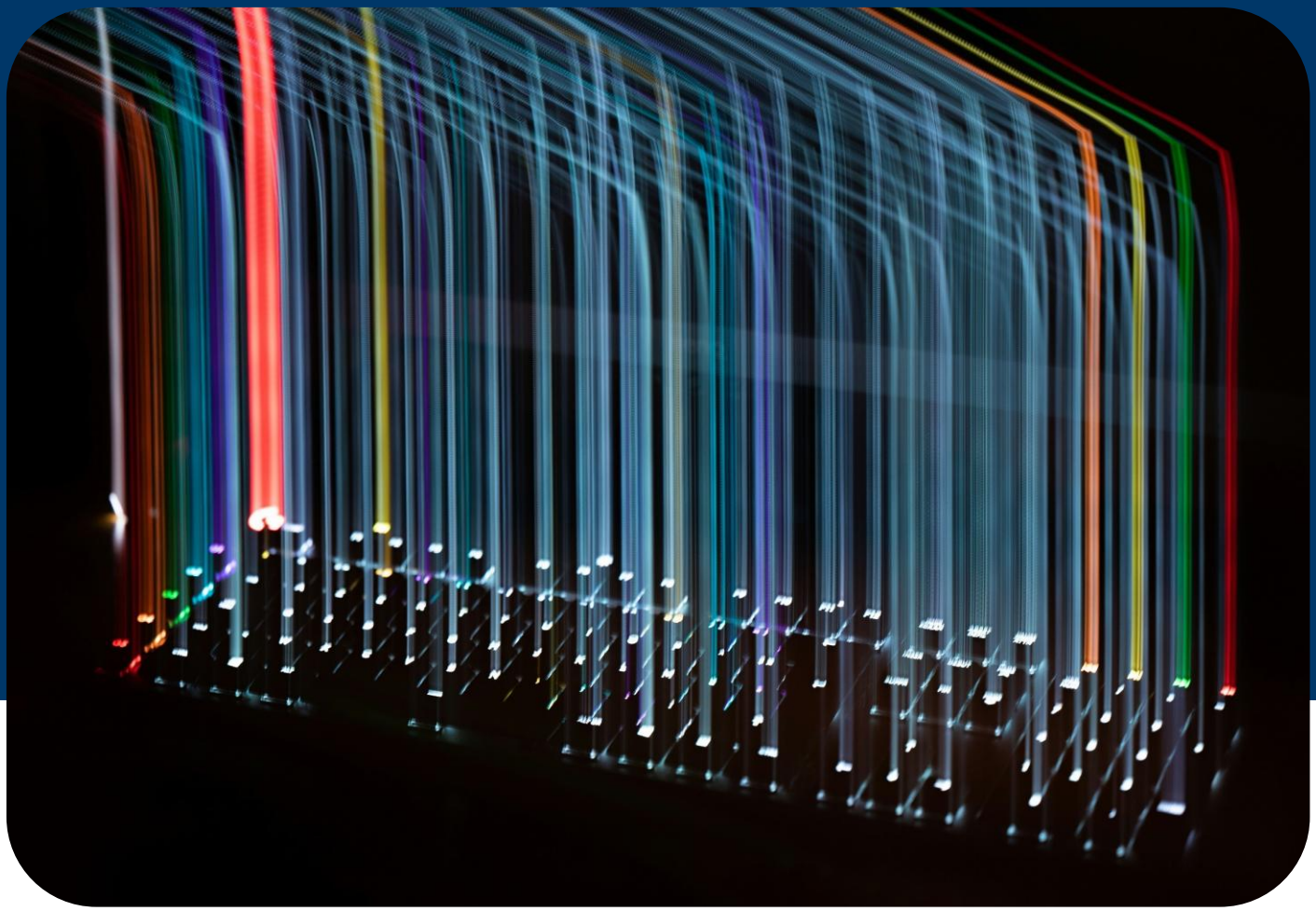
dialogic

Onderzoek voor *onderbouwd* beleid.



Rapport

Onderzoek naar de aard en omvang van schade door online fraude bij bedrijven

Auteurs

Tessel Blom

Menno Driesse

Luuk Brouwers

Iris van Vugt

Rapport

Onderzoek naar de aard en omvang van schade door online fraude bij bedrijven

Auteurs

Tessel Blom
Menno Driesse
Luuk Brouwers
Iris van Vugt

Opdrachtgever

Wetenschappelijk Onderzoek- en Datacentrum

Publicatienummer

2024.184-11030

Citeren als

Blom, T., Driesse, M., Brouwers, L., & van Vugt, I., (2026). *Onderzoek naar de aard en omvang van schade door online fraude bij bedrijven*. WODC: Den Haag.

