ONDERZOEKSRAPPORT

Fraudevictimisatie in Nederland

Prof. dr. Marianne Junger, prof. dr. Bernard Veldkamp, Luka Koning (MSc)

29-03-2022

Onderzoeksproject gefinancierd door:

SASS STICHTING ACHMEA SLACHTOFFER EN SAMENLEVING

ICS VISA MasterCard INTERNATIONAL CARD SERVICES

POLITIE

Nederlandse Vereniging van Banken

UNIVERSITY OF TWENTE.

COLOFON

DATUM
29-03-2022

VERSIE
1

AUTEURS
Prof. dr. Marianne Junger, prof. dr. Bernard Veldkamp, Luka Koning (MSc)

E-MAIL
m.junger@utwente.nl, b.p.veldkamp@utwente.nl, l.koning@utwente.nl

POSTADRES
Postbus 217
7500 AE Enschede

WEBSITE
www.utwente.nl/fraudvic

VOORWOORD

Voor u ligt het rapport “Fraudevictimisatie in Nederland”. Het omvat onderzoek naar slachtofferschap van fraude in Nederland, met als voornaamste aspect een slachtofferstudie die voor het eerst de prevalentie hiervan meet.

Het onderzoek is gefinancierd door Stichting Achmea Slachtoffer en Samenleving (SASS), alsmede International Card Services (ICS), de Nationale Politie en de Nederlandse Vereniging van Banken (NVB).

Wij danken iedereen die dit onderzoek ondersteund heeft. Specifiek het bestuur van SASS onder leiding van Gijs de Vries, en aanspreekpunten van de andere financiers: Hans van Loon (voormalig NVB), Marco Doeland (NVB), Maurice Koot en Corinne Weeda-Hoogstad (ICS) en Peter Hagenaars (Nationale Politie). Dank aan Choukri Farahi en Priscilla Huits (ICS) voor hun feedback op de vragenlijst van de slachtofferstudie. Ook dank aan Gijs van der Linden (politie, teamleider Landelijk Meldpunt Internetoplichting) en Marco Harthoorn (politie, analist internetaangifte) en hun collega’s voor het mogelijk maken van het onderzoek bij de aangevers van internetoplichting. Dank aan Evi de Cock en haar collega’s van Centerdata voor de ondersteuning bij het uitvoeren van de slachtofferstudie. Dank aan student-assistenten Rebecca Rameckers, Jildert de Jong en Dominique Westerveld voor hun ondersteuning bij dit project. Dank aan Gea Nijland en Tom Meurs voor het proeflezen van dit stuk. Tenslotte veel dank aan Marti DeLiema, voor het verstrekken van de originele Stanford-vragenlijst en haar hulp bij het aanpassen voor de huidige slachtofferstudie (English: many thanks to Marti DeLiema, for providing the original Stanford questionnaire and her help with converting it for the current victimisation study).

BELEIDSSAMENVATTING

1.1 Achtergrond en onderzoeksopzet

Dit rapport presenteert de gegevens van de eerste slachtofferstudie naar fraude in Nederland. Deze meet integraal de prevalentie van fraude in een steekproef die representatief is voor de Nederlandse bevolking.

Op basis van eerder onderzoek werden 12 fraudecategorieën gemeten: 1) investeringsfraude, 2) aankoopfraude, 3) baanfraude, 4) prijsfraude, 5) schuldfraude, 6) goede-doelenfraude, 7) datingfraude, 8) vriend-in-noodfraude (waaronder Whatsapp-fraude), 9) phishing, 10) identiteitsfraude, 11) spoofing (waaronder helpdeskfraude) en 12) overige fraudevormen.

Gevraagd is naar hoe vaak respondenten van deze vormen slachtoffer waren in de laatste 5 jaar (2016 t/m 2020) en in het laatste jaar (2020). Ook is gevraagd of respondenten in 2020 een mislukte fraudepoging meemaakten en of zij hierop hebben gereageerd. Daarna werden per fraudecategorie vervolgvragen gesteld over de incidenten van 2020. Extra vragen werden gesteld over het belangrijkste incident van elk type fraude in 2020 en de belangrijkste mislukte pogingen van 2020.

Ter aanvulling is een online vragenlijst afgenomen onder aangevers van internetoplichting. Deze vragenlijst richtte zich met name op de aangifte-ervaring en verwachtingen van personen die internetoplichting aangeven via de website van de Nederlandse politie.

1.2 Belangrijkste bevindingen

1. In totaal was in 2020 15,7% van de Nederlanders van 16 jaar en ouder slachtoffer van fraude (grofweg 2,3 miljoen personen). 6,3% was bovendien vaker dan één keer slachtoffer. Aankoopfraude maakte in 2020 de meeste slachtoffers: 10,5%. Slachtofferschap van andere fraudevormen lag in 2020 om en nabij de 1% à 2%.

2. 41,7% van de Nederlanders van 16 jaar en ouder heeft in 2020 tenminste één fraudepoging meegemaakt (mislukt of gelukt; 15,7% slachtofferschap valt hieronder). 20,4% van de Nederlanders van 16 jaar en ouder reageerde ook op een fraudepoging (wat niet altijd leidde tot slachtofferschap).

3. Grofweg 70% van de fraude vond geheel online plaats, 17,8% was een combinatie van offline en online. Deze gebeurtenissen vonden door het hele jaar plaats. In 92,8% van de gevallen vond de fraude plaats in een privésetting (met geld/middelen van respondenten en/of hun persoonlijke relaties). Vooraf aan slachtofferschap besprak 57% de gebeurtenis met iemand; toch beschermde dit niet voor slachtofferschap.

4. Geldverlies bij een fraudegeval is relatief beperkt: de grootste groep verliest € 50. Er is wel een kleine groep respondenten met grote verliezen: 29,9% van de verliezen is boven € 100; 11,1% boven € 500; 4,7% boven € 2500; 3% ook boven € 5000. De grootte van geldverlies varieert per type fraude: bij aankoopfraude zijn de verliezen lager dan bij bijvoorbeeld investeringsfraude, vriend-in-noodfraude en spoofing. Betalingen gaan vaak

(47,7%) via de bank (iDeal of handmatige overschrijving). Bij 14,1% van de gevallen betaalt het slachtoffer met contant geld. Grofweg in 70% van de gevallen krijgen slachtoffers geen geld terug of vergoed, en is het geldverlies permanent. In 20,1% van de gevallen krijgen slachtoffers echter de gehele schade terug of vergoed. Opvallend is dat ongeveer 40% van de slachtoffers met openstaand geldverlies nooit heeft geprobeerd geld terug of vergoed te krijgen en dat ook niet van plan is.

5. Geschat wordt dat de complete schade van de Nederlandse bevolking (16+) in 2020 € 2,75 miljard bedroeg. Vanwege de grote verschillen in de bedragen die slachtoffers verliezen, kent deze schatting echter een behoorlijke onzekerheid.[1]

6. Voor de meeste slachtoffers is de impact van slachtofferschap van fraude beperkt. Slachtoffers denken maar weinig terug aan deze gebeurtenissen (29,2% nooit; 39,7% zelden). 80% à 90% heeft geen financiële, mentale, lichamelijke of sociale problemen ervaren.

   Echter, een significante minderheid heeft echter wél serieuze problemen ervaren. Voor deze groep, 5% à 15% van de slachtoffers, heeft slachtofferschap financiële, mentale, lichamelijke of sociale problemen veroorzaakt. Hoewel zulke impact relatief zeldzaam is gaat dit in absolute aantallen om enkele honderdduizenden personen in Nederland. Hoe meer geld is verloren bij een incident, hoe groter de impact is.

7. Slechts bij 11,8% van de slachtofferschapsgebeurtenissen wordt contact opgenomen met de politie. Dit gebeurt vaker als het geldverlies hoger is. Melders zijn tevreden over het contact met de politie, maar vaak ontevreden over de uitkomst. Respondenten die besloten geen contact op te nemen met de politie geven vooral als reden dat ze dachten dat de politie toch niks zou doen. Met andere professionele organisaties (banken, creditkaartmaatschappijen, betaaldiensten) wordt vrijwel nooit contact opgenomen. Dit beperkt het zicht op fraude.

   Daarnaast geven de respondenten aan dat ze de ervaring vooral achteraf bespreken met persoonlijke relaties, zoals vrienden/familie: 63,5% en professionele relaties, zoals collega's: 9,2%.

   Er wordt niet of nauwelijks psychologische hulp gezocht; enkele slachtoffers zoeken wel juridische hulp. Bijna een derde van de slachtoffers bespreekt de ervaring achteraf met niemand en zoekt dus ook geen enkele vorm van hulp.

8. Respondenten is gevraagd te reflecteren op hoe zij slachtofferschap hadden kunnen voorkomen. Vaak wordt gezegd dat ze meer informatie hadden moeten opzoeken (26,6%) of dat ze alerter hadden moeten zijn (22,1%). Soms had een derde partij iets kunnen doen (13,1%). Respondenten die een mislukte fraudepoging meemaakten is gevraagd waarom zij geen geld verloren. Veel respondenten herkenden de fraudepoging op basis van kennis (54,6%) of voelden wantrouwen (18,3%). Daarnaast werden onder andere persoonlijke veiligheidsregels gevolgd of werd meer informatie opgezocht. Ook bevatten frauduleuze boodschappen geregeld onjuistheden die fraude verraadden.

[1] Dit bedrag is gebaseerd op de gewogen gemiddelde schade van respondenten in de slachtofferstudie (€ 189). Dit gemiddelde is vermenigvuldigd met de grootte van de Nederlandse bevolking van 16 jaar en ouder (14,606,402).

9. Er is niet één type slachtoffer; iedereen kan slachtoffer worden. Zowel mannen als vrouwen worden slachtoffer van fraude; maar, mannen worden wel iets vaker slachtoffer van investeringsfraude. Jongeren worden iets vaker slachtoffer van fraude dan ouderen. Uitzondering hierop is de fraudecategorie spoofing, waaronder (telefonische) bankhelpdeskfraude valt: hiervan worden ouderen vaker slachtoffer. De mate waarin personen aangeven cyberveilig gedrag te vertonen heeft weinig invloed op slachtofferschap, ondanks het feit dat veel gebeurtenissen online plaatsvinden.

10. Zelfcontrole en kennis over fraude zijn de belangrijkste voorspellers voor slachtofferschap: personen met weinig zelfcontrole worden vaker slachtoffer, terwijl personen met kennis over fraude vaker fraudepogingen kunnen weerstaan.

    Voor preventie betekent dit dat het verminderen van snelle beslissingen, hoewel lastig, preventief zou kunnen werken. Meer voorlichting over de werkwijzen van fraudeurs, en ook de procedures van legitieme organisaties, is waarschijnlijk de beste manier om slachtofferschap van fraude tegen te gaan.

Samengevat: fraude is omvangrijk en divers in Nederland. Een aanzienlijk deel van de Nederlandse bevolking komt met fraude in aanraking. Fraude vindt vooral online plaats. De verliezen door en impact van fraude zijn vaak klein, maar soms ook heel groot. Maar weinig slachtoffers zoeken contact met de politie of andere partijen, terwijl dit belangrijk is om zicht te houden op fraude. Snelle beslissingen verminderen en kennis over fraude vergroten zou slachtofferschap kunnen tegengaan.

Leeswijzer

In dit rapport beschrijven wij beknopt de belangrijkste resultaten van het onderzoek. De online bijlage bevat een volledige versie van de methode en resultaten. De online bijlage bevat ook interactieve figuren en tabellen: dit maakt het mogelijk gegevens zelf te rangschikken of te bekijken per fraudecategorie (zie hoofdstuk 1 van de online bijlage voor uitleg).

INHOUDSOPGAVE

1 INLEIDING

Burgers maken zich gewoonlijk op zijn minst enige zorgen over de omvang van de criminaliteit in hun gemeenschap [1-3]. Gegevens over de omvang en de kenmerken van criminaliteit zijn daarom belangrijk voor zowel burgers, belangengroepen als beleidsmakers. Daarom heeft Nederland, net als veel andere Westerse landen, een uitgebreid overzicht van verschillende type periodieke statistieken en afzonderlijke studies om de criminaliteit te meten; het gaat onder meer om slachtofferstudies, zelf-gerapporteerde criminaliteit en justitiële statistieken. Echter, over fraude, en met name online fraude, is weinig empirisch onderzoek beschikbaar. Dit terwijl er verschillende aan elkaar gerelateerde ontwikkelingen spelen die het fraudeprobleem extra urgent maken:

1) *Crime drop, maar stijging van fraude.* Sinds eind jaren ’90 dalen de geregistreerde criminaliteit en slachtofferpercentages, zowel in Nederland [4] als in de gehele Westerse wereld [5-7]. Dit is een inmiddels vaak bestudeerd verschijnsel dat de ‘crime drop’ is gaan heten. Deze daling staat in schril contrast met de door onderzoekers waargenomen stijging van fraude. Tussen 2005 en 2017 nam in Nederland criminaliteit met een 'misleiding'-aspect toe met een factor 2.3, criminaliteit met 'vervalsing' nam toe met een factor 2.4, criminaliteit met 'afpersing' nam toe met een factor 1.8 en criminaliteit met het 'hacken van een computersysteem' nam toe met een factor 3.9 [8]. Wereldwijd laten fraudestatistieken eveneens een alarmerende toename zien, met nieuwe pieken in de VS [9, 10], in het VK [11] en elders in Europa [12].

2) *Criminaliteit gebeurt steeds vaker online.* De genoemde opvallende toename van fraude ligt naar alle waarschijnlijkheid aan het feit dat veel fraude cybergerelateerd is. Dergelijke fraude wordt daarom opgenomen in meerdere categorieën wanneer criminaliteitscijfers worden gemeten [13]. Daarnaast lijken verschillende typen criminaliteit nieuwe digitale vormen te hebben aangenomen: in plaats van winkeldiefstal is er nu online aan- en verkoopfraude; in plaats van bankovervallen wordt er nu gefraudeerd met bankpassen. Veel van deze nieuwe vormen van criminaliteit worden nu als fraude gecategoriseerd [14-17]. Kortom, criminaliteit is tegenwoordig vaak cybercriminaliteit, en veel cybercriminaliteit is – in juridische zin – fraude.

3) *Weinig zicht op fraude.* Behalve een aantal algemene cijfers op basis van politieregistratie is er weinig informatie over de prevalentie en de aard van fraude. Dit geldt voor zowel Nederland als andere landen [18-20]. Nederlands fraudeonderzoek heeft zich tot dusver voornamelijk gericht op verticale fraude (fraude waarbij de overheid het slachtoffer is) [21-24] en op daders van fraude [25, 26]. Er is minder Nederlands onderzoek gedaan naar fraude waarvan particulieren het slachtoffer zijn. Helaas werd fraude ook niet meegenomen in Nederlandse slachtofferstudies. Recent zijn aan de Nederlandse slachtofferstudie (de Veiligheidsmonitor) wel vragen over cybercrime toegevoegd (over aan- en verkoopfraude, betalingsverkeerfraude, identiteitsfraude, phishing, hacken en online bedreiging en intimidatie) [27]. Maar hiermee wordt fraude niet in brede zin gemeten.

4) *Weinig zicht op online criminaliteit.* Criminaliteit verschuift grotendeels naar de digitale wereld [28-31]. Veelal gaat het om fraude die online plaatsvindt. Voor de politie is het

moeilijk om zicht te krijgen op de omvang van deze online criminaliteit [32]. Voor bedrijven die slachtoffer worden van online criminaliteit gaat het vaak tegen hun belangen in om slachtofferschap te melden [33]. Tenslotte blijkt dat de politie moeite heeft met het registreren, opsporen en melden van cybercriminaliteit [34, 35]. Dit betekent dat er minder zicht is op de online criminaliteit vanuit de samenleving dan eerder het geval was met de offline criminaliteit [36]. Deze ontwikkelingen tezamen bemoeilijken het opwerpen van barrières tegen cybercrime.

5) *De groei van online activiteiten.* Tenslotte, meer in het algemeen, is de verwachting dat steeds meer activiteiten online plaatvinden en dat het internet steeds belangrijker wordt. Online handel groeit bijvoorbeeld jaarlijks. E-commerce omvatte in 2020 10 tot 15% van alle detailhandel in Europa en dat cijfer stijgt [37]; zowel in Europa als wereldwijd is er een aanzienlijke groei voorspeld voor de komende jaren. Ook online betalingen vinden steeds vaker plaats [38, 39].

6) *De COVID-19-pandemie.* De coronapandemie heeft een verdere versnelling aangebracht in de groei van online activiteiten, waardoor wat er online gebeurt nog relevanter is geworden voor fraude en cybercriminaliteit. Een aantal ontwikkelingen kan worden opgemerkt. Online shoppen is bijvoorbeeld meer gestegen in 2020 dan aanvankelijk werd verwacht [39, 40]. Thuiswerk nam ook sterk toe [41], wat gepaard ging met een enorme stijging van online vergaderingen [42, 43]. De COVID-19-pandemie heeft er dus zeker voor gezorgd dat meer mensen meer tijd online doorbrachten, waarmee de digitalisering van de samenleving die al lang gaande was verder is versneld. Het is belangrijk om hierbij te vermelden dat de toename van fraude ook al langer is ingezet, zoals hieronder wordt beschreven.

