachtoffers – omdat beide groepen in de enquête worden bevraagd – zodat een risicoprofiel kan worden geschetst. Tot slot is er, zeker bij de LISS-paneldata, de mogelijkheid om dit risicoprofiel gedetailleerd op te stellen omdat er in de enquête naar veel persoonskenmerken is gevraagd: in hoeverre zien we verschillen tussen de slachtoffers en niet-slachtoffers op het gebied van internetgebruik, sociale-mediagedrag, computerbeveiliging enzovoort?

Onfeilbaar is de enquêtemethode echter niet. Respondenten kunnen zich bijvoorbeeld zaken niet of verkeerd herinneren. Het zou kunnen dat gevallen van identiteitsfraude de respondent niet zijn opgevallen (bijvoorbeeld vanwege het onvoldoende controleren van de bankrekening), de respondent kan de incidenten wellicht niet correct in de tijd plaatsen (bijvoorbeeld: het incident is langer dan twee jaar geleden maar de respondent herinnert het zich als een recent delict), of het kan voorkomen dat de respondent wel iets heeft meegemaakt, maar daar in de enquête niet over wil praten. Deze foutenbronnen kunnen aanwezig zijn, maar het is moeilijk in te schatten hoe vaak. Een optie zou zijn om de in slachtofferenquêtes opgegeven incidenten – waarvan de slachtoffers zeggen ze ook te hebben aangegeven bij een instantie, zoals politie of bank – te verifiëren in registratiebestanden. Een andere beperking is dat ernstige fraude-incidenten vanwege hun lage prevalentie niet vaak gemeten zullen worden in steekproeven van enkele duizenden burgers. Indien de aandacht juist naar dit soort incidenten uitgaat, verdienen registratiebestanden van banken of politie waarschijnlijk juist de voorkeur voor onderzoek.

Om meer te weten te komen over de modus operandi van identiteitsfraudeurs, bieden de slachtofferenquêtegegevens van het LISS-panel geen goede mogelijkheden, omdat die voor veel slachtoffers in de enquête onbekend is. Daarom is gekozen voor het houden van interviews met een aantal experts op het gebied van identiteitsfraude. Om een zo goed mogelijk beeld te krijgen van de modus operandi, vertegenwoordigen de experts uiteenlopende sectoren op het gebied van identiteitsfraude (publiek en privaat). Daarnaast is aan de experts telkens dezelfde vragenlijst voorgelegd, zodat de antwoorden goed vergeleken konden worden. Uiteindelijk hebben de interviews bruikbare informatie verschaft om de onderzoeksvraag te kunnen beantwoorden. In dit licht moet wel gesteld worden dat de experts vaak niet met zekerheid konden antwoorden. Daarnaast heeft elke expert de vragen beantwoord vanuit zijn of haar werkveld. Uit de interviews is gebleken dat dit de resultaten enigszins kan beïnvloeden. Bepaalde experts spraken elkaar soms tegen, omdat zij de vragen vanuit hun oogpunt en expertise hebben beantwoord. Een voorbeeld is dat een respondent, vanwege de lowtech-zaken waar hij mee te maken krijgt, dacht dat de modus operandi van identiteitsfraude vooral lowtech van aard is en dat daders ook niet samenwerken. Deze visie bleek op zichzelf te staan, omdat de overige respondenten het tegenovergestelde signaleerden in de praktijk.

In hoeverre kunnen we, op basis van dit onderzoek, identiteitsfraude kwalificeren als een groot maatschappelijk probleem, nu en in de toekomst? Wanneer naar de omvang en de geleden schade wordt gekeken, is gebleken dat identi-

teitsfraude qua omvang (4,6% in 2012) niet veel afwijkt van andere vormen van criminaliteit, zoals fietsendiefstal (3,7% van de bevolking werd slachtoffer in 2012, CBS). Ten tweede is gebleken dat de meerderheid van de slachtoffers uiteindelijk geen schade lijdt, omdat in meer dan 80 procent van de gevallen de schade vergoed wordt, meestal door de bank. Daarnaast lieten de resultaten zien dat wanneer er wel een nettoschadebedrag overblijft, meer dan 90 procent van de slachtoffers niet meer dan 50 euro kwijt is. De uiteindelijke individuele financiële schade lijkt dus, uitzonderingen daargelaten, mee te vallen. Niettemin draaien banken en verzekeringsmaatschappijen wel op voor deze kosten – en uiteindelijk hun klanten. Er is dus zeker sprake van een hoge maatschappelijke schade, naar schatting tussen de 134 en 228 miljoen euro in de periode 2010 tot 2012. In deze context moet ook nog worden gesteld dat de banken vanaf 2014 hun regels hebben verscherpt op het gebied van vergoeding. Zo moeten cliënten van een aantal banken[33] volgens de Consumentenbond (NOS, 2013), elke week hun bankafschriften controleren en mogen ze nergens hun pincode opschrijven, ook niet in versleutelde vorm. Wanneer een consument zich niet aan deze regels houdt, is de kans op vergoeding kleiner. Verder onderzoek zou moeten uitwijzen of de nettoschade voor slachtoffers door deze regeling juist weer toeneemt of dat de nettoschade voor slachtoffers laag blijft. Een ander aandachtspunt voor de toekomst in deze context, is dat het vergoedingsbeleid mogelijk selectief is. Onderzoek van Van Wilsem en anderen (2013) laat bijvoorbeeld zien dat lager opgeleiden een kleinere kans hebben om de gerapporteerde schade vergoed te krijgen. In hoeverre dat in het nieuwe vergoedingsstelsel geldt, dient nader te worden onderzocht. Hoewel schade en omvang van identiteitsfraude geen extreme vormen aan lijken te nemen, kan op basis van de literatuur en de resultaten uit dit onderzoek wel gesteld worden dat het een groter maatschappelijk probleem zou kunnen worden.

Een opvallend resultaat dat naar voren is gekomen in dit onderzoek, is dat slachtofferschap van identiteitsfraude – en met name bankfraude – nauwelijks op individueel niveau verklaard kan worden. Hoewel er de beschikking was over een groot databestand en gedetailleerde metingen van individueel gedrag (zoals op het gebied van internetgebruik, persoonlijke levensomstandigheden en impulsiviteit), bleken er weinig verbanden te zijn met het wel of niet meemaken van identiteitsfraude. Zowel de enquête als de experts schetsen het beeld dat individueel gedrag niet de enige risicofactor vormt, maar dat beveiliging

33 Elke bank hanteert andere voorwaarden. Het verschilt per bank welke regels zijn gesteld met betrekking tot het vergoeden van schade geleden door slachtofferschap van identiteitsfraude.

van gegevens door organisaties, een andere belangrijke component vormt. Uit de literatuur en uit de interviews is gebleken dat er hierbij sprake is van een gedeelde verantwoordelijkheid. Ten eerste is uit onderzoek gebleken dat de gemiddelde Nederlander in honderden databestanden (Schermer & Wagemans, 2009) geregistreerd staat met zijn of haar persoonlijke gegevens. Volgens Schermer en Wagemans (2009) zal dit aantal, ook door digitalisering van de maatschappij, alleen nog maar toenemen. Hoewel burgers vaak wel weten dat ze in databestanden geregistreerd staan, weten ze vaak niet op welke schaal en voor welke doeleinden hun informatie wordt gebruikt. Wanneer deze databestanden niet goed beveiligd zijn, zijn ze voor plegers van identiteitsfraude een aantrekkelijk doelwit. Dat dergelijke bestanden niet altijd voorzien zijn van een waterdichte beveiliging, is onder andere gebleken uit hacks bij KPN, Diginotar en het Groene Hart Ziekenhuis in Gouda. PricewaterhouseCoopers (2013c) meldt in een rapportage dat vandaag de dag, bedrijven vaak vertrouwen op de veiligheid van beveiligingsstrategieën van gisteren. Kwaadwillenden gebruiken, volgens de auteurs, juist de technologieën van de toekomst en de bedrijven zijn hier niet altijd op ingespeeld. Hoewel bedrijven en overheden dus een bepaalde verantwoordelijkheid dragen voor het beschermen van de persoonsgegevens van hun cliënten, is het belangrijk dat de consument zelf zich ook hiermee bezighoudt. Bijlsma en anderen (2014) spreken in dit verband over de privacyparadox. Burgers eisen enerzijds dat de overheid zo min mogelijk gegevens verzamelt, daar voorzichtig mee omgaat en hun privacy zo min mogelijk schendt, maar anderzijds zorgen ze er ook zelf voor dat hun gegevens, en soms zelfs details van hun persoonlijke leven, openbaar worden gemaakt. Door gebruik te maken van bijvoorbeeld sociale media, apps, webshops en chatrooms, gaat de consument bewust en onbewust akkoord met voorwaarden die zijn privacy vaak niet ten goede komen. Of dit ligt aan het feit dat burgers hier niet van op de hoogte zijn, of aan het feit dat de voordelen van het gebruik van dergelijke diensten opwegen tegen het opgeven van de privacy, dient nader te worden uitgezocht.

Een belangrijk middel om dergelijke problemen onder de aandacht van een groot publiek te brengen, zijn bijvoorbeeld reclames, informatiepunten, websites en folders. Voor sommige methoden om identiteitsfraude te plegen, is dit door de overheid in het verleden gedaan. Denk hierbij aan de campagnes 'Veilig Bankieren' en 'Pas op je Pas', om bewustzijn te kweken voor respectievelijk phishing en de money mules. Daarnaast bestaan er verschillende websites (onder andere van de Fraudehelpdesk) die informatie over identiteitsfraude verschaffen. Op het gebied van onder andere Facebook, WhatsApp, apps,

inschrijvingen bij diverse websites en bedrijven, is echter niet of nauwelijks informatie beschikbaar die inzichtelijk maakt hoe er met persoonlijke gegevens wordt omgegaan. Het zou goed zijn om de burger bewuster te laten worden van het feit dat identiteitsfraude ook op deze manieren kan plaatsvinden. Bijlsma en anderen (2014) noemen in deze context het voorbeeld van een privacykeurmerk. Zij stellen dat door keurmerken te gebruiken, de burger vooraf geïnformeerd kan worden of een bedrijf zich aan de regels houdt met betrekking tot bescherming van hun gegevens. Een dergelijke oplossing is een voorbeeld van hoe het bewustzijn onder burgers vergroot kan worden. Naast informatieverstrekking aan burgers, moeten ook bedrijven die met persoonsgegevens omgaan, goed geïnformeerd zijn (én blijven) op het gebied van beveiliging van gegevens en de daaraan gerelateerde gevaren. Rhee, Ryu en Kim (2012) hebben door middel van interviews met Amerikaanse IT-specialisten onderzocht of er sprake is van een té positief denken over risico's met betrekking tot cyberaanvallen. Zij stelden dat er onder deze groep regelmatig sprake is van een zogeheten optimistische bias en dat, hoewel de specialisten op de hoogte zijn van risico's, ze niet denken dat hun organisatie zelf een doelwit is en dat dus de risico's voor hun organisatie klein zijn. Een dergelijke bias kan de mate van cybersecurity beïnvloeden. Om dus de juiste voorlichting te kunnen verstrekken, zou het nuttig zijn in kaart te brengen hoe het er op dit moment voor staat met het beveiligingsgedrag van bedrijven in Nederland en welke overwegingen zij hanteren om op een bepaalde manier en in een bepaalde mate te beveiligen.