Datum

15 april 2026

Beeld omslag

Adrien via Unsplash

Dankwoord

Dit onderzoek is uitgevoerd in de periode maart 2025 tot en met maart 2026 in opdracht van het Wetenschappelijk Onderzoek- en Datacentrum (WODC) van het ministerie van Justitie en Veiligheid (JenV). Voor het begeleiden van het onderzoek is door WODC een onafhankelijke begeleidingscommissie ingesteld. Wij bedanken de leden van de begeleidingscommissie voor hun waardevolle inbreng gedurende het gehele onderzoeksproces.

Deze begeleidingscommissie bestond uit de volgende leden:

- Em. prof. dr. ir. J. van den Berg (voorzitter)
- Dr. S.G.A. van de Weijer (lid)
- Dr. C.A. Meerts (lid)
- J.W. Veldsink, MSc (lid)
- L.R.L. Poffé (beleidsdirectie)
- Dr. H.C.J. van der Veen (projectbegeleider)

Inhoud

Managementsamenvatting

Aanleiding van het onderzoek

Online fraude is in recente jaren een steeds belangrijker en actueler onderwerp geworden voor het Nederlandse bedrijfsleven. Door technologische ontwikkelingen, waaronder verdere digitalisering van bedrijfsprocessen en communicatie, hebben fraudeurs meer mogelijkheden gekregen om bedrijven online te misleiden. Tegelijkertijd **ontbreekt het aan actuele en betrouwbare kennis over de aard en omvang van online fraude bij bedrijven en over de directe financiële schade die bedrijven hierdoor lijden**. Bestaande literatuur en onderzoeken bieden vooral achtergrondinformatie of richten zich op particulieren, cybercriminaliteit in brede zin of specifieke fraudevormen, maar geven geen samenhangend beeld van online fraude bij bedrijven in Nederland. Deze kennis is echter noodzakelijk om gerichte beleidsmaatregelen te kunnen ontwikkelen en om bedrijven die slachtoffer worden van online fraude beter te ondersteunen.

Doelstelling en onderzoeksvragen

Het doel van dit onderzoek was om inzicht te krijgen in de aard en omvang van de schade door online fraude bij bedrijven in Nederland. Daarbij is niet alleen gekeken naar de uitkomsten zelf, maar ook naar de vraag in hoeverre databronnen beschikbaar zijn en welke methoden gebruikt kunnen worden om op basis van deze bronnen online fraude bij bedrijven te schatten. Vervolgens is getracht dit daadwerkelijk in kaart te brengen. Hierbij is ook expliciet aandacht besteed aan de (on)mogelijkheden van deze exercitie, aannames, onzekerheden en mogelijkheden voor verbetering van toekomstige schattingen.

Onderzoeksaanpak

Het onderzoek bestond uit een vooronderzoek en een hoofdonderzoek. In het vooronderzoek is een literatuurstudie uitgevoerd en zijn interviews gehouden met stakeholders en experts op het gebied van online fraude. Het vooronderzoek heeft onder andere geleid tot een **taxonomie van online fraude bij bedrijven**, die ook in de toekomst gebruikt kan worden om fraudevormen eenduidig te classificeren en te registreren (zie Figuur 1).

Figuur 1: Taxonomie van online fraude bij bedrijven.

Daarnaast is een **inventarisatie van beschikbare databronnen gedaan**, waarbij de mogelijkheden en beperkingen van de bron in kaart zijn gebracht, net als beperkingen in de huidige uitvoeringspraktijk. Voor het onderzoek zijn vier bronnen geïdentificeerd die op dit moment inzicht kunnen bieden in de aard en omvang van online fraude bij bedrijven. **Deze databronnen kennen echter duidelijke beperkingen die grote invloed hebben op de betrouwbaarheid van schattingen.** Deze databronnen zijn:

1. *Politieregistraties*. Politieregistraties kunnen een belangrijke bron zijn voor inzichten over online fraude, doordat zij een groot landelijk meldpunt zijn voor slachtoffers. **De registratiepraktijk bij de politie is momenteel echter onvoldoende voor het in kaart brengen van slachtofferschap van online fraude bij bedrijven**. Meldingen en aangiftes zijn vaak onvolledig, waarbij niet duidelijk is of het slachtoffer een bedrijf of een particulier is. Ook worden er geen eenduidige definities gehanteerd voor verschillende fraudevormen en ontbreken schadebedragen.
2. *Fraudehelpdesk Zakelijk*. De Fraudehelpdesk Zakelijk is een online meldpunt voor bedrijven voor fraude. **Data van de Fraudehelpdesk Zakelijk bevat uitgebreide en consistente informatie over fraude-incidenten en fraudevormen**. Bij de Fraudehelpdesk Zakelijk wordt echter geen informatie verzameld over de

kenmerken van bedrijven die melding maken, waardoor deze databron geen verdere inzichten kan bieden over het type bedrijven dat slachtoffer wordt.