1.1 Doelstelling van het huidige onderzoek

Om de kennis over fraude te vergroten, effectief beleid te ondersteunen, preventieve interventies te ontwikkelen en slachtoffers te helpen, is het huidige onderzoek opgezet. Dit richt zich op fraude in integrale zin, zowel offline als online, aangevuld met vormen van cybercrime (hierna worden voor de leesbaarheid al deze varianten aangeduid met ‘fraude’). De doelstellingen van het onderzoek zijn als volgt:

1. **Het beschrijven van fraude, slachtoffers en risico- en preventiefactoren onder een representatieve steekproef van de bevolking**

    1. Wat is de prevalentie van de drie stadia van fraude onder de Nederlandse bevolking?

    2. Wat is werkwijze van fraudeurs en welke technieken gebruiken potentiële slachtoffers om fraudepogingen te weerstaan (preventiestrategieën)?

    3. Wat is de rol van anderen in de nabijheid van het potentiële slachtoffer?

    4. Welke informatie hebben slachtoffers over fraudeurs?

    5. Wat zijn risico- en preventiefactoren voor slachtofferschap?

Belangrijk zijn met name socio-demografische kenmerken en persoonlijkheidskenmerken. Over de invloed hiervan op slachtofferschap is weinig bekend, zowel in het algemeen als per type fraude.

2. Het beschrijven van de meldingsbereidheid

1. Wat is de meldingsbereidheid van slachtoffers, en wat is de reactie van deze organisatie(s)?

2. Wat zijn de verwachtingen van slachtoffers en in welke mate worden die verwachtingen gerealiseerd?

3. Het beschrijven van de gevolgen van slachtofferschap

1. Wat is de impact van slachtofferschap en wordt er hulp gezocht voor problemen?

2 METHODE

Het huidige onderzoek bestaat uit 2 deelstudies: 1) een slachtofferstudie met het LISS-panel en 2) een vragenlijst onder personen die online aangifte deden van internetoplichting bij de Nederlandse politie.

Hierna wordt de methode van elke deelstudie kort beschreven. Een volledigere versie van de methode van elke deelstudie is te vinden in de online bijlage.

2.1 Slachtofferstudie LISS-panel

Van 11 januari tot 2 februari 2021 is een vragenlijst afgenomen via het LISS-panel (Longitudinal Internet Studies for the Social Sciences-panel [44]). Het LISS-panel is een online panel dat bestaat uit ongeveer 5000 Nederlandse huishoudens, grofweg 7500 individuen, en wordt beheerd door CentERdata (verwant aan Tilburg University). Deelnemende huishoudens zijn door middel van een aselecte steekproef geworven uit het bevolkingsregister van het Centraal Bureau voor Statistiek; als huishoudens niet over een computer en/of internetverbinding beschikken, kunnen ze deze ontvangen om toch deel te nemen [44]. Deze werving levert goede representativiteit voor de Nederlandse bevolking op [45-48].

3623 willekeurig geselecteerde LISS-panelleden zijn uitgenodigd voor deelname aan de vragenlijst, waarvan 2920 de vragenlijst startten. Na selectie op compleet ingevulde vragenlijsten resteerden hiervan 2873 respondenten. Verwijdering van 9 respondenten die onbetrouwbare antwoorden gaven leidde tot een behaalde steekproef van 2864 respondenten (responspercentage: 79%). De antwoorden van deze respondenten zijn via iteratieve post-stratificatie gewogen naar de Nederlandse bevolking, met frequenties van geslacht, leeftijd en opleidingsniveau.

De afgenomen vragenlijst is gebaseerd op de door DeLiema et al. [49] ontwikkelde fraudeslachtofferschapsstudie, welke als pilot is uitgevoerd in de Verenigde Staten. Zij gebruikten de fraudedefinitie van Titus [50]:

> *"Bij fraude gaat het om de verkeerde voorstelling van feiten met de intentie om te misleiden met de belofte van goederen, diensten of andere financiële voordelen die in feite niet bestaan of die nooit bedoeld waren om te worden verstrekt."* [2]

De door DeLiema et al. [49] toegepaste fraudetaxonomie is uitgebreid in het huidige onderzoek. Relatiefraude is opgesplitst in datingfraude en vriend-in-noodfraude (waaronder Whatsapp-fraude valt). Daarnaast zijn de fraudevormen identiteitsfraude (gebaseerd op de Veiligheidsmonitor van het CBS [51]), phishing (gebaseerd op werk van Näsi [52]) en spoofing (waaronder helpdeskfraude valt) toegevoegd.

[2] Vertaald: "*They involve the misrepresentation of facts and the deliberate intent to deceive with the promise of goods, services, or other financial benefits that in fact do not exist or that were never intended to be provided".*

Figuur 1 toont schematisch de toegepaste fraudetaxonomie (de vragen vormen de definities van de fraudecategorieën). Bij phishing en identiteitsfraude was slachtofferschap ook mogelijk zonder geldverlies, namelijk als gegevens van een respondent waren gestolen of misbruikt. Bij alle andere fraudevormen was geldverlies een vereiste om te worden aangemerkt als slachtoffer.

De vragenlijst van de slachtofferstudie bestond uit verschillende delen:

1. *Victimisatiescreening*. Respondenten gaven voor elke fraudecategorie in Figuur 2.1 aan hoe vaak zij hiervan slachtoffer waren in het afgelopen jaar (1 januari t/m 31 december 2020) en de afgelopen vijf jaar (1 januari 2016 t/m 31 december 2020).[3] Ook gaven respondenten voor elke vraag naar fraude aan of zij een mislukte fraudepoging hebben meegemaakt, en, zo ja, of zij hier ook op hebben gereageerd (bij identiteitsfraude is dit niet bevraagd, omdat bij deze fraudevorm geen contact nodig is tussen de dader en het slachtoffer).

2. *Vervolgvragen bij elke fraudecategorie*. Hierna volgden voor iedere fraudecategorie waarvan een respondent in 2020 slachtoffer was een aantal vervolgvragen. Deze bestonden uit 1) vragen specifiek over de incidentcategorie (bijvoorbeeld bij investeringsfraude, 'Wat voor investering was het?') en 2) standaardvragen die bij elke incidentcategorie gesteld werden (bijvoorbeeld, hoeveel geld er betaald/verloren was). Respondenten moesten voor deze vervolgvragen denken aan het incident per fraudecategorie waarbij ze het meeste geld hadden verloren (indien geen verlies: de meest memorabele gebeurtenis).

3. *Belangrijkste incident en mislukte fraudepoging.* Vervolgens werden verdiepende vragen gesteld over het belangrijkste incident in 2020 (indien slachtoffer) en de belangrijkste mislukte fraudepoging in 2020 (indien meegemaakt). Bij de belangrijkste fraude moesten respondenten antwoorden voor het incident in 2020 waarbij het verlies het grootste was (indien geen verlies: de meest memorabele fraude). Bij de belangrijkste mislukte fraudepoging moesten respondenten antwoorden voor de meest memorabele mislukte fraudepoging in 2020.

4. *Achtergrondvragen.* Tenslotte vulden respondenten enkele achtergrondvragen in die risicofactoren maten: een zelfcontroleschaal (gebaseerd op werk van Dickman [53]; dit meet zelfcontrole) en een cyberveiligheidsschaal die riskant online gedrag meet (gebaseerd op werk van Domenie et al. [54] en het CBS [55]). Ook werd respondenten gevraagd voor elke fraudecategorie aan te geven of zij, voor het invullen van de vragenlijst en voor zij mogelijk zelf in aanraking kwamen met de fraudevorm, hiervan wel eens gehoord hadden (ja/nee) (dit meet fraudekennis). Omdat CentERdata een grote hoeveelheid achtergrondinfo levert over de respondenten van het LISS-panel hoefden bijvoorbeeld demografische vragen niet meer gesteld te worden.

[3] Een vraag over de laatste vijf jaar helpt de respondent bij het zich herinneren en wordt gebruikt om respondenten in staat te stellen relatief recente incidenten te melden zonder ze vooruit te schuiven in de rapportageperiode. Verder worden cijfers over de afgelopen vijf jaar op zichzelf in het algemeen als minder betrouwbaar beschouwd (zie ook de reflectie op de methodologie in hoofdstuk 3).

Figuur 1: Fraudetaxonomie van de huidige slachtofferstudie

Fraudecategorie	(Hoe vaak is het gebeurd dat...)
Investeringsfraude	… u uw geld hebt **geïnvesteerd** omdat iemand hoge of gegarandeerde opbrengsten beloofde, maar de investering leverde veel minder op of uw geld werd helemaal niet geïnvesteerd?
Aankoopfraude	… u hebt betaald voor een **product dat, of dienst die**, u nooit ontving of die oplichting was?
Baanfraude	… u betaalde om **een baan te krijgen die niet bestond, een nepvacature,** waardoor u geld verloor of die niet zo winstgevend was als was beloofd?
Prijsfraude	… u betaalde om een **prijs, subsidie, erfenis of loterijwinst** te ontvangen, die u uiteindelijk nooit ontving?
Schuldfraude	… u hebt betaald voor het **aflossen van een schuld** die niet bestond of voor **een rekening** van iets dat u niet gekocht hebt?
Goede-doelenfraude	… u geld doneerde aan een **goede doelen-organisatie of een goed doel** (bijvoorbeeld op een crowdfundingswebsite) die/dat (waarschijnlijk) nep was?
Datingfraude	… u geld gaf of leende aan iemand **die deed alsof hij/zij verliefd op u was**?
Vriend-in-noodfraude (o.a. WhatsApp-fraude)	… u geld gaf of leende aan iemand die **deed alsof ze een familielid, vriend of bekende** van u waren?
Phishing	… u uw gebruikersnaam, wachtwoord of bank- of creditkaartgegevens aan buitenstaanders hebt gegeven in reactie op **phishing via e-mail of via een website**.
Identiteitsfraude	(Naast de vorige vraag…) Hoe vaak heeft iemand zonder dat u dat wilde **gebruik gemaakt van uw persoonlijke gegevens** (bv. naam, bankgegevens, BSN/Sofinummer) voor financieel gewin, bijvoorbeeld voor het opnemen of overmaken van geld, het afsluiten van een lening, het opvragen van officiële documenten, het kopen van producten en/of diensten of het afsluiten van abonnementen?
Spoofing (o.a. helpdeskfraude)	(Naast de vorige vragen…) … u geld bent verloren doordat **iemand deed alsof ze iemand anders waren** (bv. een medewerker van uw bank)?
Overige fraude	(Naast de vorige vragen…) Hoe vaak is er **iets anders** gebeurd waarbij u geld hebt betaald doordat iemand informatie verkeerd voorstelde, loog over informatie of informatie achterhield?

Voor de start van de analyse van de slachtofferstudie zijn alle door respondenten ingevulde antwoorden uitgebreid gecontroleerd. Geregeld gaven respondenten een mislukte fraudepoging aan als een slachtofferschapsgebeurtenis, of werden gebeurtenissen gemeld onder een categorie die daar niet bij paste. Waar nodig zijn de antwoorden van specifieke gebeurtenissen verwijderd of overgeplaatst naar andere categorieën.

De gehele analyse is uitgevoerd met weging naar de Nederlandse bevolking (beschreven onder 2.1). Alle gepresenteerde statistieken zijn dus representatief voor de Nederlandse bevolking. Uitzondering hierop zijn de absolute respondentenaantallen en regressieanalyses; deze zijn ongewogen.

Een uitgebreidere beschrijving van de methodologie, is online beschikbaar. Een bespreking van methodologische aspecten van het meten van fraude is opgenomen in bijlage 1 van dit rapport. De gehele vragenlijst, data en de analysecode in R zijn ook online beschikbaar.

2.2 Vragenlijst online aangevers internetoplichting

In 2021 is een vragenlijst afgenomen bij aangevers van internetoplichting.
Na afronding van een aangifte op de website van de Nederlandse politie (politie.nl) werd een uitnodiging met een link naar de vragenlijst getoond. Dit gebeurde nadat aangifte was gedaan van aan- of verkoopfraude, vriend-in-noodfraude of helpdeskfraude.

446 respondenten namen deel aan de vragenlijst. Respondenten konden kiezen voor een waardebon van € 7.50 als beloning voor hun deelname; er waren 350 waardebonnen beschikbaar. Nadat 350 respondenten aanspraak hadden gemaakt op een waardebon werd de vragenlijst gesloten. Respondenten werden bevraagd over het incident waarvan ze aangifte deden en hun ervaring daarbij. Daarnaast werden respondenten bevraagd over hun motieven en verwachtingen in relatie tot de aangifte.

Een uitgebreidere beschrijving van de methodologie is online beschikbaar. De gehele vragenlijst is ook online beschikbaar.

2.3 Ethische toetsing

De procedure van de twee studies is goedgekeurd door de ethische commissie van de Behavioural, Management, and Social Sciences-faculteit van de Universiteit Twente (slachtofferstudie LISS-panel: #201477; vragenlijst online aangevers internetoplichting: #211216).

3 RESULTATEN EN DISCUSSIE

In deze sectie worden per onderzoeksdoel de belangrijkste resultaten gepresenteerd en bediscussieerd.

Een volledige rapportage met een uitgebreid verslag van de resultaten per onderzoek staat in de online bijlage. De online bijlage bevat ook interactieve figuren en tabellen: dit maakt het mogelijk gegevens zelf te rangschikken of te bekijken per fraudecategorie (zie hoofdstuk 1 van de online bijlage voor uitleg).

3.1 Fraude, slachtoffers en risicofactoren

3.1.1 Prevalentie van de drie stadia van fraude onder de Nederlandse bevolking

De slachtofferstudie mat hoe vaak verschillende fraudevormen in 2020 en in de laatste 5 jaar (2016 t/m 2020) voorkwamen in de Nederlandse bevolking van 16 jaar en ouder.[4] Figuur 2 toont de gemeten prevalentie.

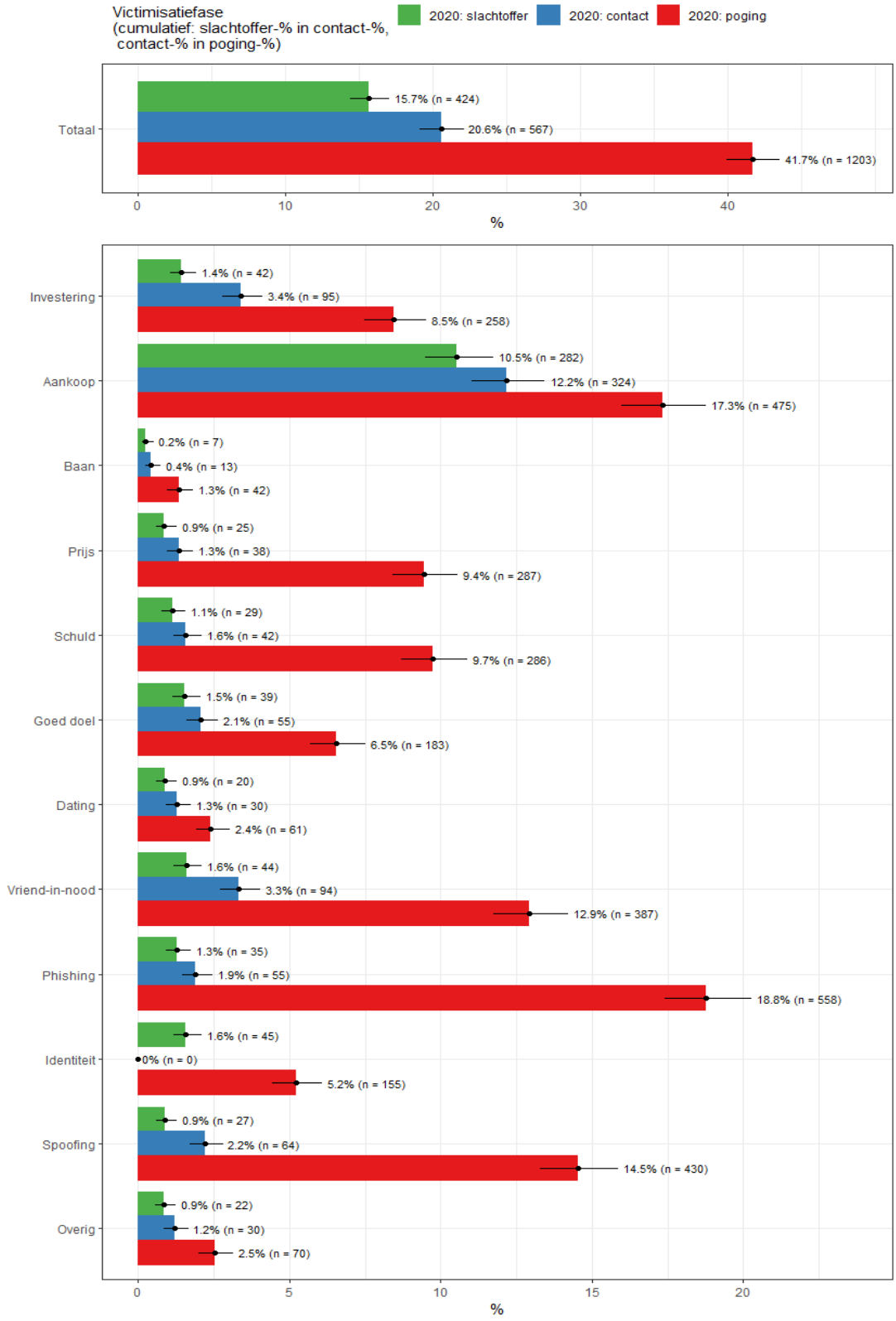
De prevalentie is gemeten voor drie stadia van fraude. Fraude kan namelijk worden gezien als een proces met verschillende stappen. Onderscheid kan gemaakt worden tussen: 1) een poging: benaderd worden door een fraudeur, dan wel op een website uitkomen waardoor iemand in de gelegenheid komt om slachtoffer te worden, 2) een reactie van het potentiële slachtoffer op de fraudeur (‘contact’) en 3) daadwerkelijk slachtofferschap, dat wil zeggen: een betaling of anderzijds verlies van geld. Door fraude op deze manier te benaderen kan een beter begrip van slachtofferschap en het voorkomen ervan worden bereikt [50, 56].