Het beeld dat uit dit geheel oprijst, is dat identiteitsfraude een probleem is dat zeker niet alleen door de politie aangepakt dient te worden. Sterker nog, omdat veel acties die vanuit de politie worden opgestart aangiftegestuurd zijn, is er weinig druk, gezien het beperkte aantal slachtoffers dat aangifte doet van identiteitgerelateerde delicten (circa 10% volgens onze gegevens). Uiteraard is er voor de politie een duidelijke taak om te investeren in opsporing van identiteitsfraude – wat gezien de aspecten omtrent territorialiteitskwesties, expertise en mankracht geen sinecure is –, maar er ligt ook een duidelijke verantwoordelijkheid, met name op het gebied van preventie, bij andere partijen. Een belangrijke rol ligt daarin zoals gezegd bij burgers zelf, maar ook bij banken (voor investeringen in de beveiliging van hun betalingsverkeer en blijvende ontwikkeling van risico-instrumenten om verdachte transacties te herkennen), providers (om klanten tegen malware te beschermen) en andere organisaties in de private of publieke sector (om zorg te dragen voor adequate beveiliging van klantgegevens en authenticatieprocedures). Verder ligt bij deze partijen voor het mogelijk maken van een adequate opsporing door politie en justitie ook een

verantwoordelijkheid voor informatiedeling. Ofwel, bij preventie van identiteitsfraude kan de politie vooral door te 'signaleren en adresseren' eraan bijdragen dat de juiste partijen erbij worden betrokken.

Ten slotte is het belangrijk voortdurend onderzoek te blijven doen naar het fenomeen identiteitsfraude. Dit delict zal naar verwachting met de huidige en toekomstige technische ontwikkelingen meegroeien. Voor politie, justitie, maar ook voor andere organisaties en bedrijven is het dus van belang dat de kennis op dit gebied actueel blijft.

Literatuur

Ablon, L., Libicki, M.C. & Golay, A.A. (2014). *Markets for Cybercrime Tools and Stolen Data: Hackers' Bazaar.* Rand Corporation.

Allison, S.F.H., Schuck, A.M. & Lersch, K.M. (2005). Exploring the crime of identity theft: Prevalence, clearance and victim/offender characteristics. *Journal of Criminal Justice*, 33(1), 19-29.

Anderson, K.B. (2006). Who Are the Victims of Identity Theft? The Effect of Demographics. *American Marketing Association*, 25(2), 160-171.

Anderson, K.B., Durbin, E. & Salinger, M.A. (2008). Identity Theft. *Journal of Economic Perspectives*, 22(2), 171-192.

Bijleveld, C.C.J.H. (2006). *Methoden en Technieken van Onderzoek in de Criminologie.* Den Haag: Boom Juridische Uitgevers.

Bijlsma, M., Straathof, B. & Zwart, G. (2014). *Kiezen voor privacy. Hoe de markt voor persoonsgegevens beter kan.* Geraadpleegd op http://www.cpb.nl/publicatie/kiezen-voor-privacy-hoe-de-markt-voor-persoonsgegevens-beter-kan.

Bilge, L., Strufe, T., Balzarotti, D. e.a. (2009). All your contacts belong to us: automated identity theft attacks on social networks. *Proceedings of the 18th internationals conference on World wide web*, 551-560. ACM.

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

Bossler, A.M., Holt, T.J. & May, D.C. (2010). Low Self-Control, Deviant Peer Associations and Juvenile Cyberdeviance. *American Journal of Criminal Justice*, 37(3), 378-395.

Bossler, A.M., Holt, T.J. & May, D.C. (2012). Predicting online harassment victimization among a juvenile population. *Youth & Society*, 44, 500-523.

Brody, R.G., Mulig, E. & Kimball, V. (2007). Phishing, pharming and identity theft. *Academy of Accounting and Financial Studies Journal*, 11(3), 43-56.

Centraal Bureau van de Statistiek (2013). *Veiligheidsmonitor* 2012. Geraadpleegd op http://www.cbs.nl/nl-NL/menu/themas/veiligheid-recht/publicaties/publicaties/archief/2013/2013-veiligheidsmonitor-2012-pub.htm.

CIPPIC (2007). *Techniques of Identity Theft, CIPPIC Working Paper No. 2* (ID theft series). Ottawa: Canadian Internet Policy and Public Interest Clinic.

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

Collins, J.M. & Hoffman, S.K. (2004). *Identity Theft: Predator Profiles*. Unpublished manuscript.

Copes, H. & Vieraitis, L.M. (2009). Understanding Identity Theft: Offenders' Accounts of Their Lives and Crimes. *Criminal Justice Review*, 34(3), 329-349.

Copes, H., Kerley, K.R. & Huff, R. e.a. (2010). Differentiating Identity theft: An exploratory study of victims using a national victimization survey. *Journal of Criminal Justice*, 38(5), 1045-1052.

Dijkhof, K. (2014, 12 maart). Amendement identiteitsfraude [blogpost]. Geraadpleegd op https://dijkhoff.info/2014/03/amendement-identiteits-fraude-2/.

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

Dynamics/Fellowes. (2012). *ID Fraud Prevention Research 2012*. Commissioned by Fellowes.

Europol (2013). *EU Serious and Organised Crime Threat Assessment (SOCTA) 2013*. Geraadpleegd op https://www.europol.europa.eu/content/eu-serious-and-organised-crime-threat-assessment-socta.

Foresight (2013). *Future Identities. Changing Identities in the UK: The Next 10 Years*. Londen: Government Office for Science.

Genova, M. (2014). *Komt een vrouw bij de hacker*. Meppel: Just Publishers.

Gercke, M. (2007). Internet-Related Identity Theft. *Economic Crime Division, Directorate General of Human Rights and Legal Affairs, Strasbourg, France*.

Harrell, E. & Langton, L. (2013). Victims of Identity Theft, 2012. *Bureau of Justice Statistics*.

Holt, T.J. (2013). Exploring the social organization and structure of stolen data markets. *Global Crime*, 14(2-3), 155-174.

Holt, T.J. & Turner, M.G. (2012). Examining Risks and Protective Factors of On-Line Identity Theft. *Deviant Behavior*, 33(4), 308-323.

ITRC (2013). *Identity Theft: The Aftermath* 2013. Geraadpleegd op http://www.idtheftcenter.org/images/surveys_studies/Aftermath2013.pdf.

Javelin Strategy and Research (2014). *2014 Identity Fraud Report*. Geraadpleegd op https://www.javelinstrategy.com/uploads/web_brochure/1405.R_2014IdentityFraudReportBrochure.pdf.

Koninklijke Marechaussee/Korps landelijke politiediensten, Expertise Centrum Identiteitsfraude en Documenten (2014). *Statistisch Jaaroverzicht Documentfraude* 2013.

Koops, B.J. (2012). De dynamiek van cybercrimewetgeving in Europa en Nederland. *Justitiële Verkenningen*, 38(1), 9-24.

Koops, B.J., Leenes, R., Meints, M. e.a. (2009). A Typology Of Identity-Related Crime. Conceptual, technical and legal issues. *Information, Communication & Society*, 12(1), 1-24.

Marshall, A.M. & Tompsett, B.C. (2005). Identity theft in an online world. *Computer Law & Security Report*, 21(2), 128-137.

Martijn, M. (2014, 20 maart). Dit geef je allemaal prijs als je inlogt op een openbaar wifi netwerk. *De Correspondent*. Geraadpleegd op https://decorrespondent.nl/845/dit-geef-je-allemaal-prijs-als-je-inlogt-op-een-openbaar-wifi-netwerk/64356981260-dfc3519d.

Meulen, N. van der (2006). The challenge of countering identity theft: recent developments in the United States, the United Kingdom, and the European Union. *Report Commissioned by the National Infrastructure Cyber Crime program (NICC)*.

Meulen, N. van der (2010). *Fertile Grounds: The Facilitation of Financial Identity Theft in the United States and the Netherlands*. (Doctoral dissertation)

Meulen, N. van der (2012). Eigen schuld, dikke bult? Aansprakelijkheid bij fraude met Internetbankieren. *Informatiebeveiliging*, 10(8), 7-11.

Ministerie van Binnenlandse Zaken en Koninkrijkrelaties (2013). *Identiteit in Cijfers, versie 1*. Ministerie van Veiligheid en Justitie (2010). *Handreiking politie Identiteitsfraude*.

Nederlandse Vereniging van Banken (2014). Fraude [blogpost]. Geraadpleegd op http://www.nvb.nl/thema-s/veiligheid-fraude/166/fraude.html.

Nationaal Cyber Security Centrum (2014). *Cybersecuritybeeld Nederland 4*. Geraadpleegd op https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/trendrapporten/cybersecuritybeeld-nederland-4.html.

Newman, G.R. & McNally, M.M. (2005). Identity theft literature review. *United States Department of Justice: National Institute of Justice.*

Ngo, F.W. & Paternoster, R. (2011). Cybercrime Victimization: An examination of Individual and Situational level factors. *International Journal of Cyber Criminology*, 5(1), 773-793.

NOS (2013, 24 januari). Banken minder coulant bij phishing. Geraadpleegd op https://nos.nl/artikel/465968-banken-minder-coulant-bij-phishing.html.

Oosterveer, D. (2014, 13 maart). De laatste cijfers van het socialmediagebruik in Nederland. Alle cijfers op een rijtje van onder andere Twitter, Facebook, LinkedIn, Google+, Pinterest, Instagram en meer [blogpost]. Geraadpleegd op: http://www.marketingfacts.nl/berichten/socialmediagebruik-in-nederland-update-maart-2014.

PricewaterhouseCoopers (PwC) (2013a). *Centraal Meld- en informatiepunt Identiteitsfraude en -fouten. Analyse meldingen 2011-2012.* Geraadpleegd op http://www.rijksdienstvooridentiteitsgegevens.nl/dsresource?objectid=43141&type=pdf.

