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.