Uit de resultaten blijkt dat van de Nederlandse bevolking van 16 jaar en ouder in 2020 15,7% slachtoffer was van fraude (grofweg 2,3 miljoen personen). 41,7% van alle Nederlanders van 16 jaar en ouder heeft in 2020 een fraudepoging meegemaakt (mislukt of gelukt; 15,7% slachtofferschap valt hieronder). 20,6% van alle Nederlanders van 16 jaar en ouder reageerde ook een fraudepoging (hetgeen niet altijd leidt tot slachtofferschap).

6,3% (40,2% van de slachtoffers) van de Nederlandse bevolking van 16 jaar en ouder is bovendien meer dan één keer slachtoffer geworden in 2020; 3,9% (24,6% van de slachtoffers) werd zelfs drie keer of vaker slachtoffer.

[4] Op 1 januari 2021 waren, naar cijfers van het CBS, 14.606.402 personen in Nederland 16 jaar of ouder. 1% van de Nederlandse bevolking van 16 jaar en ouder staat daarmee gelijk aan 146.064 personen.

Figuur 2: Fraude onder de Nederlandse bevolking (met 95% betrouwbaarheidsinterval)



Aankoopfraude kende de meeste slachtoffers: 10,5% in 2020 (grofweg 1,5 miljoen personen), en 18,6% in de afgelopen 5 jaar. Daarna volgen zes type incidenten waarbij de slachtofferpercentages liggen tussen de 1% en 2% voor 2020, en wat hoger voor de afgelopen vijf jaar: identiteitsfraude: 1,6% en 3,3%, vriend-in-noodfraude: 1,6% en 3%, goede doelen-fraude: 1,5% en 3%, investeringsfraude: 1,4% en 5,4%, phishing: 1,3%[5] en 2,3% en tenslotte schuldfraude: 1,1% en 2%, respectievelijk.

Tenslotte volgen vier type incidenten die door iets minder dan 1% van de respondenten worden gemeld, in 2020 of de afgelopen vijf jaar: overige fraude: 0,9% en 3%, spoofing: 0,9% en 2,4%, prijsfraude: 0,9% en 2,1%, datingfraude: 0,9% en 1,9% en tenslotte baanfraude: 0,2% en 0,5%, respectievelijk.

Bij phishing komen de meeste pogingen voor: 18,8% maakte dit mee in 2020. Dit wordt gevolgd door aankoopfraude (17,3%), spoofing (14,5%) en vriend-in-noodfraude (12,9%).

Van belang is om zich te realiseren dat wanneer 15,7% van de bevolking slachtoffer is van fraude, in een jaar, dit 2.293.205 mensen betreft [57].

Vergelijking met Nederlands onderzoek

Een belangrijke vraag is: in hoeverre de gevonden cijfers overeenkomen met voorgaand Nederlands onderzoek? Het is echter lastig om te vergelijken met andere Nederlandse studies, omdat fraude in Nederland nooit expliciet en uitgebreid is gemeten. Nederlandse cijfers komen daarom vooral voort uit onderzoek naar digitale criminaliteit, met als voornaamste studie de Veiligheidsmonitor van het CBS [27] (aankoopfraude, identiteitsfraude en phishing zijn in zowel de Veiligheidsmonitor als in de huidige studie bevraagd. Bijlage 3 toont de vragen uit beide studies).

Gekeken naar individuele fraudecategorieën:

- Aankoopfraude: de huidige studie vond 10,5% slachtofferschap voor 2020. Het CBS [27] vond bij de Veiligheidsmonitor van 2021 een slachtofferschapspercentage van 6,9%. Daarbij moet worden opgemerkt dat het CBS zich enkel richtte op online aankopen, en het huidige onderzoek zich richtte op alle aankopen. Ook vermeldde de vraagstelling van het CBS dat het moest gaan om betaling voor diensten of producten die nooit geleverd werden; de huidige slachtofferstudie noemde dat het moest gaan om een betaling voor diensten of producten die nooit geleverd werden of oplichting waren[6];

[5] Bij phishing moet worden opgemerkt dat het slachtofferpercentage in werkelijkheid hoger zou kunnen liggen. Wanneer, na het invullen van informatie op een phishing website, gegevens worden doorgegeven aan een fraudeur, heeft het slachtoffer dit niet altijd door. Anders zou het slachtoffer de gegevens niet verstrekken. Het besef van slachtofferschap kan dan pas komen wanneer gegevens worden misbruikt, wat een tijd kan duren. Als gegevens worden misbruikt is het bovendien mogelijk dat het slachtoffer niet weet dat deze gegevens verkregen zijn met phishing.

[6] Respondenten zijn bevraagd over om welk type oplichting het ging bij aankoopfraude. 82,2% gaf aan dat het product of de dienst niet geleverd werd; 10,3% gaf aan dat het product/de dienst van slechte kwaliteit was, 8,2% beschreef een ander type oplichting (zie online bijlage).

- Schuldfraude: de huidige studie vond 1,1% slachtofferschap voor 2020. Het CBS [55] rapporteerde voor 2018 cijfers over vergelijkbare incidenten. Daarbij was de prevalentie van voorschotfraude 0,1% en die van neppe boetes en facturen 0,3%. Opgeteld zou dit maximaal 0,5% zijn;

- Vriend-in-noodfraude: de huidige studie vond 1,6% slachtofferschap. Eerder Nederlands onderzoek vond 0,7% slachtofferschap voor 2020, dat richtte zich echter wat specifieker op 'Whatsapp-fraude' [58];

- Phishing: de huidige studie vond 1,3% slachtofferschap. In de Veiligheidsmonitor van 2021 van het CBS [27] een prevalentie van 0,8%.

- Identiteitsfraude: de huidige studie vond 1,6% slachtofferschap voor 2020. In de Veiligheidsmonitor van 2021 vond het CBS [27] een prevalentie van 0,8%.

De cijfers van het huidige onderzoek zijn hoger dan die uit andere Nederlandse studies. Hier zijn een aantal mogelijke verklaringen voor.

Allereerst kan niet onvermeld blijven dat 2020 de start inluidde van de COVID-19-pandemie. De Nederlandse overheid heeft, vanaf maart, gedurende het jaar verschillende maatregelen tegen de verspreiding van het coronavirus genomen. Deze maatregelen hebben geleid tot een aanzienlijke wijziging in de routine van veel mensen, waarbij vooral gold dat de meeste mensen minder vaak buitenshuis en meer online waren. Deze veranderingen waren vermoedelijk grotendeels verantwoordelijk voor een toename van online delicten [59-67].

Een belangrijke reden voor relatief hogere schattingen is daarnaast waarschijnlijk de integrale wijze waarop fraude in deze studie is gemeten. De formulering van de victimisatievragen in de huidige studie is gebaseerd op een Amerikaanse vragenlijst die is ontworpen na een uitgebreide studie van de literatuur en vervolgens is getest [49, 68-70]. Zoals hierboven aangegeven, is ervoor gekozen dat het woord 'fraude' niet in de vragenlijst gebruikt is. Onderzoek heeft laten zien dat dit nauwkeuriger gegevens oplevert [71]; respondenten associëren niet altijd alle frauduleuze incidenten met politie en justitie en met criminaliteit. De vragen in de huidige victimisatiescreening werden dus op brede wijze gesteld. Onder de gegeven definities kon een grote variëteit aan incidenten worden gerapporteerd. Zo mat het huidige onderzoek mogelijk meer en meer verschillende fraude dan andere Nederlandse studies.

Wij zijn echter van mening dat de huidige studie niet te breed of te veel heeft gemeten. Er zijn namelijk verschillende andere methodieken gehanteerd om zo correct mogelijk te meten en overrapportage te vermijden:

- De screeningsvraag voor slachtofferschap in de afgelopen 5 jaar reduceert 'forward telescoping' (waarbij incidenten van vóór de rapportageperiode toch gemeld worden);

- Alle antwoorden van respondenten zijn zorgvuldig geïnspecteerd; waar nodig zijn gebeurtenissen verwijderd of her-gecategoriseerd.

Hiernaast kunnen vele verschillende aspecten van slachtofferstudies de resultaten signficant beïnvloeden, bijvoorbeeld de uitgenodigde steekproef en het responspercentage. De huidige studie behaalde een hoog responspercentage (79%) bij het LISS-panel, dat zeer goed

beoordeeld wordt op representativiteit voor de Nederlandse bevolking (zie methode). De Veiligheidsmonitor 2021 van het CBS [27] behaalde een landelijk responspercentage van 31,7%, maar had daarentegen wel veel meer deelnemers (ruim 170 duizend). Wat de precieze invloed van deze en andere verschillen is, is vaak lastig te zeggen. In Bijlage 1 wordt verder ingegaan op de methodologische aspecten van slachtofferstudies.

Vergelijking met Amerikaans onderzoek

De huidige slachtofferstudie is gebaseerd op een Amerikaanse pilot [49], die fraude heeft gemeten over de periode van 26 april 2015 t/m 3 mei 2016. De percentages van de Amerikaanse studie zijn hoger dan in de huidige studie, ondanks het feit dat de vraagstelling nagenoeg hetzelfde is: 50,4% van de respondenten was daar slachtoffer van de fraudecategorieën samen (versus 15,7% in het huidige onderzoek).

Een analyse van de verschillende tussen de huidige studie en de Amerikaanse versie is opgenomen in Bijlage 2.

GELDVERLIES

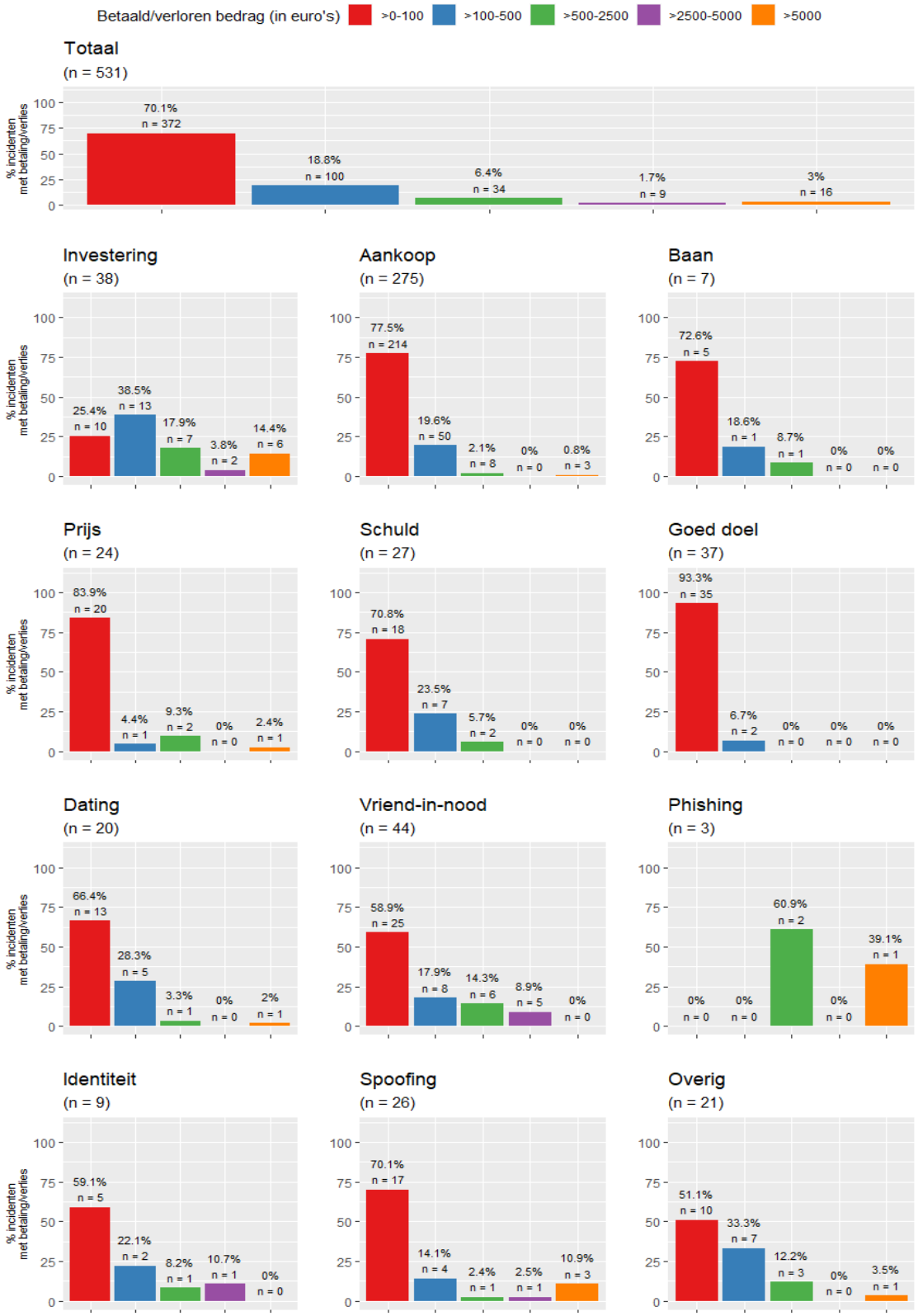
Figuur 3 toont de bedragen die respondenten van de slachtofferstudie verloren bij het belangrijkste incident per fraudecategorie (enkel incidenten inbegrepen waarbij geld betaald/verloren is).

De schade van de meeste slachtoffers is niet erg hoog. Het mediane verlies onder alle incidenten waarbij geld is verloren ligt op € 50, gemiddeld € 954 maar met een hoge standaardafwijking van ongeveer € 8600. Er is een kleine groep respondenten met grote verliezen (29,9% van de verliezen is boven € 100; 11,1% ook boven € 500: 4,7% ook boven € 2500; 3% ook boven € 5000). Het grootste verlies in deze studie was € 186.000 voor investeringsfraude met cryptovaluta.

Dat verliezen vaak onder de € 100 vallen is bij vriend-in-noodfraude (waaronder Whatsapp-fraude valt) opvallend, gezien bij verhalen in de media over deze fraudevorm vaak hogere bedragen naar voren komen (duizenden euro's). Daarbij is het vaak zo dat fraudeurs zich voordoen als een kind van het slachtoffer. In deze slachtofferstudie gaven respondenten aan dat daders zich ook voordeden als een vrienden of kennis (64%); slechts 36% gaf aan dat de daders zich voordeden als een familielid. Fraudeurs die zich voordoen als een familielid vragen meer geld dan fraudeurs die zich voordoen als een vriend (gemiddeld verlies € 791 bij familielid, versus € 475 bij vriend). Ook werden er daadwerkelijk lage bedragen gevraagd in het geval van familieleden, zo beschrijft één respondent die € 50 verloor "zoon had geld nodig, stuurde tikkie". Een studie van onderzoekers van de Haagse Hogeschool naar Whatsapp-fraude [58] vond overigens ook dat relatief lage verliezen vaak voorkomen (34% van de slachtoffers betaalde daar minder dan € 50, 20% € 50-750, 27% €750-2500, 13% €2500-500 en 6% meer dan € 5000).

Ook bij een vorm als helpdeskfraude, wat in deze slachtofferstudie onder de fraudecategorie spoofing valt, wordt vaak gesproken over relatief hoge verliezen. Deze zijn in deze studie aanwezig, maar er zijn ook kleinere verliezen. Dit komt omdat de spoofing-categorie breder is dan geformuleerd dan enkel bankhelpdeskfraude; respondenten noemen niet enkel dat fraudeurs zich voordeden als bankmedewerkers, maar ook dat fraudeurs zich voordeden als bijvoorbeeld een medewerker van Google, Ziggo of Vodafone. Bij deze andere vormen kunnen de verliezen over het algemeen lager zijn.

Figuur 3: Geldverlies bij belangrijkste incidenten per fraudecategorie



De meeste betalingen verlopen via de bank (iDeal of een handmatige overschrijving): 47,7%. Daaropvolgend werd in 14,1% van de gevallen met contant geld betaald. De rest van de betalingen verliep op uiteenlopende wijze. Slechts 0,8% van de betalingen werd met cryptovaluta gedaan.

Bij de meeste respondenten is het verlies van geld permanent: in 68,6% van de gevallen kregen slachtoffers niets terug of vergoed. In 20,1% van de gevallen kregen slachtoffers wel het hele verloren bedrag terug of vergoed.

Bij het belangrijkste incident is aan respondenten, die nog niet (al) hun geld terug hadden gekregen, gevraagd of ze proberen of hebben geprobeerd (de rest van) hun geld terug te krijgen. Opvallend is dat 39,6% dit nooit geprobeerd heeft en ook niet van plan is om dit te proberen. Dit kan te maken hebben met de relatief lage bedragen waar het vaak om draait. Ook kan het zo zijn dat de kans van slagen laag wordt ingeschat. Daarnaast kan het zo zijn dat slachtoffers van mening zijn dat zij verliezen opnemen als iets dat ze maar te nemen hebben; zelfverwijt kan ervoor zorgen dat ze niet op zoek gaan naar herstel van geleden schade.