PricewaterhouseCoopers (PwC) (2013b). *2013 Update onderzoek 'Omvang van identiteitsfraude & maatschappelijke schade in Nederland'*. Geraadpleegd op http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2013/05/23/omvang-van-identiteitsfraude-en-maatschappelijke-schade-in-nederland.html.

PricewaterhouseCoopers (PwC) (2013c). *Defending yesterday*. Orange County, California: PwC.

Reyns, B.W. (2013). Online Routines and Identity Theft Victimization: Further Expanding Routine Activity beyond Direct-Contact Offenses. *Journal of Research in Crime and Delinquency*, 50(2), 216-238.

Rhee, H.S., Ryu, Y.U. & Kim, C.T. (2012). Unrealistic optimism on information security management. *Computer & Security*, 31(2), 221-232.

Schermer, B.W. & Wagemans, T. (2009). *Onze digitale schaduw. Een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander geregistreerd staat.* College Bescherming Persoonsgegevens, Den Haag.

Smith, R.G. & Hutchings, A. (2014). Identity crime and misuse in Australia: Results of the 2013 online survey. *AIC Reports: Research and Public Policy Series.* Australian Government: Australian Institute of Criminology.

Sproule, S. & Archer, N. (2008). *Measuring Identity Theft in Canada: 2006 Consumer Survey*. Hamilton, Ontario: McMaster eBusiness Research Centre (MeRC).

Soudijn, M. & Monsma, E. (2012). Virtuele ontmoetingsruimtes voor cybercriminelen. *Tijdschrift voor Criminologie*, 54(4), 349-360.

Stol, W., Leukfeldt, E.R. & Klap, H. (2012). Cybercrime en politie: Een schets van de Nederlandse situatie anno 2012. *JustitiëleVerkenningen*, 38(1), 25-39.

Symantec Corporation (2014). *Internet Security Threat Report* 2014. Geraadpleegd op http://www.symantec.com/content/en/us/enterprise/other_resources/bistr_main_report_v19_21291018.en-us.pdf.

UK National Fraud Authority (2012). *Annual Fraud Indicator, March* 2012. Geraadpleegd op https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118530/annual-fraud-indicator-2012.pdf.

Vries, U.R.M.T. de, Tigchelaar, H., Linden, M. van der e.a. (2007). *Identiteitsfraude: Een Afbakening, een Internationale Begripsvergelijking en Analyse van Nationale Strafbepalingen*. Den Haag: Boom Juridische Uitgevers.

Wall, D.S. (2013). Policing identity crimes. *Policing & Society*, 23, 437-460.

Wilsem, J. van (2012). Slachtofferschap van identiteitsfraude. Een studie naar aard, omvang, risicofactoren en nasleep. *JustitiëleVerkenningen*, 38(1), 97-107.

Wilsem, J. van (2013). Hacking and Harassment – Do They Have Something in Common? Comparing risk factors for online victimization. *Journal of Contemporary Criminal Justice*, 29, 437-453.

Wilsem, J. van, Arnold, E. & Buren, C. van e.a. (2010). Is online zichtbaarheid riskant? Onrechtmatige bankafschrijvingen en persoonlijke informatie op sociale-netwerksites. *PROCES*, 89(5), 344-354.

Wilsem, J. van, Meulen, N. van der, Kunst, M. e.a. (2013). Je geld kwijt, en dan? Financiële schade bij slachtoffers van onrechtmatige bankafschrijvingen. *Tijdschrift voor Criminologie*, 55(4), 360-374.

Winterdyk, J. & Thompson, N. (2008). Student and Non-Student Perceptions and Awareness of Identity Theft. *Canadian Journal of Criminology and Criminal Justice*, 50(2), 153-186.

Bijlagen

1 Respondenten slachtofferenquête

De onderstaande tabel geeft de verschillen weer tussen de kenmerken van de respondenten in het LISS-panel en de kenmerken van de Nederlandse bevolking, gemeten door het CBS. Deze vergelijking is gemaakt voor beide perioden.

Tabel B1.1: Respondenten LISS-panel vergeleken met Nederlandse bevolking, in procenten

	LISS 2010	CBS 2010	LISS 2012	CBS 2012
Geslacht				
Man	46,3	49,1	46,7	49,2
Vrouw	53,7	50,9	53,3	50,8
Leeftijd				
15 t/m 24 jaar	11,4	14,8	10,1	14,8
25 t/m 34 jaar	12,6	14,6	11,1	14,6
35 t/m 44 jaar	16,2	18,1	15,8	17,1
45 t/m 54 jaar	18,7	18,0	18,8	18,2
55 t/m 64 jaar	21,9	15,8	21,5	15,7
65 jaar en ouder	19,3	18,6	22,8	19,6
Hoogst afgeronde opleiding*				
Basisonderwijs	10,7	Laag: 33,5	9,8	Laag: 33,2
Vmbo	26,6		25,8	
Havo/vwo	10,9	Middel: 39,5	11,1	Middel: 39,3
Mbo	21,7		22,6	
Hbo	21,8	Hoog: 27,0	22,7	Hoog: 27,5
Wo	7,9		8,1	
Mate van stedelijkheid				
Zeer sterk stedelijk	13,8	19,4	12,3	19,6
Sterk stedelijk	26,2	27,9	26,3	27,9
Matig stedelijk	23,1	19,2	23,9	20,2
Weinig stedelijk	21,8	22,4	22,0	21,5
Niet stedelijk	15,0	11,1	15,4	10,7

* Opleidingsniveau is bij het CBS verdeeld in laag, middelbaar en hoog onderwijs. Aangezien in deze studie gebruik wordt gemaakt van meerdere onderwijsniveaus, is ervoor gekozen sommige samen te nemen. Deze samenvoeging komt overeen met de drie categorieën gebruikt bij het CBS. Na samenvoeging komen de percentages uit het LISS-panel uit op de bovenstaande

1. Laag onderwijs: basisonderwijs + vmbo = 37,3% in 2010 en 35,6% in 2012.

2. Middelbaar onderwijs: havo/vwo + mbo = 32,6% in 2010 en 33,7% in 2012.

3. Hoog onderwijs: hbo + wo = 29,7% in 2010 en 30,8% in 2012.

2 Interviews

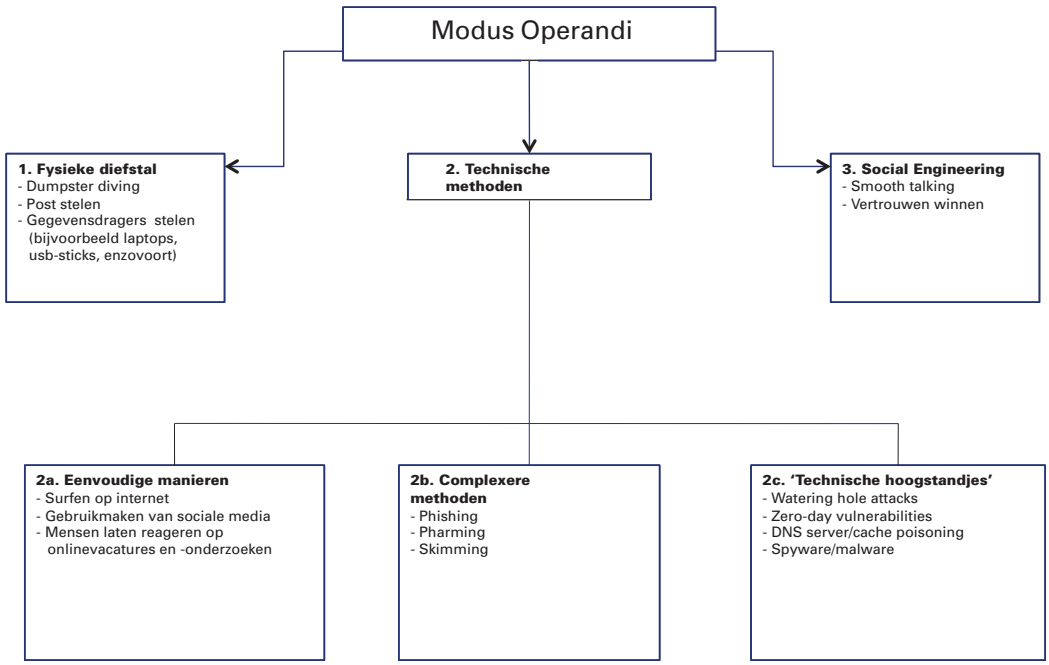
In tabel B2.1 is een overzicht van de interviews weergegeven. In de tabel is de datum van afname vermeld, de organisatie waar de respondent werkzaam is en de functie van de respondent bij die organisatie. Om de anonimiteit van de respondenten te garanderen, zijn hun namen niet in dit overzicht geplaatst.

Tabel B2.1: Overzicht afgenomen interviews: datum, organisatie en functie respondenten

	Datum	Organisatie	Functie respondent(en)
1	07-05-2014	Pilotinterview bij Landelijke Eenheid	Hoofd Landelijke Eenheid
2	13-05-2014	Centraal Meldpunt Identiteitsfraude	senior medewerker CMI
3	14-05-2014	Nederlandse Vereniging van Banken	afdelingshoofd afdeling criminaliteitsbestrijding
4	21-05-2014	Skimmingpoint	unithoofd Recherche Expertise, waar Skimmingpoint onder valt
5	22-05-2014	Electronic Crime Taskforce	teamleider
6	26-05-2014	Business Forensics	managing partner
7	27-05-2014	Electronic Crime Taskforce	teamleider
8	02-06-2014	Fraudehelpdesk	fraude-expert
9	04-06-2014	Expertisecentrum Identiteitsfraude en Documenten	leidinggevende team ECID
10	04-06-2014	Europol (EC3 (3 respondenten))	teamleider EC3 strategisch analist strategisch analist
11	06-06-2014	Team Identiteitsfraude	documentonderzoeker en -trainer adviseur Nationale Politie

Tijdens de interviews is de respondenten een schema voorgelegd waarin de modus operandi van identiteitsfraude op basis van de literatuur uiteen worden gezet (zie figuur B2.1).

Figuur B2.1: Schema modus operandi



Hierna worden de vragen weergegeven die tijdens de interviews zijn gesteld. De vragen zijn geordend per onderwerp en er zijn hoofd- en bijvragen te onderscheiden. Tijdens het interview is telkens bepaald welke vragen geschikt waren om aan de respondenten te stellen.