Geschatte schade van fraude in Nederland

Het gemiddelde opgetelde verlies van respondenten in de slachtofferstudie was € 189 (los van eventueel later teruggekregen of vergoed geld). Omgerekend naar de Nederlandse bevolking van 16 jaar en ouder betekent dit dat de omvang van fraude € 2,75 miljard zou zijn. Deze schatting bevat onzekerheid omdat deze leunt op relatief weinig respondenten. Daarnaast lijden sommige slachtoffers extreme verliezen (‘uitschieters’). Zowel slachtofferschap als de geleden schade bij slachtofferschap zou in de steekproef van deze slachtofferstudie minder of meer geobserveerd kunnen zijn dan in de werkelijke populatie. De geschatte schade zou om twee redenen in ieder geval iets hoger moeten zijn:

- Per fraudecategorie zijn er vervolgvragen werden gesteld voor één belangrijkste slachtofferschapsgebeurtenis. Daarom is dit bedrag tot stand gekomen met de verliezen van maximaal één (doch wel het grootste) verlies per fraudecategorie. Als een respondent bijvoorbeeld tweemaal slachtoffer was van aankoopfraude telde slechts één van deze twee gebeurtenissen mee in deze schatting;

- Van een aantal door respondenten verkeerd gerapporteerde slachtofferschapsgebeurtenissen is het verloren bedrag onbekend. Deze slachtofferschapsgebeurtenissen voegen niet toe aan de schatting terwijl er wel verliezen zijn geleden (deze bedragen zijn als ‘0’ opgenomen in de berekening).

Dat de omvang van schade door fraude in Nederland groot is, blijkt ook uit eerder onderzoek [72]. De Betaalvereniging Nederland rapporteert dat de totale schade in het bancaire betalingsverkeer in 2020 als gevolg van alleen al phishing en telefonische spoofing € 39,5 miljoen bedraagt.

3.1.2 Werkwijze van fraudeurs

De gepresenteerde prevalentie schetst met welke fraudevormen fraudeurs werken. In de slachtofferstudie en de vragenlijst onder aangevers van internetoplichting zijn aanvullende vragen gesteld over de kenmerken van fraudegebeurtenissen. Dit geeft meer informatie over hoe fraudeurs te werk gaan. Hieronder worden de belangrijkste resultaten gepresenteerd.

CHRONOLOGIE/TIJDSVERLOOP

Fraudegebeurtenissen in de slachtofferstudie vonden door het hele jaar plaats. Er zijn geen maanden waarin fraude duidelijk veel meer of minder voorkomt, ook niet wanneer wordt gekeken naar specifieke fraudevormen.

In de slachtofferstudie is, bij belangrijkste slachtofferschapsgebeurtenissen, gevraagd wanneer respondenten beseften dat ze hun geld verloren waren. Dit besef komt vaak óf vrijwel direct (binnen 3 uur: 23%), óf pas na een iets langere periode (3,5 dagen tot 3 maanden: 60,4%). 8,3% van de slachtoffers realiseert zich pas na 3 maanden dat zij geld zijn verloren.

CONTEXT

Privé/professioneel: in de slachtofferstudie vonden vrijwel alle gerapporteerde belangrijkste slachtofferschapsgebeurtenissen (92,8%) en mislukte fraudepogingen (88%) plaats in een privésetting (met geld en/of middelen van respondenten en/of hun persoonlijke relaties).

Offline/online: veruit de meeste belangrijkste slachtofferschapsgebeurtenissen (68,9%) en mislukte fraudepogingen (74,9%) in de slachtofferstudie vonden geheel online plaats. Respectievelijk 13,2% en 18,2% van de gebeurtenissen vonden geheel offline plaats; 17,8% en 7,2% vond zowel offline als online plaats. Daarmee kan de conclusie getrokken worden dat fraude voornamelijk bestaat uit digitale criminaliteit.

Contact met daders: bij belangrijkste slachtofferschapsgebeurtenissen in de slachtofferstudie is respondenten gevraagd of en hoe ze contact hadden met de dader(s) bij de ervaring. Opvallend is dat 34.5% van de respondenten aangeeft geen contact te hebben gehad met de dader(s). 22.6% gaf aan contact te hebben gehad via e-mail; 18.4% via een online handelsplatform; 7,5% via sociale media; 6,8% via een telefoongesprek; 5,6% via een appgesprek, 2,6% via een sms. Daarnaast ontmoette 5,2% de dader(s) aan huis.

3.1.3 Preventiestrategieën van slachtoffers & de rol van anderen in de nabijheid van het slachtoffer

In de slachtofferstudie is gevraagd of respondenten *vooraf* aan een betaling/verlies van geld een fraudegebeurtenis bespraken met iemand. Bij het belangrijkste incident deed 57% dit. Bij de belangrijkste mislukte fraudepogingen is er een iets hoger percentage dat de gebeurtenis vooraf aan een mogelijke betaling/verlies van geld besprak: 63,7%. Dit is iets meer dan bij de slachtoffers en zou erop kunnen duiden dat het vooraf bespreken enige maar beperkte beschermende werking heeft.

Zowel bij slachtofferschap als bij pogingen worden gesprekken het meest gevoerd met persoonlijke relaties (slachtofferschap: 87,4%, pogingen: 88,6%), gevolgd op grote afstand door professionele relaties (slachtofferschap: 14,3%, pogingen: 13%).

Al met al blijft het zo dat respondenten vaak van tevoren een fraudegebeurtenis bespreken, maar dat zij vervolgens vaak hun eigen weg kiezen en dus ook slachtoffer worden. Ook professionele organisaties hebben beperkte invloed wanneer zij worden geraadpleegd. De vraag is uiteraard wat potentiële slachtoffers voorleggen en welk advies zij krijgen. Op het eerste gezicht lijkt hier echter ruimte voor verbetering om slachtofferschap te voorkomen.

Reflectie op slachtofferschap

In de slachtofferstudie is gevraagd hoe, achteraf bezien, zij geldverlies hadden kunnen voorkomen. Met kwalitatieve analyse vielen een aantal verschillende typen antwoorden te onderscheiden.[7]

Informatie opzoeken: 26,6% gaf aan dat ze zelf vooraf meer informatie hadden moeten opzoeken:

> *"Niet gehaast iets bestellen. Beter onderzoeken en kritischer kijken"*
>
> *"Eerst de advertentie goed doorlezen, en jezelf afvragen of de prijs van het artikel niet te mooi is om waar te zijn"*
>
> *"Beter lezen en research doen naar [het] online bedrijf"*
>
> *"De reviews lezen over de verkoper"*

Wantrouwen: 5,9% zei dat ze niet zomaar de fraudeurs hadden moeten vertrouwen:

> *"Nooit goed gelovig zijn als er geld aan te pas komt"*
>
> *"Niet alles vertrouwen"*
>
> *"Mensen niet meer vertrouwen als ze vooraf geld vragen om naar je toe te komen"*

Alerter zijn: 22,1% zei dat ze alerter hadden moeten zijn, en/of dat er signalen waren waaraan de respondent had kunnen zien dat er sprake was van fraude:

> *"Ik had beter moeten opletten"*
>
> *"Beter letten [op] naar de site waarnaar je gelinkt wordt"*
>
> *"Beter moeten kijken naar de afzender"*

Derde partij: 13,1% gaf aan dat een derde partij iets had moeten of kunnen doen om slachtofferschap te voorkomen:

> *"Ik had eerst de reviews van de webshop moeten lezen. Deze waren zodanig slecht dat ook de bank hier wel vanaf zou moeten kunnen weten"*
>
> *"Sterker controle vanuit Marktplaats en scherper vanuit mij. Niet meteen betalen"*
>
> *"Ik ging ervan uit [dat] als iemand mocht adverteren op Facebook dat dit dan wel in orde zou zijn"*

Principes: 9% noemt dat ze bepaalde veiligheidsregels of principes hadden moeten volgen:

> *"Nooit meer kleding online bestellen of met creditcard betalen"*

[7] De opmerkingen van de respondenten zijn zo weinig mogelijk geredigeerd.

"Ik had aan mijn principes moeten vasthouden, alleen op eigen initiatief een koop doen; niet mondeling aan de telefoon"

"Door nooit meer iets via Facebook te kopen. Het was een gok om te kijken of dit daadwerkelijke producten waren. De hoeveelheid geld was gering, dus had ik er niet veel moeite mee"

"Niet opnemen als een vreemd nummer belt, vooral vanuit het buitenland"

"Niet aan de deur kopen"

Verder werd bijvoorbeeld genoemd dat respondenten er simpelweg niet mee hadden moeten gaan in wat de fraudeurs wilden (13,5%), dat ze hun gevoel hadden moeten vertrouwen (3,6%), of juist niet hun gevoel hadden moeten vertrouwen (0,5%). Daarnaast zeggen respondenten dat ze anderen hadden moeten raadplegen voor advies (7,2%) of dat ze contact hadden moeten opnemen met de persoon of organisatie als wie de fraudeur zich voordeed (3,2%). Ook genoemd wordt dat respondenten pas achteraf hadden moeten betalen of iets hadden moeten versturen, en/of ergens hadden moeten langsgaan in plaats van op afstand iets te (ver)kopen (3,2%).

Reflectie op fraudepogingen

In de slachtofferstudie is aan respondenten die een mislukte fraudepoging meemaakten gevraagd waarom zij geen geld zijn verloren of hebben betaald. In kwalitatieve analyse van de antwoorden kon onderscheid gemaakt worden tussen verschillende veelvoorkomende redenen (niet exclusief).

Fraudekennis*:* Maar liefst 54,6% noemt dat een fraudepoging werd herkend op basis van eigen kennis, bijvoorbeeld:

"Het klonk te onwaarschijnlijk voor woorden. Rare manier van doen. Ik ben financieel voldoende op de hoogte van zaakjes die stinken"

"Ik vertrouwde het niet en heb vaker van phishing gehoord"

"Omdat het duidelijk een geval van Whatsapp-fraude was"

"Omdat ik op de hoogte ben en waakzaam en alert ben"

"Omdat ik vrijwel meteen merkte dat het een nepbericht was"

"*Je bank belt je nooit op over verdachte transacties maar op dat moment dacht ik even niet goed na omdat z[e] inspelen op je angst en [om]dat ze mee[-]acteren"*

Wantrouwen: 18,3% benoemt dat zij geen slachtoffer zijn geworden door te vertrouwen op hun gevoel:

"Omdat ik me er niet goed bij voelde en [een] niet pluis gevoel had"

"Gevoelsmatig klopte het niet"

"Omdat ik het een vreemd gesprek vond"

Principes: 7,2% voorkwam slachtofferschap door principes of persoonlijke regels te volgen:

"[Ik] let goed op mijn rekeningen [en] zal niet in iets raars intrappen. Telefonisch zal [ik] nooit gegevens verstrekken, als [ik] gebeld wordt door [een] onbekende leg [ik] gelijk [de telefoon] neer"

"Ik geef nooit zomaar geld weg zonder dat ik de organisatie heb gecontroleerd. Dit doe ik zowel met energiemaatschappijen, als bij wat voor andere transactie ook. Dit schiet soms wel eens [zo ver] door dat ik legitieme partners ook niet heb betaald soms, omdat ik hun gesprekken te verdacht vond en hun informatie te karig."

"Ik maak geen afspraken online of per telefoon."

Informatie opzoeken: 6,3% gaf aan dat ze niet meegingen in de fraudepoging omdat er informatie ontbrak of omdat ze zelf eerst meer informatie opzochten:

"Informatie ingewonnen bij creditkaartmaatschappij"

"Ik heb de juistheid geverifieerd en geconstateerd dat hier sprake was van oplichting"

Onjuistheden zijn opgemerkt: 6,1% geeft aan dat aspecten van de frauduleuze boodschap niet kloppen, waardoor de respondent doorheeft dat het om een fraudepoging gaat:

"Ik heb geen dochter"

"Andere bank dan waar ik ik zelf bij ben"

"De sms was niet van mijn bank"

Eigen context: Terwijl de onjuistheden hierboven beschreven meestal betrekking hebben op de frauduleuze boodschap, verwijzen sommige respondenten naar hun eigen administratie of hun eigen omstandigheden: 2,9% gaf aan dat door fraudeurs verstrekte informatie niet klopte, wat hen behoedde voor slachtofferschap:

"Heb geen schuld, en was van iets waar ik geen contract hebt."

"Niets besteld om via PostNL te laten bezorgen"

"Omdat mijn zoon mij nooit zou vragen om geld te lenen. Na het incident bleek dat meerdere bekenden op dezelfde manier waren benaderd"

"Omdat het totale onzin is. Ik heb goed contact met mijn kinderen en daarvan weet ik dat ze niet in de financiële problemen zitten"

Redenen zoals dat de bank de transactie blokkeerde, dat anderen de respondent hebben overtuigd om niet in de poging tot fraude mee te gaan, of dat de respondent de politie heeft gebeld komen minder dan 1% voor. 8,6% geeft overige redenen op.

3.1.4 Informatie over daders

In de slachtofferstudie is gevraagd of slachtoffers contact hadden met de dader(s), en, zo ja, of zij wisten wie de daders waren. 16,3% van de slachtoffers weet in dat geval wie de daders waren. Het vaakst denken slachtoffers dan dat de daders mannelijk waren (42,9%), al weten slachtoffers vaak het geslacht niet (40,2%). Bij belangrijkste mislukte fraudepogingen worden

vergelijkbare cijfers over daders gevonden: hierbij weet 3,4% wie de daders waren; 50,1% denkt dat de daders mannelijk waren en 24,6% weet het geslacht niet. Fraudeurs bleken dus grotendeels anoniem voor de slachtoffers.

In de vragenlijst onder aangevers van internetoplichting is ook gevraagd naar wat respondenten over daders wisten. 89,6% gaf aan te denken dat er slechts één dader was bij hun gebeurtenis. Gevraagd naar het geslacht van de daders gaf 71,4% aan het niet te weten (17,8% man; 8,4% vrouw; 2,5% man en vrouw); ook bij aangevers lijken daders dus grotendeels anoniem te zijn.

3.1.5 Risicofactoren voor slachtofferschap

Bij de slachtofferstudie zijn potentiële risicofactoren gebruikt om de kans op slachtofferschap in 2020 te modelleren met multivariabele binaire logistische regressie. Dat is gedaan voor alle fraudecategorieën samen en voor elke fraudecategorie individueel.

Verschillen in slachtofferschap kunnen zowel het gevolg zijn van een verschil in blootstelling aan fraudepogingen als van een verschil in kwetsbaarheid voor fraudepogingen. Gebruikers die bijvoorbeeld veel online zijn, of waarvan het e-mailadres online te vinden is, door bijvoorbeeld een datalek, lopen een relatief grote kans om phishing e-mails te ontvangen. Daarom zijn modellen gemaakt voor de gehele steekproef (dit toont de *algemene slachtofferkans*) en een selectie van respondenten die een fraudepoging meemaakten (dit toont de *slachtofferkans bij poging*).

Hieronder wordt per risicofactor besproken wat de relatie is tot de onderzochte fraudecategorieën.

GESLACHT

Het huidige onderzoek vond enkel bij investeringsfraude dat mannen een hogere algemene slachtofferkans hebben. Bij de selectie van respondenten die een fraudepoging meemaakten gold enkel dat vrouwen vaker slachtoffer zijn van aankoopfraude.

Verder geldt echter dat er geen verschillen zijn naar geslacht. Ook een grote studie als de Engelse slachtofferstudie (n = 34.163) vond geen verschillen naar geslacht [73].

Verschillen in slachtofferschap naar geslacht spreken tot de verbeelding en zijn vaak bestudeerd. Over het algemeen zijn er inconsistente resultaten gevonden over of mannen of vrouwen vaker slachtoffer worden en/of kwetsbaarder zijn voor fraude, ook wanneer wordt gecontroleerd voor blootstelling in experimenteel onderzoek [74, 75].

LEEFTIJD

Ouderen worden minder vaak slachtoffer, in het algemeen en wanneer zij blootgesteld worden aan een fraudepoging. Een uitzondering hierop geldt bij spoofing (waaronder helpdeskfraude): wanneer ouderen daarvoor benaderd worden, worden zij vaker slachtoffer dan jongeren.

De meeste bevolkingsonderzoeken vinden eveneens dat jongeren vaker slachtoffer zijn van fraude dan ouderen [49, 73, 76-81].

Studies die naar kwetsbaarheid keken vonden dat jongeren vaker slachtoffer worden bij een poging dan ouderen [79]. Sommige studies vonden een omgekeerde U-relatie tussen

slachtofferschap van fraude en leeftijd en rapporteerden dat slachtofferschap het hoogst is in de leeftijdsgroep van 35 t/m 65; jongeren en ouderen zijn minder vaak slachtoffer [73, 77, 82, 83].

ALLEENSTAANDEN

Gekeken naar de algemene slachtofferkans zijn alleenstaanden vaker het slachtoffer van datingfraude. Dit lijkt simpel verklaarbaar omdat alleenstaanden waarschijnlijk vaker op zoek zijn naar een romantische partner. Bij investeringsfraude zijn alleenstaanden ook vaker slachtoffer en kwetsbaarder voor pogingen; wellicht is dit zo omdat zij dergelijke investeringen vooraf niet met een partner of huisgenoten kunnen bespreken.

Verder werden er geen significante effecten van alleenstaand zijn op slachtofferschap gevonden.

INKOMEN

Personen met een lager persoonlijk netto inkomen zijn significant vaker slachtoffer van baanfraude. Bij blootstelling aan een poging geldt ook dat personen met een lager inkomen vaker slachtoffer worden van investeringsfraude, prijsfraude en identiteitsfraude. Dit verhoogde slachtofferschap zou gedeeltelijk verklaard kunnen worden doordat vooral deze personen op zoek zijn naar manieren om geld te verdienen en/of door dat zij die manieren ook (harder) nodig hebben.