Introductie

Ten eerste hartelijk dank voor uw medewerking. Ik zal beginnen met mezelf even voor te stellen en het onderzoek van mij en mijn collega toe te lichten. Ik ben Levy Paulissen en in augustus 2013 ben ik afgestudeerd in de Forensische Criminologie. Voor mijn stage heb ik onderzoek gedaan naar de sociale kenmerken van hackers bij Team High Tech Crime van de Landelijke Recherche. Na mijn afstuderen, ben ik door Johan van Wilsem, mijn huidige begeleider, gevraagd voor dit project. We voeren dit onderzoek uit in opdracht van Politie en Wetenschap en zijn in februari 2014 van start gegaan. Met ons onderzoek richten we ons op de aard, omvang en modus operandi van identiteitsfraude. Ook kijken we naar de schade en de risicofactoren van dit delict. We proberen dus een compleet overzicht te geven,

omdat dat tot nu toe in de literatuur ontbreekt. Onze onderzoeksvragen worden beantwoord door het analyseren van representatieve slachtofferenquêtes van het LISS-panel (Langlopende Internet Studies voor de Sociale wetenschappen). Aangezien de slachtoffers van identiteitsfraude vaak zelf niet veel weten over de modus operandi die tegen hen is gebruikt, willen we voor dit onderwerp experts van verschillende organisaties interviewen. De vragen zullen zich dus voornamelijk richten op de modus operandi en de ontwikkelingen op dit gebied. Het interview zal ongeveer anderhalf uur in beslag nemen.

Verder wil ik graag vermelden dat het interview anoniem is. Uw naam zal dus niet genoemd worden in het uiteindelijke rapport. Daarnaast zal de informatie in het rapport niet naar u herleidbaar zijn. Geeft u wel toestemming de naam van de organisatie te noemen in het rapport?

Ik zou het gesprek graag willen opnemen met een voicerecorder, geeft u hier toestemming voor? Zo nee, wat is de reden hiervoor?

Mocht u geen antwoord willen of kunnen geven op bepaalde vragen – bijvoorbeeld omdat het buiten uw expertisegebied ligt of vanwege vertrouwelijkheid – dan kunt u dit uiteraard aangeven. Ook kunt u aangeven wanneer u wel vermoedens heeft van bepaalde zaken of ontwikkelingen, maar het niet zeker weet.

Heeft u zelf nog vragen of opmerkingen voordat we van start gaan?

1 Algemene vragen

Ik ga eerst beginnen met het stellen van wat algemene vragen.

- Zou u wat kunnen vertellen over uw achtergrond en loopbaan?
- Wat is uw functie binnen de organisatie?
- Zou u wat kunnen vertellen over hoe uw organisatie zich bezighoudt met identiteitsfraude en/of identiteitsdiefstal?
  - Is dit preventief of repressief?
  - Is dit dader- of slachtoffergericht?
  - Met welke andere organisaties werkt u samen om het probleem van identiteitsfraude aan te pakken?
- Hoe wordt identiteitsfraude binnen uw organisatie gedefinieerd?

Ons onderzoek richt zich op onrechtmatige bankafschrijvingen, misbruik van creditcards en misbruik van persoonlijke informatie voor frauduleuze doeleinden. Vooral onrechtmatige bankafschrijvingen en misbruik van creditcards zien wij terug in ons onderzoek.

- Welke vorm of vormen van identiteitsfraude komt u het meest tegen in uw werk?
  - Houdt uw organisatie zich ook bezig met documentfraude? **Zo ja, ga door naar de derde vraag onder het volgende kopje, zo nee, sla de volgende vier vragen over.**

Vragen voor ECID en Team Identiteitsfraude:

- U krijgt voornamelijk te maken met documentfraude, wat valt hier allemaal onder (of wat valt hier niet onder)?
- Besteedt uw organisatie ook aandacht aan de digitale component van identiteitsfraude en zo ja, op welke manier?
- Uit cijfers van de Koninklijke Marechaussee (2012) blijkt dat fraude met documenten aan het stijgen is. Wat kunt u hierover vertellen?
  - Is er sprake van een stijging van een bepaalde methode om documentfraude mee te plegen?

2 *Methoden identiteitsfraude*

Dan ga ik nu verder met wat inleidende vragen over de modus operandi van identiteitsfraude. Kijkend naar de literatuur, zijn er eigenlijk een paar clusters te onderscheiden in de modus operandi (extra bijlage uitdelen). Ten eerste zijn er de plegers die de informatie op een **(a) fysieke manier** stelen, bijvoorbeeld via dumpster diving. Daarnaast is **(b) social engineering** een aparte techniek die vaak wordt ingezet, zeker om informatie bij organisaties los te krijgen. De derde cluster betreft diefstal met behulp van **(c) digitale/technische middelen**. Hier zijn ook nog een aantal categorieën in te onderscheiden. Ten eerste is de makkelijkste manier om via internet op zoek te gaan naar informatie, bijvoorbeeld op sociale-netwerksites. Andere, wat moeilijker manieren, die daarnaast vaak worden gebruikt, zijn phishing, pharming en skimming. Ten derde zijn er de manieren die echt onder de technische hoogstandjes vallen. Dit zijn de meer ingewikkelde hacks. Zero-day vulnerabilities en watering-hole attacks zijn hier voorbeelden van.

- Ziet u deze indeling ook terug in de praktijk?
  - Zo nee, wat ziet u dan wel terug?
  - Zijn er nog methoden die in deze indeling ontbreken?
  - Welke methode is naar uw idee op dit moment het meest populair onder de plegers van identiteitsfraude en waarom?
  - Hoe vaak wordt deze methode gebruikt in tegenstelling tot andere methoden?
- Zijn er methoden die minder of niet meer worden gebruikt en zo ja, welke methoden zijn dit?
  - Waarom worden deze methoden niet meer gebruikt door de plegers?
- Wat komt in de praktijk het meest voor, de lowtech methoden, of de meer complexe, hightech methoden?
  - Komt het ook gecombineerd voor?
  - Als er op dit gebied een bepaalde ontwikkeling is waar te nemen is, hoe ziet die ontwikkeling er dan uit?

Ik zou graag nog even terug willen komen op de meest technische methoden om identiteitsfraude mee te plegen. In de sociaalwetenschappelijke literatuur wordt aan technische hoogstandjes weinig aandacht besteed en wanneer een artikel hier wel op ingaat, is de uitleg vaak ingewikkeld. Daarom hebben we een paar methoden op een rijtje gezet, waarvan we graag kort zouden willen weten hoe deze uitgevoerd worden. Het is uiteraard geen probleem als u geen antwoord heeft op deze vragen.

- Hoe werken watering-hole attacks en hoe worden deze ingezet om identiteitsfraude te plegen?
- Wat zijn zero-day vulnerabilities en hoe worden deze ingezet om identiteitsfraude te plegen?
- Wat is Domain Name System Poisoning en hoe kunnen plegers deze methode gebruiken om identiteitsfraude te plegen?
- Wat is Domain Name System Cache Poisoning en hoe kan deze methode worden ingezet om identiteitsfraude te plegen?
- Wat is het verschil tussen spyware en malware en hoe worden deze middelen ingezet om identiteitsfraude te plegen?
- Missen we in dit rijtje nog een belangrijke technische methode die vaak gebruikt wordt, maar nu niet behandeld is?

Het is algemeen bekend dat identiteitsfraude een tweefasedelict is. De eerste stap is om de informatie te stelen en de tweede stap is om met die informatie fraude te plegen.

- In hoeverre denkt u dat identiteitsfraude een delict is waarbij één persoon de informatie steelt en met die informatie ook fraudeert?
  - Is het zo dat bij eenvoudige manieren van diefstal vaak alleen wordt gehandeld en bij meer technisch ingewikkelde manieren samen?

Er bestaan speciale netwerken, zogenaamde carder networks, die vraag en aanbod in persoonlijke informatie faciliteren. Deze netwerken worden bezocht door kopers, verkopers en tussenpersonen die geïnteresseerd zijn in persoonlijke informatie. Op deze netwerken kunnen geïnteresseerden ook anderen zoeken om mee samen te werken, mee te praten en tips mee uit te wisselen.

- Zou u voor me kunnen beschrijven hoe belangrijk deze netwerken zijn voor plegers van identiteitsfraude?
- Wanneer er wordt samengewerkt, is er dan sprake van een bepaalde taakverdeling en zo ja, hoe ziet die taakverdeling er dan meestal uit?
  - Wanneer er sprake is van verschillende personen die stelen en frauderen, wie zijn de identiteitsdieven en wie zijn de identiteitsfraudeurs (bijvoorbeeld hackers stelen en anderen frauderen)?
- Zijn het vaste groepen die samen identiteitsfraude plegen of is het contact vluchtig?
- Is er op het gebied van samenwerking sprake van een ontwikkeling en zo ja, kunt u die ontwikkeling dan voor me beschrijven?
- In hoeverre is identiteitsfraude een delict dat plaatsvindt binnen de landgrenzen?
  - Als het een transnationaal delict betreft, op welke manier wordt er dan vaak samengewerkt?
  - Is er een ontwikkeling waar te nemen op het gebied van internationale samenwerking en zo ja, hoe ziet die ontwikkeling er uit?

De voorgaande vragen richtten zich vooral op het stelen van informatie. De tweede stap bij identiteitsfraude is het frauderen met de informatie.

- Hoe frauderen plegers met de gegevens?
  - Hoe maken ze winst?

  - Hoe wordt er omgegaan met een grote hoeveelheid aan persoonlijke informatie? Als iemand bijvoorbeeld honderden creditcardnummers heeft gestolen, wat doet hij er dan daarna mee?
  - Kan hij in één keer al die nummers misbruiken, of verkoopt hij ze per stuk?
- In hoeverre hangt de manier van fraude plegen samen met de modus operandi?

3 *Literatuur versus praktijk*

In de volgende vragen noem ik wat ontwikkelingen die zich volgens de literatuur voor zouden doen in Nederland. Ik zou graag willen weten of deze ontwikkelingen overeenkomen met de praktijk die u ziet in Nederland.

Uit onderzoek is gebleken dat skimming een van de meest gebruikte methoden is om identiteitsfraude te plegen. Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (2012) stelt echter dat schade van identiteitsfraude aan het afnemen is, omdat skimming minder vaak voorkomt.

- Wat is uw mening hierover?
- Onderzoek van PricewaterhouseCoopers (2013) stelt dat ook phishing als gebruikte methode aan het afnemen is. Hoe denkt u hierover?
- Is het dan zo dat de methode echt minder gebruikt wordt, of dat er meer ingewikkelde technieken voor in de plaats komen, die gebaseerd zijn op die methode? **Voorbeeld: pharming en spear-phishing zijn meer complexe methoden die zijn gebaseerd op phishing.**
- Hoe groot is de rol van sociale-netwerksites als we spreken over identiteitsfraude?
  - Hoe wordt identiteitsfraude via sociale-netwerksites precies gepleegd?
  - Zijn er sociale-netwerksites die vaker het doelwit zijn van daders dan andere sociale-netwerksites en zo ja, welke zijn dit dan?
  - De laatste tijd is steeds meer in het nieuws dat onbeschermde wifi-netwerken een ideale bron zijn voor plegers van identiteitsfraude, wanneer ze op zoek zijn naar persoonlijke informatie. Ziet u dit ook terug in de praktijk?

4 Overige ontwikkelingen op het gebied van identiteitsfraude

Dan zijn we nu aangekomen bij het laatste deel van het interview. In dit deel wil ik graag aandacht besteden aan overige factoren die met identiteitsfraude samenhangen. Daarnaast zal ik ook wat vragen stellen over ontwikkelingen op het gebied van identiteitsfraude.

Uit de eerste resultaten van ons onderzoek blijkt dat bepaalde risicovolle gedragingen op internet (bijvoorbeeld downloaden, chatten enzovoort) slachtofferschap van identiteitsfraude niet goed voorspellen. Dit zou dus kunnen betekenen dat het misschien niet aan het slachtoffer zelf ligt dat zijn of haar identiteit wordt gestolen, maar dat bijvoorbeeld organisaties hiervoor 'verantwoordelijk' zijn. De informatie komt dan beschikbaar na een datalek, in plaats van dat het slachtoffer zelf onvoorzichtig is geweest.

- Wat is uw mening hierover?
  - Ziet u hier een bepaalde verschuiving in (bijvoorbeeld van individu naar organisatie) en zo ja, hoe ziet die verschuiving eruit?
  - Wat is de rol van medewerkers van organisaties als we praten over identiteitsfraude voorkomen, maar misschien ook wel over plegen?
- Kunt u omschrijven welke ontwikkelingen, die we nog niet hebben besproken, in de loop der jaren hebben plaatsgevonden?
- Kunt u een voorspelling doen over de toekomst? Waar gaan we naartoe?
- Heeft u zelf nog iets toe te voegen? Ben ik bijvoorbeeld iets belangrijks vergeten waar u graag nog wat meer over vertelt?

Dan zijn we nu aan het einde gekomen van het interview. Ik zou u graag nogmaals hartelijk willen bedanken voor uw medewerking. Nogmaals, we gaan zorgvuldig om met deze gegevens. Zou ik voor eventuele vragen naar aanleiding van dit interview nog contact met u mogen opnemen?

3 Analyses achtergrondkenmerken en (online)activiteiten

In tabellen B.3.1 tot en met B3.5 zijn de resultaten te vinden van de correlatie-analyse en de logistische regressieanalyse uitgevoerd met de achtergrondkenmerken, kenmerken en online activiteiten van de respondenten gerelateerd aan slachtofferschap.

Tabel B3.1: Spearman rangcorrelatietabel, gedragingen, activiteiten op het internet en slachtofferschap van bankfraude, creditcardfraude en overige fraude in de perioden 2008- 2010 en 2010- 2012

	Bankfraude		Creditcardfraude		Overige fraude	
	2010	2012	2010	2012	2010	2012
Gedragingen:						
Lage zelfcontrole	.041**	.021	-.009	.022	.024	.049**
Onlineactiviteiten:						
Internetenquêtes	.038**	.037**	.015	.046**	.008	.014
Webcam	.026	.020	.040**	.033*	.005	.032*
Controle virussen	.004	.001	.030*	.039*	-.009	-.014
Creditcardgebruik	.047**	.015	.092**	.085**	-.017	-.008
Uur per week online:						
E-mail	.026*	.033*	.031*	.006	.005	-.014
Informatie zoeken	.017	.009	.020	.001	-.008	-.022
Producten vergelijken	.039**	.004	.034*	.015	.011	-.014
Producten kopen	.032*	.003	.029*	.018	.002	-.003
Korte films kijken	.013	.010	.027*	.038**	.015	.022
Tv of films kijken	.004		.012		.015	
Downloaden software	.041**		.026		.022	
Downloaden film en muziek	.016		.004		.026*	
Downloaden (2012)		-.008		.044**		.027
Gokken	.007		.017		.046**	
Internetbankieren	.045**	.024	.005	.010	.006	.004
Gamen	-.015	-.009	-.010	-.021	.016	.003
Lezen nieuwssites	.019	.012	.035**	.013	-.006	.018
Bezoeken nieuwsgroepen	.039**	.012	.008	.024	.024	.043**
Chatten	.008	-.010	-.002	.023	.017	.040**
Fora bezoeken	.017	.005	.031*	.022	-.001	.009
Overige bezigheden	.024	.015	.020	.015	.003	.012
Sociale media (2012)		-.005		.006		.001
Bloggen (2012)		-.001		.028*		.047**
Skype (2012)		.003		.029*		.042**
Twitter (2012)		-.001		.044**		.025
Datingsites (2012)		-.019		-.006		.010
Sociale media:						
Aantal sites	.046**	.021	.030*	.026	.025*	.013
Achternaam	.041**	.018	.036*	.015	.015	.012
Leeftijd	.048**	.014	.037*	.013	.008	.005
Adres	.061**	.018	-.005	-.009	-.014	-.009
Telefoonnummer	.037**	.019	.017	.000	.023	-.010
E-mailadres	.037**	.015	.026*	.022	.018	-.008
Foto's	.037**	.013	.033**	.015	.019	.012
Preventief:						
Firewall	.028*	.045**	.026*	.049**	.004	-.013
Virusscanner	.041**	.022	.032*	.042**	.003	-.016
Antispy-software	.034*	.029*	.035**	.050**	-.009	.000
Trojanscanner	.010	.018	.033**	.061**	.004	.008
Spamfilter	.030*	.032*	.045**	.051**	-.013	-.013
Beveiliging wifi	.029*	.036**	.031*	.062*	.009	-.006
Computeronwetendheid	.028*	.040**	.038**	.053**	-.003	.006

* = $p<.05$; ** = $p<.01$

Tabel B3.2: Logistische regressieanalyse bankfraude 2010

	Model 1		Model 2		Model 3		Model 4		Model 5	
	B	s.e.	B	s.e.	B	s.e.	B	s.e.	B	s.e.
Constante	-3.338	.745	-4.378	.856	-4.362	.869	-4.467	.907	-4.447	.945
Vrouw	-.232	.151	-.162	.155	-.172	.157	-.090	.166	-.162	.171
Leeftijd	-.034	.048	.031	.054	.036	.060	.011	.064	-.001	.065
Stedelijk	-.157**	.060	-.158*	.062	-.176	.063	-.170**	.064	-.169**	.064
Inkomen	-.035	.049	-.049	.052	-.047	.051	-.044	.051	-.043	.051
Opleiding	.125*	.051	.042	.054	.050	.055	.065	.057	.074	.057
Alleenstaand	-.275	.187	-.235	.193	-.220	.195	-.223	.196	-.211	.197
Lage zelfcontrole	.746	.430	.746	.452	.738	.455	.752	.466	.700	.470
Online enquêtes			.095	.065	.091	.065	.091	.066	.091	.066
Controle virussen			-.009	.060	-.012	.060	-.033	.061	.004	.065
Creditcardgebruik			.241	.169	.228	.171	.245	.175	.275	.176
iDEAL			.281*	.124	.285	.126	.240	.132	.284*	.134
Webcam			.027	.194	.006	.201	.031	.208	.047	.209
Aantal sociale netwerksites					-.017	.119	.017	.122	.026	.123
Achternaam					-.429	.319	-.403	.322	-.396	.324
Leeftijd					.324	.345	.293	.349	.293	.350
Adres					1.196	.326	1.182**	.328	1.170**	.329
Telefoonnummer					-.485	.351	-.471	.356	-.475	.356
E-mailadres					-.364	.268	-.360	.269	-.358	.270
Foto's					.247	.285	.210	.288	.203	.288
Aantal uur per week:										
E-mail							-.030	.019	-.030	.019
Informatie zoeken							-.038	.032	-.039	.031
Vergelijken producten							.077	.053	.082	.053
Kopen producten							.052	.126	.053	.126
Korte filmpjes kijken							.043	.085	.037	.085
Tv en films kijken							-.056	.094	-.059	.094
Downloaden software							.029	.118	.038	.119
Downloaden muziek en films							.001	.065	.009	.065
Gokken							.225	.553	.188	.554
Internetbankieren							.187*	.085	.185*	.085
Gamen							-026	.043	-.022	.043
Nieuws lezen							.042	.053	.045	.053
Bezoeken nieuwsgroepen							.195	.108	.192	.108
Chatten							-.016	.035	-.014	.035
Fora							-.142	.087	-.129	.086
Overige activiteiten							.006	.045	.003	.045
Preventief:										
Firewall									-.281	.220
Virusscan									.040	.280
Antispy									.132	.210
Trojanscanner									-.290	.214
Spamfilter									.024	.204
Wifi-beveiliging									-.030	.180
Computeronwetendheid									.026	.054
Nagelkerke R^2	.019		.025		.038		.054		.059	
Df	7		12		19		35		42	

* $p < .05$; ** $p < .01$

Tabel B3.3: Logistische regressieanalyse bankfraude 2012

	Model 1		Model 2		Model 3		Model 4		Model 5	
	B	s.e.	B	s.e.	B	s.e.	B	s.e.	B	s.e.
Constante	-3.950	.745	-5.160	.873	-5.010	.882	-4.981	.903	-4.996	.936
Vrouw	-.052	.150	.036	.154	.049	.155	.054	.161	.081	.164
Leeftijd	-.032	.048	.040	.053	.000	.060	-.018	.063	-.013	.063
Stedelijk	-.093	.060	-.088	.061	-.092	.062	-.097	.062	-.094	.062
Inkomen	-.017	.045	-.019	.047	-.019	.047	-.023	.047	-.022	.048
Opleiding	.128*	.051	.056	.055	.057	.055	.056	.056	.052	.057
Alleenstaand	-.142	.197	-.101	.203	-.113	.204	-.167	.206	-.163	.207
Lage zelfcontrole	.753	.424	.727	.442	.763	.447	.840	.453	.862	.455
Online enquêtes			.172**	.065	.174**	.065	.176**	.065	.180**	.065
Controle virussen			.000	.062	.005	.062	.009	.063	.010	.067
Creditcardgebruik			-.039	.168	-.018	.169	-.029	.173	-.047	.174
iDEAL			.268*	.127	.290*	.128	.307*	.133	.297*	.135
Webcam			.181	.176	.202	.179	.227	.191	.220	.192
Aantal sociale netwerksites					.068	.099	.104	.102	.101	.103
Achternaam					.011	.319	-.055	.323	-.061	.327
Leeftijd					-.185	.296	-.170	.298	-.161	.299
Adres					.299	.329	.313	.330	.301	.330
Telefoonnummer					-.089	.334	-.076	.336	-.074	.335
E-mailadres					-.160	.255	-.146	.257	-.152	.258
Foto's					-.209	.278	-.173	.280	-.175	.280
Aantal uur per week:										
E-mail							.010	.014	.010	.014
Informatie zoeken							-.057	.037	-.057	.037
Vergelijken producten							.038	.065	.041	.066
Kopen producten							-.072	.123	-.075	.124
Korte filmpjes kijken							-.009	.051	-.010	.052
Downloaden							-.076	.059	-.075	.060
Internetbankieren							.044	.078	.042	.078
Gamen							.012	.025	.012	.025
Nieuws lezen							.033	.049	.031	.050
Bezoeken nieuwsgroepen							.099	.070	.097	.070
Chatten							.020	.026	.021	.026
Fora							.019	.049	.015	.049
Sociale media							-.029	.033	-.028	.033
Bloggen							-.101	.122	-.112	.123
Skype							-.024	.073	-.025	.074
Twitter							.005	.037	.004	.037
Datingsites							-1.113	.677	-1.114	.678
Overige activiteiten							.030	.025	.031	.025
Preventief:										
Firewall									.433	.235
Virusscan									-.478	.260
Antispy									-.002	.217
Trojanscanner									-.093	.212
Spamfilter									.057	.209
Wifi-beveiliging									.082	.197
Computeronwetendheid									-.002	.053
Nagelkerke R^2	.010		.018		.021		.032		.037	
Df	7		12		19		37		44	