Eerder onderzoek onder ouderen vond dat het inkomen ‘a key determinant of vulnerability’ is [84]; een lager inkomen verhoogt kwetsbaarheid voor fraudepogingen. Eerder Nederlands onderzoek vond echter geen verband tussen slachtofferschap van online consumentenfraude en inkomen [85]. Ander onderzoek rapporteerde weer dat personen met hogere inkomens relatief vaker slachtoffer lijken te zijn van identiteitsfraude [80, 83]. Tenslotte zijn er studies die, net als voor leeftijd, een omgekeerde U-relatie vinden waarbij middeninkomens het meest frequent slachtofferschap van fraude vermelden [77, 78].

OPLEIDINGSNIVEAU

Een hoger opleidingsniveau verhoogt significant de kans op identiteitsfraude en investeringsfraude. Na controle voor gelegenheid blijkt dat alleen de kans op investeringsfraude samenhangt met opleidingsniveau. Verder heeft opleidingsniveau geen significante invloed. Omdat investeringsfraude gekenmerkt wordt door een laag inkomen, een hoge opleiding en het vaak alleenstaanden betreft, lijkt het erop dat dit tot op zekere hoogte studenten betreft.

De Amerikaanse pilot [49] vond dat een hoger opleidingsniveau samenhangt met meer slachtofferschap van investeringsfraude. De onderzoekers vonden verder weinig verschillen naar opleiding tussen slachtoffers en niet-slachtoffers. Uit meerdere andere studies blijkt dat opleidingsniveau geen belangrijke voorspeller is [77]. Ook zijn er studies die juist rapporteren dat respondenten met een relatief hoge opleiding vaker slachtoffer worden [73, 80]; dit geldt vooral voor online fraude.

ZELFCONTROLE

In het huidige onderzoek is zelfcontrole een zeer belangrijke voorspeller van slachtofferschap gebleken. Zowel bij alle respondenten als bij aan fraudepogingen blootgestelde respondenten speelde zelfcontrole een belangrijke preventieve rol, voor het totaal aan fraudecategorieën en bij diverse typen fraude. Steeds gold daar dat een hogere mate van zelfcontrole leidde tot minder slachtofferschap. Dit bevestigt zo de eerdere bevindingen over zelfcontrole en fraude [85, 86] en toont dat ze ook gelden voor andere vormen fraude en ook na controle voor gelegenheid.

CYBERVEILIG GEDRAG

Gekeken naar de algemene slachtofferkans bleek dat cyberveilig gedrag een preventieve rol speelde bij schuldfraude. Onder de groep die een poging meemaakte gold dit naast schuldfraude ook voor datingfraude en phishing.

Verder speelde cyberveilig gedrag geen rol. Gezien het grote aandeel gebeurtenissen dat online plaatsvond kan dat als opvallend worden gezien. In Nederland is ook eerder gevonden dat online gedrag in het algemeen geen verband hield met slachtofferschap van phishing [87, 88].

FRAUDEKENNIS

Wanneer wordt gekeken naar de algemene slachtofferkans speelt fraudekennis geen enkele keer een significante rol. Wanneer echter wordt gekeken naar de selectie van respondenten die fraudepogingen meemaakten dan speelt fraudekennis een zeer belangrijke preventieve rol. Bij het totaal aan fraudecategorieën, en specifiek bij investeringsfraude, aankoopfraude, prijsfraude, goede-doelenfraude en vriend-in-noodfraude, verminderde fraudekennis de kans dat respondenten slachtoffer werden bij blootstelling aan fraudepogingen. Voorlichting die informeert over welke fraudevormen voorkomen zou dus zeer effectief kunnen zijn voor preventie.

Eerdere studies vonden geen relatie tussen kennis over fraude/phishing en onveilig gedrag online [89-91]. Maar deze studies vroegen niet eerst of respondenten in de gelegenheid waren om op een poging tot fraude te reageren. Een studie die wel over informatie over pogingen beschikte stelde vast dat potentiële slachtoffers veel moeite hebben om de ‘rode vlaggen’ te herkennen wanneer zij een fraudepoging tegenkomen [92]. Tenslotte, onderzoek naar de effectiviteit van interventies die het kennisniveau verbeteren liet zien dat de kans op slachtofferschap afneemt [93].

Samenvattend, kijkend naar slachtofferschap in zijn algemeen is lage zelfcontrole de belangrijkste voorspeller. Wanneer alleen naar pogingen wordt gekeken dan speelt naast zelfcontrole ook fraudekennis een belangrijke rol. Vrijwel alle type fraude hangt samen met lage zelfcontrole, met uitzondering van baanfraude, prijsfraude en identiteitsfraude. Maar ook fraudekennis speelt een rol en vermindert de kans om slachtoffer te worden bij 8 van de 12 fraudecategorieën. Tabel 1 toont een typering van de kenmerken van slachtoffers per fraudecategorie.

Tabel 1: Typering van fraudeslachtoffers (kenmerken die slachtofferkans verhogen)

	Algemene slachtofferkans	Slachtofferkans bij poging
Totaal	Jong, lage zelfcontrole	Jong, lage zelfcontrole, weinig fraudekennis
Investeringsfraude	Man, hoge opleiding, lage zelfcontrole, alleenstaand	Laag inkomen, tendens: hoge opleiding, lage zelfcontrole, alleenstaand, weinig fraudekennis
Aankoopfraude	Jong, lage zelfcontrole	Vrouw, lage zelfcontrole, weinig fraudekennis
Baanfraude	Laag inkomen	
Prijsfraude		Laag inkomen, weinig fraudekennis
Schuldfraude	Jong, lage zelfcontrole, weinig cyberveilig	Jong, lage zelfcontrole, weinig cyberveilig, alleenstaand
Goede-doelenfraude	Lage zelfcontrole	Lage zelfcontrole, weinig fraudekennis
Datingfraude	Lage zelfcontrole, alleenstaand	Tendens: lage zelfcontrole, weinig cyberveilig, alleenstaand
Vriend-in-noodfraude (o.a. Whatsapp-fraude)	Lage zelfcontrole	Lage zelfcontrole, weinig fraudekennis
Phishing	Lage zelfcontrole	Lage zelfcontrole, weinig cyberveilig, tendens: weinig fraudekennis
Identiteitsfraude	Man, laag inkomen, hoge opleiding, lage zelfcontrole	Laag inkomen
Spoofing (o.a. helpdeskfraude)	Lage zelfcontrole	Oud, lage zelfcontrole, tendens: weinig fraudekennis
Overige fraude	Lage zelfcontrole	Laag inkomen

De online bijlage bevat effectgrafieken van alle geteste risicofactoren.

3.2 Melden van fraude

3.2.1 Meldingsbereidheid

In de slachtofferstudie is gevraagd met wie slachtoffers fraudegebeurtenissen achteraf bespreken. Kijkend naar de belangrijkste slachtofferschapsgebeurtenissen, is het zo dat incidenten achteraf voornamelijk besproken worden met persoonlijke relaties (63,5%). Naast de politie (12,3%), professionele relaties (9,2%) en de bank (7%), worden gebeurtenissen achteraf met vrijwel niemand anders besproken. Per type fraude verschilt dit soms wel: zo bespreekt ruim de helft van de slachtoffers van spoofing (waaronder helpdeskfraude) dit met hun bank. 29,9% spreekt achteraf met niemand over het incident.

Kijkend naar de belangrijkste mislukte fraudepogingen wordt duidelijk dat vrijwel nooit contact wordt opgenomen met de politie: dit gebeurt in slechts 2,2% van de gevallen. Pogingen worden ook minder besproken met persoonlijke relaties: 57,5% doet dit. Net als bij slachtofferschapsgebeurtenissen worden fraudepogingen daarnaast besproken met professionele relaties (10,7%) en de bank (7%), maar verder met vrijwel niemand. Het zicht dat organisaties hebben op fraudepogingen is daarmee beperkt.

Het percentage slachtoffers dat contact opneemt met de politie is relatief laag, lager dan wat men in andere Nederlandse slachtofferstudies vindt [32]: 24% bij consumentenfraude versus 11,2% bij aankoopfraude in het huidige onderzoek, bij identiteitsfraude respectievelijk 26,3% versus 16,7%. Het is bekend dat cybercrime weinig wordt gemeld bij de politie [32]. Dat er weinig contact wordt opgenomen met de politie zou te maken kunnen hebben met de relatief kleine verliezen die de respondenten geleden hebben; uit een binaire regressieanalyse bleek dat de kans om contact op te nemen stijgt wanneer het verlies groter is.

Respondenten van de slachtofferstudie die geen contact opnamen met de politie is gevraagd waarom niet (meerdere redenen opgeven was mogelijk). 37,4% zegt dat contact met de politie toch niets zou helpen. 22,1% (meerdere redenen opgeven was mogelijk) zei simpelweg geen zin of tijd ervoor te hebben. 28,6% gaf aan dat het geen zaak was voor de politie, 21,3% vond het niet belangrijk genoeg en 19,3% zei dat er geen of weinig schade was. 5,8% gaf aan dat de schade al vergoed was en 7,5% gaf aan dat de problemen al waren opgelost. 2,8% gaf aan dat schuld of schaamte een reden waren om geen contact op te nemen met de politie. Daarnaast lukte het 2,1% niet om contact op te nemen met de politie.

ONLINE AANGEVERS

In de vragenlijst onder online aangevers van internetoplichting viel op dat relatief veel personen zonder daadwerkelijk geldverlies, die dus geen slachtoffer waren, toch aangifte deden. 56% van de respondenten was geen geld verloren. De verliezen van aangevers met geldverlies waren ten opzichte van de slachtofferstudie wel groter (gemiddeld € 1465, mediaan € 153, grootste bedrag €47.728). Dit is mogelijk verklaarbaar met de eerdergenoemde bevinding uit de slachtofferstudie dat de kans om aangifte te doen groter is als het verlies groter is.

39,6% van de respondenten uit de aangifte-vragenlijst gaf aan zelf te hebben besloten om aangifte te doen. 24,7% deed het op advies van persoonlijke relaties; 24,7% op advies van de bank; 18,9% op advies van een creditkaartmaatschappij; 19,2% op advies van de politie.

3.2.2 Verwachtingen van de politie

In de slachtofferstudie geven respondenten aan dat ze contact met de politie als overwegend positief ervaren, hoewel dat niet voor iedereen geldt (8,6% zeer slecht; 20,6% slecht; 27,4% neutraal; 38,3% goed; 5% zeer goed). Respondenten van de aangifte-vragenlijst zijn overwegend positief over het online aangiftesysteem van de politie (56,2% tevreden; 26,1% heel tevreden).

Respondenten van de slachtofferstudie die bij het belangrijkste incident nog geen uitkomst van het politiecontact hadden hebben relatief goede verwachtingen van hoe tevreden ze zullen zijn met de uitkomst (5,6% zeer ontevreden; 11,1% een beetje ontevreden; 38,5% neutraal; 26,3% een beetje tevreden; 18,4% zeer tevreden). Ook onder online aangevers zijn de meeste respondenten tevreden over de website en de wijze waarop zij aangifte konden doen.

Maar respondenten die al een uitkomst hadden zijn hier overwegend ontevreden mee (43,4% zeer ontevreden; 16% een beetje ontevreden; 4,2% neutraal; 16,9% een beetje tevreden; 19,6% zeer tevreden). Bij hen leidde het politiecontact er dan ook vrijwel nooit toe dat verloren geld terugkwam (5,4% verloren geld teruggekregen; 0% zegt dat het nog misschien kan gebeuren; 73,1% zegt dat het niet meer gaat gebeuren; bij 21,6% is geld terugkrijgen niet van toepassing). De relatief goede verwachtingen die slachtoffers hebben van de politie lijken dus maar heel beperkt te worden waargemaakt.

Ongeveer driekwart van de respondenten van de slachtofferstudie die het belangrijkste frauduleuze incident of mislukte fraudepoging rapporteerden bij de politie zou dat echter wel opnieuw doen bij een soortgelijke situatie in de toekomst (let wel: grofweg de helft van deze respondenten had nog geen uitkomst van het politiecontact). Respondenten die aangeven dat ze in de toekomst niet opnieuw contact op zouden nemen met de politie beschrijven vooral dat de politie in hun ogen toch niets doet:

> *“[De politie] doet niets met internetoplichting, behalve als er tientallen aangiften zijn”*
>
> *“Ze doen er niets mee en informeren slachtoffers gewoon helemaal niet. De aangifte ligt waarschijnlijk op die bewuste grote stapel die nooit meer wordt behandeld en uiteindelijk wordt vernietigd”*
>
> *“Er wordt toch niets meegedaan, dus [het is] de moeite niet waard”*

ONLINE AANGEVERS

In de vragenlijst onder online aangevers van internetoplichting is gevraagd wat aangevers willen bereiken met hun aangifte (meerdere redenen waren mogelijk). Interessant is dat de meeste aangevers aangifte doen om te voorkomen dat anderen slachtoffer worden (83,4%); 65,8% wil straf voor de dader(s) bereiken; 53,2% wil laten weten dat wat hen is gebeurd voorkomt. Meer praktische redenen worden ook opgegeven: 30,7% wil geld terug via opsporing van de dader(s); 6,4% doet aangifte zodat geld kan worden vergoed via de verzekering. Daarnaast doet 36,6% aangifte om zichzelf te beschermen in de toekomst.

De meeste aangevers hebben bescheiden verwachtingen ten aanzien van het bereiken van deze doelen (zie Tabel 2). Met name doelen als een ‘straf voor de dader’ en ‘geld terugkrijgen via opsporing van de dader(s)’ worden als relatief onwaarschijnlijk om te bereiken beschouwd.

Tabel 2: Doelen bij aangifte en geschatte waarschijnlijkheid dat deze bereikt worden

	% aangevers dat doel heeft	% aangevers dat doel heeft per geschatte waarschijnlijkheid dat het doel bereikt wordt	
		(Heel) onwaarschijnlijk	*(Heel) waarschijnlijk*
Anderen beschermen in de toekomst	81,2	26,3	39,1
Straf voor de dader(s)	64,1	70,9	9,6
Laten weten dat dit type misdaad voorkomt	51,8	7,7	75,5
Mijzelf beschermen in de toekomst	35,7	30,3	45,5
Geld terug via opsporing dader(s)	29,9	65,6	12,3
Geld terug via verzekering	6,3	64	16

Sommige groepen uit de aangifte-vragenlijst lijken meer te hechten aan specifieke motivaties om aangifte te doen. Onder respondenten die geld waren verloren had 66,1% als motivatie om ‘zichzelf te beschermen’, onder diegenen die geen geld waren kwijtgeraakt was dit slechts 31,4%. Andere typen van de motivatie verschilden niet aanzienlijk tussen deze twee groepen aangevers. 23,7% van de aangevers verwachtte tevreden of zeer tevreden te worden met de uiteindelijke uitkomst van de aangifte, 56,6% staat er neutraal tegenover en 19,7% verwacht ontevreden te zijn. Aangevers met geldverlies hebben wat hogere verwachtingen van de politie: 26,1% verwachtte tevreden te worden met de uitkomst; onder aangevers zonder geldverlies geldt dit voor slechts 14,5%. De aangevers zijn dus niet in alle opzichten homogeen.

Gevraagd is ook hoeveel begrip aangevers ervoor hebben dat de politie niet elke aangifte in behandeling kan nemen. 53,3% heeft hiervoor (een beetje) begrip, 29,4% heeft er geen of weinig begrip voor en 17,3% staat er neutraal tegenover.

Respondenten uit de aangifte-vragenlijst willen graag een reactie van de politie: 55,4% wil graag een ontvangstbevestiging, 66,7% hoort het graag wanneer de politie besluit het incident al dan niet te onderzoeken en 77,8% wil graag geïnformeerd worden indien de politie na onderzoek de dader(s) heeft opgespoord. Daarnaast hebben sommige slachtoffers zorgen over de veiligheid van hun telefoon en zijn ze op zoek naar informatie ten behoeve van preventie. Tenslotte zou 90,6% opnieuw aangifte doen als iets vergelijkbaars hen zou overkomen.

3.3 Impact van slachtofferschap

3.3.1 Gevolgen van fraude

Bij de meeste slachtoffers was de impact van het belangrijkste incident beperkt. Op de vraag: '*Op een schaal van 1 t/m 10, hoeveel impact heeft het incident gehad op uw leven*?' is het antwoord gemiddeld een 3. Maar 26,3% van de slachtoffers geeft aan dat de impact een vijf of meer was, voor 10,7% was de impact 7 of meer en 6,8% geeft de impact een acht of meer, hetgeen wijst op een serieuze impact. Omgerekend naar de Nederlandse bevolking van 16 jaar en ouder betekent dit dat ongeveer 156.000 mensen jaarlijks een fraude incident meemaken dat een heftige impact heeft. 15,9% geeft, voor de impact op het leven *nu*, een cijfer van een vijf of meer. Omgerekend naar de Nederlandse bevolking van 16 jaar en ouder betekent dit dat ongeveer 365.00 mensen jaarlijks een incident meemaken dat voor langere tijd een duidelijke impact heeft op hun leven.

Een relatief grote groep slachtoffers nemen het zichzelf kwalijk dat ze geld hebben verloren. Op de vraag '*In hoeverre neemt u het uzelf kwalijk dat u geld hebt verloren/betaald?'*, eveneens op een schaal van 1 tot 10, vermeldt 55,3% van de slachtoffers een 5 of meer en 22,6% antwoordt een 8 of meer.

6,6% heeft financiële problemen gekregen door het incident, waarvan 1,1% die nog steeds heeft. 14,5% heeft mentale problemen gekregen, bij 2,8% zijn die nog altijd actueel. 5,8% meldt lichamelijke klachten en bij 6,6% van de slachtoffers hebben sociale relaties geleden onder het incident.