* $p < .05$; ** $p < .01$

Tabel B3.4: Logistische regressieanalyse creditcardfraude 2010

	Model 1		Model 2		Model 3		Model 4		Model 5	
	B	s.e.	B	s.e.	B	s.e.	B	s.e.	B	s.e.
Constante	-3.332	1.613	-6.349	1.882	-6.552	1.919	-7.052	2.007	-6.533	2.089
Vrouw	-.984**	.323	-.758*	.325	-.813*	.330	-.769*	.343	-.806*	.354
Leeftijd	-.125	.097	-.142	.109	-.109	.122	-.053	.133	-.080	.135
Stedelijk	-.066	.118	-.003	.120	-.015	.121	-.016	.122	-.015	.122
Inkomen	.050	.087	.022	.094	.015	.095	.016	.097	.024	.097
Opleiding	.361**	.109	.180	.112	.192	.114	.222	.120	.221	.119
Alleenstaand	-.431	.363	-.390	.367	-.384	.372	-.372	.383	-.376	.389
Lage zelfcontrole	-.440	1.049	-.165	1.073	-.209	1.084	-.270	1.098	-.393	1.121
Online enquêtes			-.022	.139	-.023	.140	-.010	.142	-.005	.143
Controle virussen			.154	.130	.151	.132	.145	.135	.157	.144
Creditcardgebruik			1.0968**	.415	1.998**	.417	2.031**	.435	2.022**	.436
iDEAL			-.339	.250	-.331	.255	-.279	.264	-.220	.267
Webcam			.418	.336	.468	.347	.394	.366	.388	.367
Aantal sociale netwerksites					-.306	.251	-.388	.258	-.385	.256
Achternaam					.207	.615	.175	.634	.175	.645
Leeftijd					.795	.640	.886	.649	.894	.665
Adres					-1.306	.780	-1.328	.802	-1.393	.809
Telefoonnummer					.426	.656	.478	.671	.494	.674
E-mailadres					-.310	.453	-.323	.465	-.275	.468
Foto's					.197	.506	.189	.514	.166	.522
Aantal uur per week:										
E-mail							-.014	.029	-.018	.029
Informatie zoeken							-.030	.057	-.031	.058
Vergelijken producten							.164	.092	.173	.092
Kopen producten							-.092	.274	-.121	.278
Korte filmpjes kijken							.187	.151	.178	.152
Tv en films kijken							-.032	.184	-.039	.189
Downloaden software							.146	.242	.167	.247
Downloaden muziek en films							-.291	.199	-.304	.203
Gokken							1.016	.812	1.000	.828
Internetbankieren							-.433	.238	-.435	.238
Gamen							-.023	.091	-.014	.092
Nieuws lezen							.118	.091	.120	.091
Bezoeken nieuwsgroepen							-.136	.253	-.158	.258
Chatten							.061	.058	.064	.058
Fora							.047	.116	.057	.116
Overige activiteiten							.049	.072	.048	.072
Preventief:										
Firewall									-.794	.420
Virusscan									-.069	.580
Antispy									-.007	.422
Trojanscanner									.006	.389
Spamfilter									.577	.440
Wifi-beveiliging									-.158	.340
Computeronwetendheid									-.102	.124
Nagelkerke R^2	.056		.114		.129		.160		.171	
Df	7		12		19		35		42	

* $p < .05$; ** $p < .01$

Tabel B3.5: Logistische regressieanalyse creditcardfraude 2012

	Model 1		Model 2		Model 3		Model 4		Model 5	
	B	s.e.	B	s.e.	B	s.e.	B	s.e.	B	s.e.
Constante	-6.313	1.321	-11.213	1.660	-11.056	1.668	-11.889	1.772	-12.002	1.831
Vrouw	-.659*	.285	-.366	.292	-.384	.295	-.243	.309	-.097	.322
Leeftijd	-.098	.089	-.108	.101	-.208	.115	-.184	.121	-.134	.124
Stedelijk	.096	.108	.136	.111	.134	.111	.160	.114	.167	.116
Inkomen	-.158	.107	-.194	.121	-.190	.119	-.201	.124	-.205	.128
Opleiding	.483**	.108	.341**	.111	.359**	.113	.397**	.118	.386**	.118
Alleenstaand	-.326	.349	-.359	.359	-.402	.363	-.468	.380	-.554	.386
Lage zelfcontrole	1.567*	.698	1.894**	.716	2.035**	.724	2.006**	.748	2.129**	.758
Online enquêtes			.286*	.115	.301*	.115	.347**	.119	.343**	.120
Controle virussen			.348*	.137	.350	.137	.383**	.138	.342*	.146
Creditcardgebruik			1.316**	.347	1.371**	.348	1.557**	.364	1.520**	.369
iDEAL			.201	.240	.295	.242	.263	.253	.202	.257
Webcam			.296	.295	.407	.303	.538	.327	.469	.331
Aantal sociale netwerksites					.007	.169	-.005	.178	-.012	.177
Achternaam					-.184	.562	-.100	.581	-.129	.595
Leeftijd					-.154	.493	-.049	.507	.007	.520
Adres					-.734	.670	-.798	.700	-.786	.703
Telefoonnummer					-.147	.587	-.070	.618	-.098	.622
E-mailadres					.115	.451	.075	.453	.036	.460
Foto's					-.328	.480	-.221	.487	-.212	.491
Aantal uur per week:										
E-mail							-.054	.033	-.054	.033
Informatie zoeken							-.038	.062	-.038	.064
Vergelijken producten							-.011	.128	-.011	.130
Kopen producten							.092	.229	.083	.234
Korte filmpjes kijken							.209**	.065	.216**	.065
Downloaden							-.049	.098	-.061	.102
Internetbankieren							-.093	.201	-.078	.203
Gamen							-.071	.077	-.069	.077
Nieuws lezen							-.081	.101	-.096	.102
Bezoeken							-.077	.158	-.064	.162
nieuwsgroepen										
Chatten							-.023	.084	-.007	.081
Fora							.063	.086	.049	.086
Sociale media							-.093	.068	-.094	.069
Bloggen							.052	.173	.032	.178
Skype							-.098	.141	-.115	.148
Twitter							.044	.062	.049	.062
Datingsites							-.783	.925	-.702	.932
Overige activiteiten							.055	.035	.051	.035
Preventief:										
Firewall									-.173	.459
Virusscan									-.400	.582
Antispy									-.324	.419
Trojanscanner									.548	.377
Spamfilter									.149	.416
Wifi-beveiliging									.694	.440
Computeronwetendheid									-.103	.133
Nagelkerke R^2	.064		.129		.142		.176		.189	
Df	7		12		19		37		44	

* $p < .05$; ** $p < .01$

Leden Redactieraad Programma Politie & Wetenschap

Secretariaat
Programmabureau Politie & Wetenschap
Politieacademie
Arnhemseweg 348
7334 AC Apeldoorn

Postbus 834
7301 BB Apeldoorn
www.politieenwetenschap.nl

Uitgaven in de reeks Politiewetenschap

1. ***Kerntaken van de politie. Een inventarisatie van heersende opvattingen***
   C.D. van der Vijver, A.J. Meershoek & D.F. Slobbe, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2001
2. ***Bevoegdheden overd(r)acht. Een onderzoek naar delegatie en mandaat van beheersbevoegdheden in de politiepraktijk***
   H.B. Winter & N. Struiksma, Pro Facto B.V., Universiteit Groningen, 2002
3. ***Sturing van politie en politiewerk. Een verkennend onderzoek tegen de achtergrond van een veranderende sturingscontext en sturingsstijl***
   J. Terpstra, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2002
4. ***Woninginbrekers en zware jongens. Daders vanuit het voormalig Joegoslavië aan het woord***
   M. van San, E. Snel & R. Boers, Risbo, Erasmus Universiteit Rotterdam, 2002
5. ***Zeg me wie je vrienden zijn. Allochtone jongeren en criminaliteit***
   F.M.H.M. Driessen, B.G.M. Völker, H.M. Op den Kamp, A.M.C. Roest & R.J.M. Molenaar, Bureau Driessen, Utrecht, 2002
6. ***Op deugdelijke grondslag. Een explorerende studie naar private forensische accountancy***
   J. van Wijk, W. Huisman, T. Feuth & H.G. van de Bunt, Vrije Universiteit, Amsterdam, 2002
7. ***Voorbij de dogmatiek. Publiek-private samenwerking in de veiligheidszorg***
   A.B. Hoogenboom & E.R. Muller, COT, Den Haag, 2003
8. ***Hennepteelt in Nederland. Het probleem van de criminaliteit en haar bestrijding***
   F. Bovenkerk, W.I.M. Hogewind, D. Korf & N. Milani, Willem Pompe Instituut, Universiteit Utrecht, 2003
9. ***Politiekennis in ontwikkeling. Een onderzoek naar het verzamelen en veredelen van informatie voor het Politie Kennis Net***
   I. Bakker & C.D. van der Vijver, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2003

10a. ***Politie en geweld. Een verkenning van politiereacties op geweldsincidenten in vier Nederlandse regiokorpsen***
   C.J.E. In 't Velt, W.Ph. Stol, P.P.H.M. Klerks, H.K.B. Fobler, R.J. van Treeck & M. de Vries, NPA-Politie Onderwijs- en Kenniscentrum, LSOP, Apeldoorn, 2003

10b. ***Geweldige informatie? Onderzoek naar de informatiehuishouding van geweldsmeldingen bij de politie***
   R. van Overbeeke, O. Nauta, A. Beerepoot, S. Flight & M. Rietveld, DSP-groep, Amsterdam, 2003

11. ***Blauwe Bazen. Het leiderschap van korpschefs***
    R.A. Boin, P. 't Hart & E.J. van der Torre, Departement Bestuurskunde, Universiteit Leiden/COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2003
12. ***Over de grens. Een verkenning van projecten voor probleemjeugd in Duitsland, Engeland en Zweden***
    I. van Leiden, G. Verhagen & H.B. Ferwerda, Advies- en Onderzoeksgroep Beke, Arnhem, 2003
13. ***Integriteit in het dagelijkse politiewerk. Meningen en ervaringen van politiemensen***
    J. Naeyé, L.W.J.C Huberts, C. van Zweden, V. Busato & B. Berger, Centrum voor Politiewetenschappen, VU Amsterdam, 2004
14. ***Politiestraatwerk in Nederland. Noodhulp en gebiedswerk: inhoud, samenhang, verandering en sturing***
    W. Ph. Stol, A.Ph. van Wijk, G. Vogel, B. Foederer & L. van Heel, Nederlandse Politieacademie, Onderzoeksgroep, LSOP, Apeldoorn, 2004
15. ***De kern van de taak. Kerncompetenties van de politie als criterium voor de afbakening van kerntaken in de praktijk***
    A. Mein, A. Schutte & A. van Sluis, ES&E, Den Haag, 2004
16. ***Professionele dienstverlening en georganiseerde criminaliteit. Hedendaagse integriteitsdilemma's van advocaten en notarissen***
    F. Lankhorst & J.M. Nelen, Vrije Universiteit Amsterdam, Faculteit der Rechtsgeleerdheid, Sectie Criminologie, Amsterdam, 2004
17. ***Paradoxaal Politiebestel. Burgemeesters, Openbaar Ministerie en Politiechefs over de sturing van de politie***
    L.W.J.C. Huberts, S. Verberk, K. Lasthuizen & J.H.J. van den Heuvel, Vrije Universiteit Amsterdam/B&A Groep, 's-Gravenhage, 2004
18. ***Illegale vuurwapens in Nederland: smokkel en handel***
    A.C. Spapens & M.Y. Bruinsma, IVA, Tilburg, 2004
19. ***Samenwerking en netwerken in de lokale veiligheidszorg***
    J. Terpstra & R. Kouwenhoven, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2004
20. ***Uit balans: politie en bestel in de knel. State-of-the-art: bundeling van kennis en inzicht***
    H.G. van de Bunt, A.B. Hoogenboom, LW.J.C. Huberts, E.R Muller, J. Terpstra, C.D. van der Vijver & C. Wiebrens, 2004
    Redactie: G.C.K. Vlek, C. Bangma, C. Loef & E.R. Muller
21. ***Politie en media. Feiten, fictie en imagopolitiek***
    H. Beunders & E.R. Muller, Erasmus Universiteit Rotterdam/COT, Instituut voor Veiligheids- en Crisismanagement, Leiden, 2005 (2e druk 2009)

22. ***Integriteit van de politie. State-of-the-art: wat we weten op basis van Nederlands onderzoek***
L.W.J.C. Huberts & J. Naeyé, Centrum voor Politie- en Veiligheidswetenschappen/Vrije Universiteit, Amsterdam, 2005
23. ***De sociale organisatie van mensensmokkel***
R. Staring, G. Engbersen, H. Moerland, N. de Lange, D. Verburg, E. Vermeulen & A. Weltevrede; m.m.v. E. Heyl, N. Hoek, L. Jacobs, M. Kanis & W. van Vliet, Erasmus Universiteit Rotterdam: Criminologie – Sociologie – Risbo, 2005
24. ***In elkaars verlengde? Publieke en private speurders in Nederland en België***
U. Rosenthal, L. Schaap J.C. van Riessen, P. Ponsaers & A.H.S. Verhage, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag/Universiteit Gent, 2005
25. ***De strafrechtelijke rechtshulpverlening van Nederland aan de lidstaten van de Europese Unie. De politieke discussie, het juridische kader, de landelijke organisatie en de feitelijke werking***
C.J.C.F. Fijnaut, A.C. Spapens & D. van Daele, Universiteit van Tilburg, Vakgroep Strafrechtwetenschappen, 2005
26. ***Niet zonder slag of stoot. De geweldsbevoegdheid en doorzettingskracht van de Nederlandse politie***
J. Naeyé, Faculteit der Rechtsgeleerdheid, Vrije Universiteit Amsterdam, 2005
27. ***Preventief fouilleren. Een analyse van het proces en de externe effecten in tien gemeenten***
E.J. van der Torre & H.B. Ferwerda, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag/Advies- en Onderzoeksgroep Beke, Arnhem, 2005
28. ***Zedenmisdrijven in Nederland. Aangiften- en verdachtenanalyses op basis van HKS-gegevens***
A.Ph. van Wijk, S.R.F. Mali, R.A.R. Bullens, L. Prins & P.P.H.M. Klerks, Politieacademie Onderzoeksgroep, Apeldoorn, Vrije Universiteit Amsterdam. KLPD, 2005
29. ***Groepszedenmisdrijven onder minderjarigen. Een analyse van een Rotterdamse casus***
I. van Leiden & J. Jakobs, Advies- en Onderzoeksgroep Beke, Arnhem, 2005
30. ***Omgaan met conflictsituaties: op zoek naar goede werkwijzen bij de politie***
O. Adang, N. Kop, H.B. Ferwerda, J. Heijnemans, W. Olde Nordkamp, P. de Paauw & K. van Woerkom, Onderzoeksgroep Politieacademie, Apeldoorn/Advies en Onderzoeksgroep Beke, Arnhem, 2006
31. ***De strategische analyse van harddrugsscenes. Hoofdlijnen voor politie en beleid***
E.J. van der Torre, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2006

32a. ***Cijfers en stakeholders. Prestatiesturing en de gevolgen voor de maatschappelijke en politiek-bestuurlijke relaties van de politie***
A. van Sluis, L. Cachet, L. de Jong, C. Nieuwenhuyzen & A. Ringeling, Centre for Local Democracy, Erasmus Universiteit Rotterdam, 2006

32b. *Operationele betrokkenheid. Prestatiesturing en bedrijfsvoering Nederlandse politie*
A.B. Hoogenboom, Nivra-Nyenrode, Breukelen, 2006

32c. *Op prestaties gericht. Over de gevolgen van prestatiesturing en prestatieconvenanten voor sturing en uitvoering van het politiewerk*
M.P.C.M. Jochoms, F. van der Laan, W. Landman, P.S. Nijmeijer & A. Sey, Politieacademie, Apeldoorn/Twynstra Gudde, Amersfoort/Universiteit van Amsterdam, 2006

33. *Het nieuwe bedrijfsmatig denken bij de politie. Analyse van een culturele formatie in ontwikkeling*
J. Terpstra & W. Trommel, IPIT Instituut voor Maatschappelijke Veiligheidsvraagstukken, Universiteit Twente 2006

34. *De legitimiteit van de politie onder druk? Beschouwingen over grondslagen en ontwikkelingen van legitimiteit en legitimiteitstoekenning*
Bundel onder redactie van C.D. van der Vijver & G.C.K. Vlek, IPIT Instituut voor Maatschappelijke Veiligheidsvraagstukken, Universiteit Twente/Politie & Wetenschap, 2006

35. *Naar beginselen van behoorlijke politiezorg*
M.J. Dubelaar, E.R. Muller & C.P.M. Cleiren, Faculteit der Rechtsgeleerdheid, Universteit Leiden, 2006

36a. *Asielmigratie en criminaliteit*
J. de Boom, G. Engbersen & A. Leerkes, Risbo Contractresearch BV/Erasmus Universiteit, Rotterdam, 2006

36b. *Criminaliteitspatronen en criminele carrières van asielzoekers*
M. Althoff & W.J.M. de Haan, m.m.v. S. Miedema, Vakgroep Strafrecht en Criminologie, Faculteit der Rechtsgeleerdheid, Rijksuniversiteit Groningen, 2006

36c. *'Ik probeer alleen maar mijn leven te leven'. Uitgeprocedeerde asielzoekers en criminaliteit*
A. Leerkes, Risbo Contractresearch BV/Erasmus Universiteit, Rotterdam; Amsterdamse School voor Sociaal Wetenschappelijk Onderzoek/Universiteit van Amsterdam, Amsterdam, 2006

37. *Positie en expertise van de allochtone politiemedewerker*
J. Broekhuizen, J. Raven & F.M.H.M. Driessen, Bureau Driessen, Utrecht, 2007

38. *Lokale politiechefs. Het middenkader van de basispolitiezorg*
E. J. van der Torre, COT Instituut voor Veiligheids- en Crisismanagement, Den Haag, 2007

39. *Nog niet verschenen*

40. *Conflict op straat: strijden of mijden? Marokkaanse en Antilliaanse jongeren in interactie met de politie*
N. Kop, Martin Euwema, m.m.v. H.B. Ferwerda, E. Giebels, W. Olde Nordkamp & P. de Paauw, Politieacademie, Apeldoorn, Universiteit Utrecht, 2007

41. *Opsporing onder druk*
C. Liedenbaum & M. Kruijsen, IPIT Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2008

42. *Symbolen van orde en wanorde. Broken windows policing en de bestrijding van overlast en buurtverval*
B. van Stokkom, Centrum voor Ethiek, Radboud Universiteit Nijmegen, 2008

43. *Verkeershandhaving: prestaties leveren, problemen aanpakken*
G. Meershoek & M. Krommendijk, IPIT, Instituut voor maatschappelijke veiligheidsvraagstukken, Universiteit Twente, 2008

44. *De frontlinie van opsporing en handhaving. Stelselmatige bedreigingen door burgers als contrastrategie*
M.J.G. Jacobs, M.Y. Bruinsma & J.W.M.J. van Poppel, IVA Tilburg, 2008

45a. *'Kracht van meer dan geringe betekenis'. Deel A: Politiegeweld in de basispolitiezorg*
R. Bleijendaal, J. Naeyé, P. Chattellon & G. Drenth, Vrije Universiteit, Amsterdam, 2008