De gevolgen van slachtofferschap zijn scheef verdeeld, waarbij een grote groep relatief weinig impact heeft ervaren, maar een significante minderheid wel serieuze problemen heeft ervaren of nog steeds ervaart.

De relatief geringe impact bij het merendeel van de slachtoffers hangt waarschijnlijk samen met de relatief lage verliezen van de gerapporteerde slachtofferschapsgebeurtenissen.

3.3.2 Hulpbehoefte van slachtoffers

In de slachtofferstudie is bij het belangrijkste frauduleuze incident gevraagd met wie slachtoffers de gebeurtenis achteraf besproken hebben of bij wie ze de gebeurtenis gemeld hebben.

Het is waarschijnlijk dat slachtoffers voor hulp grotendeels leunen op hun persoonlijke relaties (bijvoorbeeld familie en vrienden) (63,5% bespreekt het incident hiermee achteraf) en in mindere mate met ook op hun professionele relaties (bijvoorbeeld collega's) (9,2% bespreekt hiermee achteraf).

Zoals hierboven beschreven wordt hulp vooral gezocht bij de politie, waarschijnlijk voornamelijk in de vorm van een melding en/of aangifte (12,3% bespreekt achteraf met de politie). Ook bij banken (7%), creditkaartmaatschappijen (2%), betaaldiensten (1,3%), de Fraudehelpdesk (1,4%), consumentenorganisaties (0,9%) en claimorganisaties (0,3%) wordt mogelijk hulp gezocht, maar in mindere mate. Contact zoeken bij instanties verschilt sterk per type fraude. Wanneer slachtoffers contact zoeken doen zij dat het meest bij spoofing (politie: 58,8%, banken: 46,8%), identiteitsfraude (politie: 30.1%, banken: 19,2%), en bij vriend-in-nood (politie: 22,5%, banken: 15,9%). Met creditkaartmaatschappijen wordt contact gezocht bij aankoopfraude (2,8%).

Daarnaast hebben sommige slachtoffers ook achteraf contact over de gebeurtenis met juridische actoren: met een rechtsbijstandsverzekeraar (1%), een advocaat (0,8%) of het Juridisch Loket (of andere gratis rechtshulp) (0,4%). Ook dit gebeurt echter relatief weinig.

Geen enkel slachtoffer gaf aan contact te hebben opgenomen met Slachtofferhulp. Slechts 0,4% besprak de gebeurtenis met een psychologische hulpverlener; 0,2% besprak het met de huisarts. Deze cijfers geven aan dat er niet - tot geen - psychische hulp wordt gezocht door slachtoffers. Hierbij geldt wederom de kanttekening dat de verliezen en de impact, bij veel fraudes relatief klein was.

Opvallend is dat 29,9% van de slachtoffers, bijna één op de drie, de gebeurtenis achteraf met niemand bespreekt en dus ook geen enkele vorm van hulp zoekt.

4 CONCLUSIE EN AANBEVELINGEN

In het huidige onderzoek is een slachtofferstudie uitgevoerd onder een representatieve steekproef van 2864 Nederlanders van 16 jaar en ouder. Daarnaast is een vragenlijst afgenomen onder 446 personen die aangifte deden van internetoplichting via de website van de Nederlandse politie.

Samenvattend is het zo dat een aanzienlijk deel van de Nederlandse bevolking in aanraking komt met fraude. Fraude kent vele vormen en vindt voornamelijk online plaats. De verliezen door en de impact van fraude zijn meestal beperkt, maar zijn bij een significante minderheid soms wel heel groot.

Slechts weinig slachtoffers zoeken contact met de politie of andere partijen. Hier valt potentieel nog veel winst te behalen, want het is belangrijk dat slachtoffers aangifte doen. Met aangiftes kan er zicht gehouden worden op fraude, een fenomeen dat constant in ontwikkeling is. Zo blijft niet alleen de omvang van het probleem bekend maar kan er ook effectief beleid ontwikkeld worden. Ook het vaker en herhaald uitvoeren van slachtofferstudies kan hieraan bijdragen.

4.1.1 Suggesties voor de preventie van fraude

Op grond van de huidige studie bleken twee factoren van groot belang: zelfcontrole (impulsiviteit) en kennis over fraude. Uit zowel kwantitatieve als kwalitatieve gegevens bleek in dit onderzoek dat kennis over fraude helpt bij het weerstaan van fraudepogingen. Impulsiviteit is moeilijk te beïnvloeden. Maar kennis kan worden overgedragen. Daarom stellen wij voor om preventieve interventies te ontwikkelen om potentiële slachtoffers, dat wil zeggen, het Nederlandse publiek, meer en beter dan nu nog, proactief te informeren en te waarschuwen.

Op dit moment geven heel veel organisaties, zoals de Nederlandse banken, de creditkaartmaatschappijen en de politie, via hun website goede informatie over fraude. Maar dit betekent dat potentiële slachtoffers zelf actief op zoek moeten gaan naar informatie over fraude. Slachtoffers vermoeden echter meestal geen fraude, anders zouden ze er niet voor vallen, en daarom gaan ze dus meestal ook niet op zoek naar informatie. Vandaar de noodzaak om proactieve preventieve interventies te ontwikkelen om mensen alerter te maken en kennis over fraude over te brengen.

Wat zouden deze interventies kunnen zijn? Voorafgaand is het van belang om een algemeen punt ten aanzien van fraude te bespreken. Bij fraude gaat het altijd om deceptie. Maar, fraude is ook specifiek en divers: fraudevormen verschillen sterk van elkaar. Fraudeurs passen steeds andere technieken toe. Bij spoofing slagen zij er bijvoorbeeld in de suggestie te wekken dat ze bellen namens de bank van het slachtoffer; het werkelijke telefoonnummer van de bank wordt getoond. Bij phishing suggereren ze vaak een juiste afzender en een correcte link, en zijn e-mails vaak niet van echt te onderscheiden. Bij vriend-in-noodfraude proberen ze een gesprek met een vriend of een kind na te bootsen, waarbij soms heel specifieke persoonlijke details worden aangehaald. Bij investeringsfraude wordt met cijfers gegoocheld en is het handig om iets te weten over investeringen [94]. Steeds moeten potentiële slachtoffers alert zijn op iets anders. Wat effectieve interventies zijn is daarom niet makkelijk te bepalen.

Een algemene tip kan zijn, hoewel lastig, om potentiële slachtoffers te adviseren minder impulsief te handelen. Zij zouden met interventies kunnen worden gestimuleerd beslissingen minder snel te nemen en eerst een dubbele check te doen voordat ze overgaan tot een betaling.

Meer toegesneden op verschillende typen fraude is het raadzaam om informatie te verspreiden over de belangrijkste werkwijzen van fraudeurs en de werkwijzen van organisaties. Zo verwijst een aantal slachtoffers bijvoorbeeld, naar kennis over de werkwijze van banken (‘*Je bank belt je nooit op over verdachte transacties’, sectie 3.1.3).* Daarom is informatie over de daadwerkelijke procedures van organisaties ook belangrijk: bijvoorbeeld, een bank vraagt nooit om een pincode. Een goed voorbeeld van een proactieve interventie is de berichtgeving over deze onderwerpen die sommige banken regelmatig prominent in hun online bankierenapp tonen.

Uit eerder onderzoek blijkt dat informatie helpt om online fraude te voorkomen [93]. Bullee en Junger (2020) onderzochten de effectiviteit van interventies om online fraude, ofwel *social engineering*, te voorkomen [95]. Interventies werden aangeboden als training, in een gesprek; of door middel van een fysiek document. Soms was de training interactief, bijvoorbeeld wanneer gebruikers in een klaslokaal communiceren met een trainer. De inhoud van de interventies varieerde sterk: sommige trainingen gebruikten expliciete waarschuwingen, anderen meer subtiel met behulp van nudging, zoals *priming*, een impliciete waarschuwing. Uit de evaluatie bleek dat sommige interventies niet helpen, enkele interventies zelfs een averechts effect hebben en sommige interventies effectief zijn om de impact van online fraude te beperken. De ideale interventie, op basis van hun meta-analyse is een interventie waarin de volgende elementen zitten:

a) De interventie is interactief is (bijv. een spel);
b) Er is contact is met gebruikers (bijv. een les);
c) De interventie heeft een specifieke focus en behandelt één of twee concrete onderwerpen (bijv. over URL’s);
d) De interventie is intensief. Intensief betekent dat de gebruiker actief betrokken wordt in het leerproces, zoals bij een spel met vraag en antwoord.

Deze suggesties zijn handig binnen organisaties. Ook in scholen zijn dergelijke interventies goed uit te voeren en ook effectief gebleken. Aangezien jongeren vaker slachtoffer worden van fraude, is meer aandacht hiervoor van belang. Uit onderzoek van Lastdrager et al. (2017) bleek dat anti-phishing-training een positief effect heeft bij jonge kinderen [96]. In Veenendaal, bijvoorbeeld, wordt momenteel ook een interventie op scholen uitgevoerd en wetenschappelijk geëvalueerd. Wel geldt hierbij dat effecten afnemen na verloop van tijd. Regelmatige herhaling is dus van belang.

Aanvullend zou men kunnen denken aan het opzetten van grotere publiekscampagnes om burgers te informeren, via traditionele media, zoals de krant, de radio of televisie, en via sociale media. Massamediacampagnes zijn berichten die worden verspreid ten behoeve van meer bewustwording of gedragsveranderingen bij een beoogde populatie, via kanalen die een breed publiek bereiken. Deze kanalen zijn de traditionele media zoals radio, televisie, tijdschriften, billboards en kranten, maar tegenwoordig natuurlijk ook de nieuwe technologieën zoals e-mail, mobiele telefoons en interactieve websites’ [97]. Meestal proberen publiekscampagnes een integrale strategie te volgen en van meerdere media en kanalen gebruik maken.

Er is nauwelijks experimenteel onderzoek naar mediacampagnes op het terrein van online fraude [98-100]. Andere wetenschapsterreinen, zoals gezondheidscommunicatie of risicocommunicatie

kunnen wellicht nuttige informatie opleveren. Mediacampagnes kunnen zeer verschillende uitkomsten hebben: vaak positief maar soms niet-effectief en helaas zijn er soms ook averechtse effecten [97, 101-106]. De positieve effecten zijn, in het veld van de gezondheidscommunicatie, meestal bescheiden [97]. Er is nog maar weinig onderzoek gedaan naar de impact van campagnes via de nieuwe media, zoals websites, maar de eerste signalen hierover zijn positief [97]. Er zijn meerdere vereisten aan effectieve campagnes. Zo is het belangrijk om een beeld te hebben van het te bereiken publiek, en het aantal herhalingen moet voldoende zijn zodat mensen de boodschap ook onthouden [97]. Overwogen kan worden om te focussen op groepen die extra risico lopen, zoals jongeren of personen die al eens slachtoffer werden. Slachtoffers die fraude aangeven bij de politie hebben vaak behoefte aan informatie over wat hen is overkomen en tips voor preventie.

Het adequaat evalueren van interventies en van mediacampagnes is belangrijk. Zoals aangegeven zijn sommige interventies en campagnes niet effectief, en dan wordt geld verkwist; sommige interventies en campagnes beklijven niet, en dan is het belangrijk om dit te weten en herhalingen uit te voeren en sommige interventies en campagnes zijn effectief en kunnen dan wellicht breder en langduriger worden ingezet.

Met betrekking tot de opsporing: de pakkans voor fraudeurs lijkt over het algemeen zeer gering [107]. Dat is extra spijtig omdat het verhogen van de pakkans (niet de strafmaat) wel degelijk helpt om criminaliteit tegen te gaan [107, 108]. De vraag is of de politie, meer dan nu, kan onderzoeken in hoeverre, al dan niet geautomatiseerd, meer kan worden gedaan om fraudeurs op te sporen. Sommige aangevers van fraude leveren in het meldingssysteem informatie over daders, zoals telefoonnummers, die de politie mogelijk zou kunnen benutten. Ook kan worden gecheckt of de communicatie met slachtoffers wellicht beter kan worden geregeld. Of slachtoffers geld terugkrijgen ligt meestal niet in de macht van de politie.

Vermeldenswaardig is een pilot die de politie recent heeft uitgevoerd, waarbij fraudeurs direct aansprakelijk werden gehouden voor de schade via een alternatieve privaatrechtelijke procedure waarbij slachtoffers hun schade konden verhalen op daders. Verwachtingen van slachtoffers werden daarbij in grote mate waargemaakt en het vertrouwen in de politie steeg, zonder dat de strafrechtketen extra werd belast.

Tenslotte kunnen organisaties die via hun klanten betrokken zijn bij slachtofferschap van fraude, wellicht extra maatregelen nemen om fraude te bestrijden. Technische maatregelen die acties van fraudeurs onmogelijk maken zijn vaak de beste manier om fraude te voorkomen [109, 110]. Zo is bekend dat prepaid telefoonkaarten fraude gemakkelijk maken om uit te voeren.
Het standaard verlagen van limieten en alleen op verzoek van de klant (tijdelijk) verhogen zou helpen om potentiële verliezen te beperken. Ook de tijdsduur die verstrijkt voordat een limiet wordt verhoogd werkt in het nadeel van de fraudeur. Verder is het gebruik maken van de IBAN Naam check[8] ook altijd te adviseren. Deze naam check geeft een waarschuwing wanneer de naam en het rekeningnummer van een bankrekening niet overeenkomen. Deze werkt nu ook bij Tikkie. Hiermee kan men altijd zien aan wie het geld wordt overgemaakt, binnen Nederland. En dat is wat veel criminelen ook zeggen tegen de klant: ‘U kunt de waarschuwing negeren’.
Ook gedacht kan worden aan technische maatregelen die slachtoffers net voor het voltooien van een betaling waarschuwen, of die een verdachte transactie ophouden voor nader onderzoek. Financiële dienstverleners zouden, al dan niet op verzoek van de klant, limieten of vertragingen in kunnen stellen. Risicogroepen, zoals mensen die al eens slachtoffer zijn geworden, zouden

[8] Zie: https://www.betaalvereniging.nl/betaalproducten-en-diensten/iban/iban-naam-check/

hiervoor proactief benaderd kunnen worden. Dergelijke vertragingen kunnen bij veel typen fraude helpen.

Als samenleving als geheel kunnen wij tenslotte nadenken over in hoeverre mensen online anoniem kunnen zijn.

5 REFERENTIES

1. Crawford, T.A.M. and K. Evans, *Crime prevention and community safety*, in *Oxford Handbook of Criminology*, A. Leibling, S. Maruna, and L. McAra, Editors. 2016, Oxford University Press: Oxford, UK.
2. Pain, R., *Place, social relations and the fear of crime: a review.* Progress in Human Geography, 2000. **24**(3): p. 365-387.
3. Hough, M. and J.V. Robert, *Public Opinion and Criminal Justice: The British Crime Survey and Beyond*, in *Surveying crime in the 21st century: commemorating the 25th anniversaryof the British crime survey*, J. Hough and M. Maxfield, Editors. 2007, Criminal Justice Press: Monsey, NY. p. 197-220.
4. de Jong, J., *Het mysterie van de verdwenen criminaliteit (The mystery of the disappeared crime)*. 2018, Statistics Netherlands (CBS): The Hague, Netherlands.
5. Blumstein, A. and J. Wallman, *The crime drop in America*. 2005, Cambridge, UK: Cambridge University Press.
6. Farrell, G., *Five tests for a theory of the crime drop.* Crime Science, 2013. **2**(1): p. 1-8.
7. Hopkins, M., *The crime drop and the changing face of commercial victimization: Reflections on the 'commercial crime drop' in the UK and the implications for future research.* Criminology & Criminal Justice, 2016. **16**(4): p. 410-430.
8. Statistics Netherlands. *Geregistreerde criminaliteit; regio (indeling 2013) 2005-2012*. 2018 Geregistreerde criminaliteit; regio (indeling 2013) 2005-2012 [cited 2018 September 3, 2014]; Available from: http://statline.cbs.nl/Statweb/publication/?DM=SLNL&PA=80344NED&D1=0&D2=a&D3=0&D4=a&HDR=G2,T,G3&STB=G1&VW=T.
9. Finklea, K.M., *Identity theft: Trends and issues*. 2014, Washington DC, USA: Congressional Research Service. Report prepared for Members and Committees of Congress.
10. Javelin, *2014 Identity fraud report: card data breaches and inadequate consumer password habits fuel disturbing fraud trends*. 2014, Javelin Research & Strategy. https://www.javelinstrategy.com/uploads/web_brochure/1405.R_2014IdentityFraudReportBrochure.pdf: Pleasanton, CA.
11. Financial Action Fraud UK, *Fraud The facts 2017. The definitive overview of payment industry fraud*. 2017, Financial Action Fraud UK,: London, UK.
12. Kemp, S., F. Miró-Llinares, and A. Moneva, *The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain.* European Journal on Criminal Policy and Research, 2020. **26**(3): p. 293-312.
13. PWC, *Pulling fraud out of the shadows. Global Economic Crime and Fraud Survey 2018*, P.W. Coopers, Editor. 2018: USA.
14. Sutton, M., *Improving national crime surveys with a focus on fraud, high-tech crimes, and stolen goods*, in *Surveying crime in the 21st century: commemorating the 25th anniversaryof the British crime survey*, J. Hough and M. Maxfield, Editors. 2007, Criminal Justice Press: Monsey, NY. p. 243-262.
15. Montoya, L., M. Junger, and P. Hartel *How 'Digital' is Traditional Crime?* European Intelligence and Security Informatics Conference (EISIC) 2013, 2013. 31-37.
16. Statistics Netherlands. *Cybercrime achterhalen in aangiften*. Webmagazine 2019 31 juli, 2010.
17. National Crime Agency (NCA), *Cyber Crime Assessment 2016*. 2016: http://www.nationalcrimeagency.gov.uk/publications/709-cyber-crime-assessment-2016/file.
18. National Academies of Sciences, E., and Medicine (NAP),, *Modernizing Crime Statistics: Report 2-New Systems for Measuring Crime*. 2018, Washington, DC, USA: The National Academies Press.
19. Piquero, N.L. and M.L. Benson, *White-Collar Crime and Criminal Careers: Specifying a Trajectory of Punctuated Situational Offending.* Journal of Contemporary Criminal Justice, 2004. **20**(2): p. 148-165.

20. Simpson, S.S., *Making sense of white-collar crime: Theory and research.* Ohio St. J. Crim. L., 2010. **8**: p. 481.
21. Bloem, B. and A. Harteveld, *Horizontale fraude: verslag van een onderzoek voor het Nationaal dreigingsbeeld 2012*. 2012, Zoetermeer, Nl.: Dienst IPOL. 184.
22. Verhoeven, W.-J., *Review Fraude in Beeld.* Tijdschrift voor Criminologie, 2008. **50**: p. 158-162.
23. Elffers, H., *Eerste schetskaart fraude door fraudologische avonturiers.* Tijdschrift voor criminologie, 2008. **51**(2): p. 6.
24. Platform Bijzondere Opsporingsdiensten, *Fraude in Beeld. Deel II. Verantwoording, resultaten en implicaties*. 2007, Den Haag, nL.: Ministerie van Sociale Zaken en Werkgelegenheid
25. Leukfeldt, E.R. and W. Stol, *De marktplaatsfraudeur ontmaskerd. Internetfraudeurs vergeleken met klassieke fraudeurs.* Secondant, 2011. **25**(6): p. 26-31.
26. Jansen, J., et al., *Offenders in a digitized society*, in *Cybercrime and the Police*, W.P. Stol and J. Jansen, Editors. 2013, Eleven International Publishing: The Hague, Nl. p. 45-59.
27. Akkermans, M., et al., *Veiligheidsmonitor 2021 (the safety monitor 2021)*. 2022, Centraal Bureau voor de Statistiek (Statistics Netherlands): Den Haag, Nl.
28. Bregant, J. and R. Bregant, *Cybercrime and Computer Crime*, in *The Encyclopedia of Criminology and Criminal Justice*. 2014, Blackwell Publishing Ltd.
29. UNODC, *Comprehensive study on cybercrime. Draft - February 2013*. 2013, UNODC. Organized crime branch, Division for treaty affairs: Vienna, Austria.
30. Reyns, B.W., B. Henson, and B.S. Fisher, *Cybercrime*, in *The Encyclopedia of Theoretical Criminology*. 2014, John Wiley & Sons, Ltd.
31. Wall, D.S., *Cybercrime: The transformation of crime in the information age*. 2007, Cambridge, UK: Polity press. 276.
32. van de Weijer, S.G., E.R. Leukfeldt, and W. Bernasco, *Determinants of reporting cybercrime: A comparison between identity theft, consumer fraud, and hacking.* European Journal of Criminology, 2018: p. 1477370818773610.
33. Spanos, G. and L. Angelis, *The impact of information security events to the stock market: A systematic literature review.* Computers & Security, 2016. **58**: p. 216-229.
34. Stol, W., *Cyberspace and safety*, in *Cyber Safety: an introduction*, R. Leukfeldt and W. Stol, Editors. 2012, Eleven: The Hague, The Netherlands. p. 19-30.
35. Stol, W., E.R. Leukfeldt, and H. Klap, *Cybercrime en politie; een schets van de Nederlandse situatie anno 2012.* Justitiële Verkenningen, 2012. **38**(1): p. 25-39.
36. Anderson, R.J., et al., *Measuring the cost of cybercrime*, in *The Economics of Information Security and Privacy*. 2013, Springer. p. 265-300.
37. Lone, S., N. Harboul, and J. Weltevreden, *2021 European E-commerce Report.* 2021.
38. Betaal Vereniging Nederland, *Factsheet betalingsverkeer 2020 (facts and figures on the dutch payment system in 2020)*. 2021.
39. Betaalvereniging Nederland. *Nederlanders deden ruim kwart meer online aankopen in 2020 (The Dutch made more than a quarter more online purchases in 2020)*. 11 March 2021 [cited 10 Janurary 2021; Available from: https://www.betaalvereniging.nl/actueel/nieuws/nederlanders-deden-ruim-kwart-meer-online-aankopen-in-2020/.
40. CBS. *11 procent meer internetaankopen in eerste helft 2020*. 15 January 2021; Available from: https://www.cbs.nl/nl-nl/nieuws/2021/02/11-procent-meer-internetaankopen-in-eerste-helft-2020.
41. Haas, M.d., M. Hamersma, and R. Faber, *Thuiswerken tijdens en na de coronacrisis. Een overzicht van drie metingen met het Mobiliteitspanel Nederland (MPN)*. 2021, Kennisinstituut voor Mobiliteitsbeleid.
42. Curry, D. *Microsoft Teams Revenue and Usage Statistics (2021)*. 11 November, 2021; Available from: https://www.businessofapps.com/data/microsoft-teams-statistics/.
43. Iqbal, M. *Zoom Revenue and Usage Statistics (2021)*. 11 November, 2021; Available from: https://www.businessofapps.com/data/zoom-statistics/.
44. CentERdata. *About the panel*. 2021; Available from: https://www.lissdata.nl/about-panel.
45. Brüggen, E., J.A.v.d. Brakel, and J. Krosnick, *Establishing the accuracy of online panels for survey research*, S.N. (CBS), Editor. 2016: The Hague, Nl.
46. De Vos, K., *Representativeness of the LISS-panel 2008, 2009, 2010*. 2010, CentERdata: Tilburg, Nl.

47. Eckman, S., *Does the inclusion of non-internet households in a web panel reduce coverage bias?* Social Science Computer Review, 2016. **34**(1): p. 41-58.
48. Scherpenzeel, A.C. and J.G. Bethlehem, *How Representative are Online Panels? Problems of Coverage and Selection and Possible Solutions*, in *Social and Behavioral Research and the Internet: Advances in Applied Methods and Research Strategies*, M. Das, P. Ester, and L. Kaczmirek, Editors. 2011, Routledge: New York, NY.
49. DeLiema, M., G.R. Mottola, and M. Deevy, *Findings from a pilot study to measure financial fraud in the United States.* Available at SSRN 2914560, 2017.
50. Titus, R.M., F. Heinzelmann, and J.M. Boyle, *Victimization of Persons by Fraud.* Crime & Delinquency, 1995. **41**(1): p. 54-72.
51. Statistics Netherlands, *Veiligheidsmonitor 2019*. 2020, Centraal Bureau voor de Statistiek (Statistics Netherlands): Den Haag, Nl. p. 113.
52. Näsi, M.J., *National experiences in cybercrime surveys: Finland*, in *Measuring cybercrime in the time of covid-19: The role of crime and criminal justice stat*. 2020: Virtual Strasbourg 2020.
53. Dickman, S.J., *Functional and dysfunctional impulsivity: personality and cognitive correlates.* Journal of personality and social psychology, 1990. **58**(1): p. 95.
54. Domenie, M.M.L., et al., *Slachtofferschap in een gedigitaliseerde samenleving. Een onderzoek onder burgers naar e-fraude, hacken en ander veel voorkomende criminaliteit (Victimization in a digitized society. A survey of citizens to e-fraud, hacking and other common crime)*. 2013, Den Haag, Nl.: Boom Lemma.
55. Statistics Netherlands, *Digitale Veiligheid & Criminaliteit 2018 (Online safety & crime 2018)*. 2019, Centraal Bureau voor de Statistiek (Statistics Netherlands): Den Haag, Nl. p. 120.
56. DeLiema, M., et al., *Exposed to Scams: What Separates Victims from Non-victims?* 2019, Stanford Center on Longevity: Stanford, CA.
57. CBS. *Bevolking op eerste van de aand; geslacht, leeftijd, migratieachtergrond (Population on the first of the month; gender, age, migration background)*. 31 januari 2022; Available from: https://opendata.cbs.nl/#/CBS/nl/dataset/83482NED/table?ts=1644156988138https:%2F%2Fwww.e-education.psu.edu%2Fstyleforstudents%2Fc5_p12.html.
58. Goede, M.S.v.t.H.-d. and E.R. Leukfeldt, *WhatsApp-fraude in Nederland (WhatsApp fraud in the Netherlands)*. 2021, De Haagse Hogeschool: The Hague, Nl.
59. Laan, J., Abhishta, and M. Junger, *The impact of the Covid-19 on phishing frequency and content.* work in progress.
60. Chigada, J. and R. Madzinga, *Cyberattacks and threats during COVID-19: A systematic literature review.* South African Journal of Information Management, 2021. **23**(1): p. 1-11.
61. Coman, I. and I.C. Mihai, *The Impact of COVID-19. Cybercrime and Cyberthreats.* European Law Enforcement Research Bulletin, 2021(SCE 5): p. tbd-tbd.
62. Kemp, S., et al., *Empty streets, busy internet: A time-series analysis of cybercrime and fraud trends during COVID-19.* Journal of Contemporary Criminal Justice, 2021: p. 10439862211027986.
63. Sjouwerman, S. *Douane ziet meer namaakartikelen door coronacrisis: 'Niet alleen van AliExpress' (Customs sees more counterfeit items due to the corona crisis: 'Not just from AliExpress')*. 20 August, 2021 20 August, 2021]; Available from: https://nos.nl/artikel/2394571-douane-ziet-meer-namaakartikelen-door-coronacrisis-niet-alleen-van-aliexpress.
64. Naidoo, R., *A multi-level influence model of COVID-19 themed cybercrime.* European Journal of Information Systems, 2020. **29**(3): p. 306-321.
65. Buil-Gil, D., et al., *Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK.* European Societies, 2020: p. 1-13.
66. Lallie, H.S., et al., *Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic.* arXiv preprint arXiv:2006.11929, 2020.
67. APWG. *Trend reports. 1st Quarter 2020 plus COVID-19 coverage*. 2020 22 August 2020]; Available from: http://www.antiphishing.org/trendsreports/.
68. Beals, M.E., M. DeLiema, and M. Deevy, *Framework for a taxonomy of fraud*. 2015, Stanford Longevity Center/FINRA Financial Investor Education Foundation/Fraud Research Center: Washington DC, USA. p. 2016.

69. Deevy, M., S. Lucich, and M.E. Beals, *Scams, schemes & swindles. A review of consumer financial fraud research*. 2012, Fraud Research Center: Stanford, CA. p. 47.
70. Deevy, M. and M.E. Beals, *The scope of the problem an overview of fraud prevalence measurement*. 2013, Fraud Research Center. Retrieved from: http://fraudresearchcenter.org/wp-content/uploads/2013/11/Scope-of-the-Problem-FINAL.pdf: Stanford, CA. p. 46.
71. Beals, M.E., et al., *How Does Survey Context Impact Self-reported Fraud Victimization?* The Gerontologist, 2015. **57**(2): p. 329-340.
72. Geldrop, A.v. and T.d. Vries. *Fraude loont...Nog steeds*. 2012. Enschede, Nl.: Stichting Toekomst der Techniek. Universiteit Twente.
73. ONS. *Nature of fraud and computer misuse in England and Wales: year ending March 2019*. 19 March 2020 5 August, 2021]; Available from: https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/articles/natureoffraudandcomputermisuseinenglandandwales/yearendingmarch2019.
74. Bullée, J.-W. and M. Junger, *Social Engineering*, in *Palgrave International Handbook of Cybercrime and Cyberdeviance*, T.J. Holt and A.M. Bossler, Editors. 2020, Palgrave Macmillan: Cham, Switserland. p. 849-875.
75. Bullée, J.-W., et al., *Spear phishing in organisations explained.* Information and Computer Security, 2017.
76. Chen, J.Y., *Guilty of indigence: The urban poor in China, 1900-1953*. Guilty of Indigence: The Urban Poor in China, 1900-1953. 2012. 1-309.
77. Anderson, K.B., *Mass-Market Consumer Fraud in the United States: A 2017 Update*. 2019, Staff Report of the Bureau of Economics, Federal Trade Commission: Washington, DC.
78. Heartfield, R., G. Loukas, and D. Gan, *You are probably not the weakest link: Towards practical prediction of susceptibility to semantic social engineering attacks.* IEEE Access, 2016. **4**: p. 6910-6928.
79. Johansson, F., *The Medici Effect, with a new preface and discussion guide: what elephants and epidemics can teach us about innovation*. 2017: Harvard Business Review Press.
80. Burnes, D., M. DeLiema, and L. Langton, *Risk and protective factors of identity theft victimization in the United States.* Preventive medicine reports, 2020. **17**: p. 101058.
81. Dickens, W.T. and J.R. Flynn, *Heritability Estimates Versus Large Environmental Effects: The IQ Paradox Resolved.* Psychological Review, 2001. **108**(2): p. 346.
82. Anthony, T., *Indigenous people, crime and punishment*. Indigenous People, Crime and Punishment. 2013. 1-248.
83. Harrell, E., *Victims Of Identity Theft, 2018*. 2021, Bureau of Justice Statistics, US. https://www.ojp.gov/library/publications/victims-identity-theft-2018: Washington DC.
84. Anderson, C.L. and R. Agarwal, *Practicing safe computing: A multimethod empirical examination of home computer user security behavioral intentions.* MIS Quarterly: Management Information Systems, 2010. **34**(SPEC. ISSUE 3): p. 613-643.
85. Fernández-Alemán, J.L., et al., *Security and privacy in electronic health records: A systematic literature review.* Journal of Biomedical Informatics, 2013. **46**(3): p. 541-562.
86. Wilsem, J.v., *Worlds tied together? Online and non-domestic routine activities and their impact on digital and traditional threat victimization.* European Journal of Criminology, 2011. **8**(2): p. 115-127.
87. Leukfeldt, E.R., *Phishing for suitable targets in the Netherlands: routine activity theory and phishing victimization.* Cyberpsychology, behavior and social networking, 2014. **17**(8): p. 551-5.
88. Leukfeldt, E.R. and M. Yar, *Applying routine activity theory to cybercrime: A theoretical and empirical analysis.* Deviant Behavior, 2016. **37**(3): p. 263-280.
89. Holt, T.J., G.W. Burruss, and A.M. Bossler, *Assessing the macro-level correlates of malware infections using a routine activities framework.* International journal of offender therapy and comparative criminology, 2018. **62**(6): p. 1720-1741.
90. Leukfeldt, E.R., R. Notté, and M. Malsch, *Slachtofferschap van online criminaliteit.* Een onderzoek naar behoeften, gevolgen en verantwoordlijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit, 2018.
91. van 't Hoff-de Goede, S., et al., *Hoe veilig gedragen wij ons online? Een studie naar de samenhang tussen kennis, gelegenheid, motivatie en online gedrag van Nederlanders*. 2019, The

Hague, Nl.: Centre of Expertise Cybersecurity, De Haagse Hogeschool & Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR). 170.
92. FINRA, *Financial fraud and fraud susceptibility in the United States. Research report from a 2012 national survey*. 2013, FINRA Investor education foundation: New York, NY.
93. Bullee, J.-W. and M. Junger, *How effective are social engineering interventions? A meta-analysis.* Information & Computer Security, 2020. **28**(5): p. 801-830.
94. Engels, C., K. Kumar, and D. Philip, *Financial literacy and fraud detection.* The European Journal of Finance, 2020. **26**(4-5): p. 420-442.
95. Bullée, J.-W. and M. Junger, *Social engineering: digitale fraude en misleiding.* Justitiele Verkenningen, 2020. **46**(2).
96. Lastdrager, E., et al. *How Effective is Anti-Phishing Training for Children?* in *SOUPS, Symposium On Usable Privacy and Security*. 2017. Santa Clara, California.
97. Abroms, L.C. and E.W. Maibach, *The effectiveness of mass communication to change public behavior.* Annu. Rev. Public Health, 2008. **29**: p. 219-234.
98. Nurse, J.R., *Cybersecurity Awareness.* arXiv preprint arXiv:2103.00474, 2021.
99. Briggs, P., D. Jeske, and L. Coventry, *Chapter 6 - Behavior Change Interventions for Cybersecurity A2 - Little, Linda*, in *Behavior Change Research and Theory*, E. Sillence and A. Joinson, Editors. 2017, Academic Press: San Diego. p. 115-136.
100. Brewer, R., et al., *Universal Communication Strategies*, in *Cybercrime Prevention*. 2019, Springer. p. 35-48.
101. McMakin, A.H. and R.E. Lundgren, *Risk communication: A handbook for communicating environmental, safety, and health risks*. 2018: John Wiley & Sons.
102. Friedman, A.L., et al., *Health communication and social marketing campaigns for sexually transmitted disease prevention and control.* Sexually transmitted diseases, 2016. **43**: p. S83-S101.
103. Freeman, B., et al., *Social media campaigns that make a difference: what can public health learn from the corporate sector and other social change marketers.* Public Health Res Pract, 2015. **25**(2): p. e2521517.
104. Shi, J., T. Poorisat, and C.T. Salmon, *The use of social networking sites (SNSs) in health communication campaigns: review and recommendations.* Health communication, 2018. **33**(1): p. 49-56.
105. Harrington, N.G., P.C. Palmgreen, and L. Donohew, *Programmatic research to increase the effectiveness of health communication campaigns.* Journal of health communication, 2014. **19**(12): p. 1472-1480.
106. Nurse, J.R. *Effective communication of cyber security risks*. in *7th International Scientific Conference on Security and Protection of Information (SPI 2013)*. 2013. Citeseer.
107. Tromp, N., et al., *Preventieve maatregelen horizontale fraude (Preventive measures against horizontal (B2B) fraud)*. 2010, Intraval: Groningen/Rotterdam, Nl. p. 112.
108. Clarke, R.V., *Situational crime prevention*, in *Environmental Criminology and Crime Analysis*, R. Wortley and L. Mazerolle, Editors. 2008, Willan: London, UK. p. 178-194.
109. Hartel, P., M. Junger, and R. Wieringa, *Cyber-crime science= crime science+ information security*. 2010, University of Twente. http://eprints.eemcs.utwente.nl/18500/: Enschede, Nl.
110. Warkentin, M. and R. Willison, *Behavioral and policy issues in information systems security: the insider threat.* European Journal of Information Systems, 2009. **18**: p. 101–105.
111. Tourangeau, R. and M.E. McNeeley, *Measuring crime and crime victimization: Methodological issues*, in *Measurement problems in criminal research: Workshop summary*, J.V. Pepper and C.V. Petrie, Editors. 2003, The National Academies Press: Washington, DC. p. 10-42.
112. Kruttschnitt, C., W.D. Kalsbeek, and C.C. House, *Estimating the incidence of rape and sexual assault.* 2014.
113. Schneider, A.L., *Methodological problems in victim surveys and their implications for research in victimology.* The Journal of Criminal Law and Criminology (1973-), 1981. **72**(2): p. 818-838.
114. Daigle, L.E., J.A. Snyder, and B.S. Fisher, *Measuring victimization: Issues and new directions.* The handbook of measurement issues in criminology and criminal justice, 2016: p. 249.
115. Schneider, A.L., *Methodological Problems in Victim Surveys and their Implications for Research in Victimology*, in *The Fear of Crime*. 2017, Routledge. p. 331-351.