45b. *'Kracht van meer dan geringe betekenis'. Deel B: Sturing en toetsing van de politiële gewelds-bevoegdheid*
G. Drenth, J. Naeyé & R. Bleijendaal, Vrije Universiteit, Amsterdam, 2008

45c. *Agressie en geweld tegen politiemensen. Beledigen, bedreigen, tegenwerken en vechten*
J. Naeyé & R. Bleijendaal, Vrije Universiteit, Amsterdam, 2008

45d. *Belediging en bedreiging van politiemensen*
J. Naeyé, m.m.v. M. Bakker & C. Grijsen, Vrije Universiteit Amsterdam, 2009

45e. *Uitgangspunten voor politieoptreden in agressie- en geweldssituaties*
J. Naeyé, Vrije Universiteit Amsterdam, 2010

46. *Wijkagenten en hun dagelijks werk. Een onderzoek naar de uitvoering van gebiedsgebonden politiewerk*
J. Terpstra, 2008

47. *Bijzonder zijn ze allemaal! Vergelijkend onderzoek naar reguliere en bijzondere opsporing*
W. Faber, A.A.A. van Nunen & C. la Roi, Faber Organisatievernieuwing, Oss, 2009

48. *Gouden bergen. Een verkennend onderzoek naar Nigeriaanse 419-fraude: achtergronden, daderkenmerken en aanpak*
Y.M.M. Schoenmakers, E. de Vries Robbé & A.Ph. van Wijk, Politieacademie, Apeldoorn/Bureau Beke, Arnhem, 2009

49. *Het betwiste politiebestel. Een vergelijkend onderzoek naar de ontwikkeling van het politiebestel in Nederland, België, Denemarken, Duitsland, Engeland & Wales*
A. Cachet, A. van Sluis, Th. Jochoms, A. Sey & A. Ringeling, Erasmus Universiteit Rotterdam/Politieacademie, Apeldoorn/Korps landelijke politiediensten, Driebergen, 2009

50. *Leven met bedreiging. Achtergronden bij aangiften van bedreiging van burgers*
B. Bieleman, W.J.M. de Haan, J.A. Nijboer & N. Tromp, Intraval & Rijksuniversiteit Groningen, 2010

51a. *Het publieke belang bij private preventie. Een economische analyse van inbraakpreventiebeleid*
B.A. Vollaard, TILEC/Universiteit van Tilburg, 2009

51b. *Het effect van langdurige opsluiting van veelplegers op de maatschappelijke veiligheid*
B.A. Vollaard, TILEC/Universiteit van Tilburg, 2010

52. *Lokale politiek over politie*
T.B.W.M. van der Torre-Eilert, H. Bergsma & M.J. van Duin, met medewerking van R. Eilert, LokaleZaken, Rotterdam, 2010

53a. *Trainen onder stress. Effecten op de schietvaardigheid van politieambtenaren*
R.R.D. Oudejans, A. Nieuwenhuys & G.P.T. Willemsen, Vrije Universiteit Amsterdam, 2010

53b. *Schieten of niet schieten? Effecten van stress op schietbeslissingen van politieambtenaren*
A. Nieuwenhuys, G.P.T. Willemsen & R.R.D. Oudejans, Vrije Universiteit, Amsterdam, 2012

53c. *Politievaardigheden onder stress. Het optimaliseren van aanhouding en zelfverdediging in de praktijk*
P.G. Renden, A. Nieuwenhuys, G.P.T. Willemsen & R.R.D. Oudejans, Vrije Universiteit, Amsterdam, 2015

53d. *Effectief omgaan met acute stress. Effecten van aanleg en trainingservaring op de schietprestatie onder druk*
A. Landman, A. Nieuwenhuys & R.R.D. Oudejans, Vrije Universiteit, Amsterdam, 2015

54. *Politie en publiek. Een onderzoek naar de communicatievormen tussen burgers en blauw*
H.J.G. Beunders, M.D. Abraham, A.G. van Dijk & A.J.E. van Hoek, DSP-groep, Amsterdam/Erasmus Universiteit, Rotterdam, 2011

55. *Managing collective violence around public events: an international comparison*
O.M.J. Adang with cooperation from: S.E. Bierman, E.B. Brown, J. Dietermann, C. Putz, M. Schreiber, R. van der Wal, J. Zeitner, Police Science & Research Programme, Apeldoorn, 2011

56. *Stads- en regioscan in de grootste Brabantse gemeenten. De achtergronden van onveilige GVI-scores*
B.M.W.A. Beke, E.J. van der Torre, M.J. van Duin, COT, Den Haag; LokaleZaken, Rotterdam & Beke Advies, Arnhem, 2011

57. *De mythe ontrafeld? Wat we weten over een goed politieleiderschap*
W. Landman, M. Brussen & F. van der Laan, Twynstra Gudde, Amersfoort, 2011

58. *Proactief handhaven en gelijk behandelen*
J. Svensson, H. Sollie & S. Saharso, Vakgroep Maatschappelijke Risico's en Veiligheid, Institute of Governance Studies, Universiteit Twente, Enschede, 2011

59a. *De sterkte van de arm: feiten en mythes*
J.H. Haagsma, T.M. Rumke, I. Smits, E. van der Veer & C.J. Wiebrens, Andersson Elffers Felix, Utrecht, 2012

59b. *Blauw, hier en daar. Onderzoek naar de sterkte van de politie in Nederland, België, Denemarken, Engeland & Wales en Nordrhein-Westfalen*
J.H. Haagsma, I. Smits, H. Waarsing & C.J. Wiebrens, Andersson Elffers Felix, Utrecht, 2012

60. *De nachtdienst 'verlicht'*
M.C.M. Gordijn, Rijksuniversiteit Groningen, 2012

61. *Opsporing Verzocht. Een quasi-experimentele studie naar de bijdrage van het programma Opsporing Verzocht aan de oplossing van delicten*
J.G. van Erp, F. van Gastel & H.D. Webbink, Erasmus Universiteit, Rotterdam, 2012

62. *Jeugdige zedendelinquenten en recidive. Een onderzoek bij jeugdige zedendelinquenten naar de voorspellende waarde van psychiatrische stoornissen en psychosociale problemen voor (zeden)recidive*
C. Boonmann, L.M.C. Nauta-Jansen, L.A. 't Hart-Kerkhoffs, Th.A.H. Doreleijers & R.R.J.M. Vermeiren, VUmc De Bascule, Duivendrecht, 2012

63. *Hoe een angsthaas een jokkebrok herkent*
J. Jolij, Rijksuniversiteit Groningen, 2012

64. *Politie en sociale media. Van hype naar onderbouwde keuzen*
A. Meijer, S. Grimmelikhuijsen, D. Fictorie, M. Thaens, P. Siep, Universiteit Utrecht, Center for Public Innovation, Rotterdam, 2013

65. *Wapengebruik. Van inzicht in modus operandi naar een effectieve aanpak*
M.S. de Vries, Universiteit Twente, Enschede, 2013

66. *Politieverhalen. Een etnografie van een belangrijk aspect van politieculturen*
M.J. van Hulst, Tilburg University, Tilburg, 2013

67. *Recherchebazen. Een empirisch onderzoek naar justitieel politieleiderschap*
E.J. van der Torre, M.J. van Duin & E. Bervoets, LokaleZaken, Rotterdam, 2013

68. *Driehoeken: overleg en verhoudingen. Van lokaal tot nationaal*
E.J. van der Torre & T.B.W.M. van der Torre-Eilert, m.m.v. E. Bervoets & D. Keijzer, LokaleZaken, Rotterdam, 2013

69. *Overvallen vanuit daderperspectief. Situationele aspecten van gewelddadige, niet-gewelddadige en afgeblazen overvallen*
W. Bernasco, M.R. Lindegaard & S. Jacques, NSCR, Amsterdam, 2013

70. ***Geweld tegen de politie. De rol van mentale processen van de politieambtenaar***
L. van Reemst, T. Fischer & B. Zwirs, Erasmus Universiteit, Rotterdam, 2013
71. ***Vertrouwen in de politie: trends en verklaringen***
L. van der Veer, A. van Sluis, S. Van de Walle & A. Ringeling, Erasmus Universiteit, Rotterdam, 2013
72. ***Mobiel banditisme. Oost- en Centraal-Europese rondtrekkende criminele groepen in Nederland***
D. Siegel, i.s.m. R. Koenraadt, D. Lyubenova, N. Sovre & A. Troscianczuk, Universiteit Utrecht, 2013
73. ***De ontwikkeling van de criminaliteit van Rotterdamse autochtone en allochtone jongeren van 12 tot 18 jaar. De rol van achterstanden, ouders, normen en vrienden***
F.M.H.M. Driessen, F. Duursma & J. Broekhuizen, Bureau Driessen, Utrecht, 2014
74. ***Speciaal blauw.Verschijningsvormen en overwegingen van specialisatie en despecialisatie binnen de Nederlandse politieorganisatie***
R.J. Morée, W. Landman & A.C. Bos, Twynstra Gudde, Amersfoort, 2014
75. ***Gevangene van het verleden. Crisissituaties na de terugkeer van zedendelinquenten in de samenleving***
M.H. Boone, H.G. van de Bunt & D. Spiegel, m.m.v. K. van de Ven, Erasmus Universiteit, Rotterdam, Universiteit Utrecht, 2014
76. ***Brandstichters onder vuur. Een empirisch onderzoek naar zaken van brandstichting en hun daders***
L. Dalhuisen & F. Koenraadt, Universiteit Utrecht, 2014
77. ***Van stadswacht naar nieuwe gemeentepolitie? Gemeentelijk toezicht en handhaving in de openbare ruimte***
T. Eikenaar & B. van Stokkom, Radboud Universiteit, Nijmegen, 2014
78. ***Politiemensen over het strafrecht***
J. Kort, M.I. Fedorova & J.B. Terpstra, Radboud Universiteit, Nijmegen, 2014
79. ***Kijken, luisteren, lezen. De invloed van beeld, geluid en schrift op het oordeel over verdachtenverhoren***
M. Malsch, R. Kranendonk, J. de Keijser, H. Elffers, M. Konter & M. de Boer, NSCR, Amsterdam, 2015
80. ***De mentale gesteldheid van de familierechercheur. Een onderzoek naar werkgerelateerde stress en secundaire posttraumatische groei binnen een bijzondere groep politieambtenaren***
L.J.A. Bollen, M.C. Saan, M.J.J. Kunst, B.W.C. Zwirs & K.F. Kuijpers, Universiteit Leiden, 2015
81. ***Na de vrijlating. Een exploratieve studie naar recidive en re-integratie van jihadistische ex-gedetineerden***
D.J. Weggemans & B.A. de Graaf, Universiteit Leiden, Universiteit Utrecht, 2015