116. Schneider, A.L. and D. Sumi, *Patterns of forgetting and telescoping: An analysis of LEAA survey victimization data.* Criminology, 1981. **19**(3): p. 400-410.
117. Elffers, H. and M. Averdijk, *Aangeven aan te geven.* Leiden: Nederlands Studiecentrum Criminaliteit en Rechtshandhaving, 2007.
118. Reep, C., *Fraude met online handel. Antwoorden uit de Veiligheidsmonitor vergeleken met het politieregister (Online trading fraud. Information from the Security Monitor compared with the Police Register)*, in *Methodologie paper*. 2017, Statistics Netherlands: Den Haag, Nl.
119. Reep, C., *Responsgedrag bij de Veiligheidsmonitor (in Dutch)(Response Behavior in the Safety Monitor)*, in *Methodology paper*. 2013, Statistics Netherlands. Available at: https://www.cbs.nl/nl-nl/achtergrond/2017/15/responsgedrag-bij-de-veiligheidsmonitor: Heerlen, Nl.
120. Dijk, J.v., J.v. Kesteren, and P. Smit, *Criminal victimisation in international perspective*. 2007: Boom Juridische Uitgevers.
121. Morgan, R.E., *Financial Fraud in the United States, 2017*, U.S.D.o.J.O.o.J. Programs, Editor. 2021, Bureau of Justice Statistics: Washington DC.
122. Lea, S., P. Fischer, and K. Evans, *The psychology of scams: Provoking and committing errors of judgement*. 2009: Prepared for the Office of Fair Trading by the University of Exeter school University of Exeter, School of Psychology.

6 BIJLAGE

6.1 Bijlage 1: Reflectie op methodologie van de slachtofferstudie

Het meten van de prevalentie van fraude is een uitdaging: fraude is een dynamisch fenomeen dat op verschillende manieren gedefinieerd kan worden. Fraudeurs zijn innovatief en ontwikkelen constant nieuwe manieren om slachtoffers geld afhandig te maken. Onderzoekers hebben verschillende fraudetaxonomieën ontwikkeld die zowel raakvlakken als verschillen kennen. Subtiele methodologische keuzes kunnen substantiële invloed hebben op de resultaten van een slachtofferstudie.

De methodologie van de huidige studie is grotendeels gebaseerd op de in de VS uitgevoerde pilot studie [49]. Reeds is beschreven hoe de resultaten van de huidige studie daarvan afwijken en welke verklaringen hiervoor zijn; het slachtofferpercentage voor verschillende fraudevormen lag in de huidige studie bijna een factor 10 lager. Dat maakt het dat verscheidene vervolgvragen, die verdere selecties maakten, beantwoord zijn door beperkte aantallen respondenten wat het generaliseren van sommige uitkomsten bemoeilijkt. Enkele regressieanalyses specifiek voor bepaalde fraudecategorieën konden niet worden uitgevoerd of kennen beperkte statistische kracht, waardoor mogelijk wel-bestaande effecten niet gevonden zijn. Daar tegenover staat dat de gevonden slachtofferpercentages, één van de belangrijke doelen van de huidige studie, wel nauwkeurigheid kennen: de betrouwbaarheidsintervallen zijn betrekkelijk klein. Het gebruik van het LISS-panel, met een hoog responspercentage (79%), zorgt voor goede representativiteit van de Nederlandse bevolking. Verschillende uitkomsten van de regressieanalyses zijn daarnaast sterk significant ($p < .01$ en $p < .001$), bijvoorbeeld het effect van zelfcontrole op slachtofferschap.

Een bekend probleem van slachtofferstudies zijn classificatiefouten [111]. Verschillende studies, zoals de Amerikaanse National Crime Victimisation Survey (NCVS), corrigeren classificatiefouten door middel van een uitgebreide controle op de antwoorden [112]. Ook in de huidige studie is dit gedaan. Bewust is de huidige opzet gekozen voor screeningsvragen met een niet-limiterende vraagstelling, waarbij relatief brede categoriedefinities (aangevuld met enkele specifieke voorbeelden) werden voorgelegd aan respondenten. Dit zorgt ervoor dat fraude integraal kan worden gemeten, waarbij geen fraudevormen worden gemist die misschien nog niet op de radar staan. De keerzijde hiervan is echter dat het voor slachtoffers moeilijker kan zijn om wat hen gebeurd is te herkennen in de gestelde vragen. Na inspectie van de gegevens die de huidige studie opleverde bleek dat het geregeld gebeurde dat slachtoffers een gebeurtenis rapporteerden die niet consistent was met de definitie van de categorie waaronder zij dit deden. Opvallend was bijvoorbeeld dat vrijwel alle gebeurtenissen die werden gerapporteerd onder de overige fraude-categorie eigenlijk vielen onder andere fraudevormen van de taxonomie. Het was daarom nodig om de antwoorden van elke gerapporteerde gebeurtenis te controleren en soms gebeurtenissen te her-categoriseren of te verwijderen. Uiteindelijk zou dit tot een nauwkeurigere schatting moeten leiden, maar er komt wel enige subjectiviteit bij deze methode kijken.

Daarnaast zijn er andere aspecten van slachtofferstudies die de resultaten kunnen beïnvloeden, waaronder:

- *Terugroepperiode*. Sommige slachtofferstudies, zoals de NCVS, gebruiken een terugroepperiode van zes maanden, en de meeste studies, zoals de huidige, gebruiken een terugroepperiode van een jaar. Beide hebben voor- en nadelen [111]. Het vergeten van incidenten lijkt vergelijkbaar bij een periode van 6 en 12 maanden [113]. De huidige studie gebruikte een terugroepperiode van 12 maanden.

- *Context*. De presentatie van een vragenlijst, inclusief de aankondigingsbrief, de inleiding en zelfs de naam van de studie, geeft informatie aan de respondent over het onderwerp en bepaalt mede de interpretatie van individuele vragen [111]. Ook beïnvloeden voorgaande vragen in de enquête wat respondenten denken, hoe ze vragen begrijpen en wat ze op latere vragen antwoorden [111]. Met betrekking tot fraude blijkt uit onderzoek dat het belangrijk is om de criminele context niet te benadrukken. Door gebruik van het woord 'fraude', dat een juridische connotatie heeft, te vermijden wordt de rapportage nauwkeuriger [71]. Veel respondenten associëren wat hen is overkomen niet met fraude. Ook zou de onderzoeker, bij het gebruik van ‘fraude’ het aan de respondent overlaten om te definiëren wat fraude is [70, 71]. Het huidige onderzoek heeft het woord ‘fraude’ daarom niet gebruikt.

- *Geheugentriggers*. De wijze waarop vragen worden geformuleerd kan het geheugen triggeren en gebeurtenissen oprakelen. Vragen over meerdere concrete items verduidelijken waar de onderzoeker in is geïnteresseerd en zorgen voor betere herinnering hiervan. Het benoemen van items werkt als een geheugensteun en leidt tot het rapporteren van meer incidenten [111, 112]. In het huidige onderzoek zijn daarom vragen gesteld over 11 specifieke typen fraude (met daarnaast een ‘overige’-categorie).

- *Telescopische problemen*. Respondenten hebben vaak moeite om zich de correcte datum van incidenten te herinneren [111, 114-116]. Ze kunnen bijvoorbeeld ten onrechte denken dat het incident buiten de terugroepperiode heeft plaatsgevonden; *backwards telescoping*. Respondenten kunnen ook ten onrechte een incident dat langer geleden heeft plaatsgevonden binnen de terugroepperiode plaatsen; *forward telescoping*.

- Forward telescoping kan aanzienlijk zijn [113, 116-118]. Een studie die informatie van slachtoffers over incidenten die aan de politie waren gemeld, vergeleek met daadwerkelijke door de politie geregistreerde incidenten, vond percentages van voorwaartse telescopen van ongeveer 30% [118]. In een soortgelijk onderzoek vond [113, 116] voorwaartse telescopische percentages tot 25%.

- Een screeningsvraag van vijf jaar helpt ook bij het herinneren en wordt gebruikt om respondenten in staat te stellen relatief recente incidenten te melden, maar ze niet vooruit te schuiven in de rapportageperiode [111, 118] en dit systeem werd gebruikt in het huidige onderzoek.

- *Zelftoediening*. Bij zelftoediening worden vragenlijsten zelfstandig door respondenten ingevuld, zonder de aanwezigheid van onderzoekers. Bij gevoelige vragen kan zelftoediening voor hogere cijfers zorgen, mogelijk omdat er meer anonimiteit wordt ervaren door de respondent [111]. De aanwezigheid van gezinsleden lijkt weinig invloed te hebben op de antwoorden van respondenten [111]. De huidige studie paste zelftoediening toe.

- *Type incident*. Eerder onderzoek [118] bestudeerde slachtofferschap van fraude door online winkelen en vergeleek gegevens uit de Nederlandse Veiligheidsmonitor met politiegegevens. Ze constateert ook dat incidenten vaker worden gemeld als ze recenter zijn gebeurd en grote financiële verliezen met zich meebrengen. Reep [119] merkte op dat de aangifte van door de politie geregistreerde incidenten veel hoger is voor fraude dan voor andere vormen van misdaad.

Het geheel overziend zou de huidige studie de best mogelijke schatting van het percentage slachtoffers van fraude in Nederland moeten zijn, gegeven dat er altijd een zekere foutmarge is. Hoe omvangrijk die foutmarge is, is echter lastig in te schatten.

6.2 Bijlage 2: Vergelijking uitkomsten slachtofferstudie met de Verenigde Staten

De huidige vragenlijst is gebaseerd op een Amerikaanse pilot [49], die zich richtte op fraude in de periode van 26 april 2015 t/m 3 mei 2016. In dat onderzoek zijn de percentages aanzienlijk hoger dan in de huidige studie, ondanks het feit dat de vraagstelling nagenoeg hetzelfde is; 50,4% van de respondenten was daar slachtoffer van de fraudecategorieën samen (versus 15,7% in het huidige onderzoek).

Ook voor specifieke fraudevormen zijn de huidige cijfers in vergelijking met de Amerikaanse pilot een stuk lager. Zij vonden voor de meeste fraudevormen slachtofferschap van grofweg 10% (met 16,5% voor investeringsfraude en 42,6% voor aankoopfraude) [49]. Dat is ongeveer een factor 10 hoger dan de cijfers uit de huidige studie. Voor de verschillen tussen de Amerikaanse pilot en het huidige onderzoek zijn enkele mogelijke verklaringen:

- De bevolking van de VS is simpelweg vaker slachtoffer van fraude dan de Nederlandse bevolking. De *International Crime Victim Survey* (ICVS) [120] ondersteunt dit; voor sommige criminaliteitsvormen werden in het verleden ook verschillen van een factor 10 gevonden. Het is daarom plausibel dat de gevonden verschillen voor een belangrijk deel het resultaat zijn van een reëel verschil tussen de VS en Nederland. Ook een eerdere Amerikaanse studie vond zeer hoge percentages voor pogingen tot fraude: 84% van de respondenten van 40 jaar en ouder, gaf aan ooit te zijn benaderd met ten minste één van de 11 soorten potentieel frauduleuze aanbiedingen [92];

- De oorspronkelijke vraag over aankoopfraude is, op aanraden van de auteurs van de Amerikaanse pilot [49], in het huidige onderzoek gewijzigd. In de oorspronkelijke vragenlijst kwamen veel klachten van ontevreden consumenten aan bod die niet als echte fraude konden worden opgevat. De gewijzigde vraagstelling moest dit voorkomen. Dat dit effect heeft gehad lijkt plausibel: 10,5% in de huidige studie versus 42,6% in de Amerikaanse pilot [49];

- Het huidige onderzoek paste een uitgebreide kwaliteitscontrole toe op de gegeven antwoorden, waarbij veelal kwalitatieve beschrijvingen (zie sectie 2.1), die niet altijd werden gevraagd in de Amerikaanse pilot [49] nauwkeurig zijn bestudeerd. Hieruit bleek dat respondenten geregeld gebeurtenissen rapporteren als fraude die eigenlijk geen fraude zijn, of gebeurtenissen rapporteren onder de verkeerde fraudecategorie. Door dit te corrigeren in de voorbewerking van de data vallen de cijfers mogelijk lager uit, maar zouden ze wel accurater moeten zijn.

Tenslotte rapporteren niet alle Amerikaanse studies veel hogere cijfers. Zo vond een onderzoek van de *Federal Trade Commission* (FTC) naar ‘mass-market consumer fraud’ een slachtofferpercentage van 15,9% voor 2017 [77]. De omschrijving van mass-market fraud was grotendeels gelijk aan het huidige onderzoek.[9]

Daarnaast vond ook een andere recent gepubliceerde Amerikaanse studie [121] aanzienlijk lagere cijfers dan die van de Amerikaanse pilot [49]. Deze recente studie richtte zich op fraude in 2017 en vond slachtofferschap van minder dan 0,3% voor investeringsfraude, baanfraude, prijsfraude, schuldfraude, goede-doelenfraude en relatiefraude (vriend-in-nood en datingfraude

[9] Het ging bij dit onderzoek om frauduleuze producten voor gewichtsverlies, frauduleuze hulp bij computerproblemen, nepschulden bij de overheid en ongeautoriseerde factureringen.

in het huidige onderzoek). De slachtofferschapscijfers voor aankoopfraude en het totaal aan fraude waren dan weer aanzienlijk lager: 0.8 en 1,3%.

Een belangrijk punt is dat er weinig overeenstemming is in de wetenschappelijke literatuur over de definitie van fraude, er grote verschillen bestaan in de concrete operationalisatie van fraude en dat verdere methodologische keuzes impact hebben op de gevonden prevalentie [71, 122].

6.3 Bijlage 3: Vergelijking vragen Veiligheidsmonitor 2021

	Vraag in Veiligheidsmonitor 2021 (CBS) [27]	*Vraag in huidige slachtofferstudie*
Aankoopfraude	Bent u weleens opgelicht bij een online aankoop? Het gaat erom dat u zelf al had betaald voor producten of diensten (bijv. tickets of reizen) die nooit werden geleverd, en waarbij de verkoper u achteraf niet terugbetaalde.	… u hebt betaald voor een **product dat, of dienst die**, u nooit ontving of die oplichting was?
Identiteitsfraude	Heeft u weleens meegemaakt dat iemand illegaal gebruik maakte van uw persoonsgegevens? Bijv. met (een kopie van) uw paspoort, ID-kaart, rijbewijs of gegevens van een online account. Ook als u dit al heeft opgegeven bij een ander voorval, willen we u vragen dit hier opnieuw mee te tellen.	Hoe vaak heeft iemand zonder dat u dat wilde **gebruik gemaakt van uw persoonlijke gegevens** (bv. naam, bankgegevens, BSN/Sofinummer) voor financieel gewin, bijvoorbeeld voor het opnemen of overmaken van geld, het afsluiten van een lening, het opvragen van officiële documenten, het kopen van producten en/of diensten of het afsluiten van abonnementen?
Phishing	Door internetcriminelen worden vaak trucs gebruikt om mensen op te lichten. Dit doen ze op verschillende manieren, bijv. via e-mail, WhatsApp, social media of telefonisch. Ze doen zich voor als een medewerker van uw bank of van een computerhelpdesk. Of ze beweren dat u de loterij gewonnen heeft, een erfenis krijgt of een boete moet betalen. Soms doen ze zich voor als een familielid in geldnood. Ook komt het voor dat er gebeld en snel opgehangen wordt in de hoop dat mensen terugbellen naar een duur buitenlands nummer.	… u uw gebruikersnaam, wachtwoord of bank- of creditkaartgegevens aan buitenstaanders hebt gegeven in reactie op **phishing via e-mail of via een website**?