3. *Enquête onder ondernemerspanel.* We hebben een enquête uitgezet onder een representatief panel van 600 ondernemers van Ipsos I&O. In deze enquête hebben we succesvol gebruik gemaakt van de opgestelde taxonomie voor online fraude. Middels extrapolatie hebben we vervolgens een schatting gemaakt van de omvang van online fraude bij bedrijven. **Bij slachtofferenquêtes is echter vaak sprake van een slachtofferbias**, wat leidt tot mogelijke overschattingen, en **het aantal slachtoffers in de steekproef is te klein** om verdiepende inzichten te krijgen in de aard van online fraude en de verschillende fraudevormen bij bedrijven.
4. *Enquête onder ondernemerspopulatie.* We hebben via VNO-NCW, MKB-Nederland en de aangesloten brancheverenigingen een enquête breed uitgezet onder ondernemers. **Hier hebben we (nogmaals) ondervonden dat ondernemers niet graag enquêtes invullen.** De respons bleef na meerdere reminders beperkt tot enkelen, waardoor deze databron niet verder gebruikt kon worden in dit onderzoek.

Tot slot is een onderzoeksaanpak vastgesteld waarbij we de omvang van online fraude proberen te schatten door middel van extrapolatie van de enquête resultaten en het gebruik van de multipliermethode. Bij multipliermethode gebruiken we de meldingspercentages uit de enquête om tot een schatting te komen van het *dark number* van de politieregistraties en de Fraudehelpdesk Zakelijk. Daarmee kunnen we een schatting maken van de totale omvang van online fraude bij bedrijven. Indien mogelijk triangulerен we deze drie schattingen vervolgens om tot een robuustere schatting te komen.

De aard en omvang van online fraude bij bedrijven

Bovenstaande methode leidt tot schattingen van de omvang online fraude die sterk verschillen tussen de databronnen. De schattingen op basis van registerdata (Fraudehelpdesk Zakelijk en politieregistraties) in combinatie met de gerapporteerde meldingspercentages in de enquête (multipliermethode) zijn vele malen lager dan de schatting op basis van extrapolatie van de enquêteresultaten en ook de 95%-betrouwbaarheidsintervallen zijn erg breed (Tabel 1). Wij kunnen hierdoor geen betrouwbare schatting maken van de omvang van online fraude bij bedrijven.

Tabel 1. Overzicht van schattingen van slachtoffers en fraude-incidenten voor de verschillende databronnen. De politieregistraties bevatten geen (betrouwbare) informatie over financiële schade door fraude-incidenten.

Databron	Schatting (95% betrouwbaarheidsinterval)
Enquête ondernemerspanel	**52.849 - 124.573** ***slachtoffers*** **80.532 - 189.825** ***incidenten met directe schade***
Fraudehelpdesk Zakelijk	**1.680 - 11.667** ***incidenten met directe schade***
Politieregistraties	**4.061 - 9.748** ***incidenten***

De schatting van de omvang van de directe financiële schade door online fraude verschilt ook sterk tussen de uitkomsten uit de enquête (extrapolatie) en uit de meldingen bij de Fraudehelpdesk Zakelijk (multipliermethode op basis van meldingspercentage uit enquête). **De directe financiële schade, geschat op basis van de enquête, ligt met een 95%-betrouwbaarheidsinterval tussen €90 miljoen en €211 miljoen**. Op basis van meldingen bij de Fraudehelpdesk Zakelijk ligt dit lager.

Tabel 2. Overzicht van schattingen van omvang van de schade voor de verschillende databronnen. De politieregistraties bevatten geen (betrouwbare) informatie over financiële schade door fraude-incidenten.

Databron	Schatting (95% betrouwbaarheidsinterval)
Enquête ondernemerspanel	**€90 miljoen - €211 miljoen** ***directe financiële schade***
Fraudehelpdesk Zakelijk	**€14 miljoen - €95 miljoen** ***directe financiële schade***

De meeste geregistreerde en gerapporteerde incidenten van online fraude bij bedrijven betreffen aan- en verkoopfraude. Incidenten van factuurfraude, CEO-fraude, identiteitsfraude en helpdeskfraude worden relatief vaker gemeld bij de politie, terwijl acquisitiefraude vaker gemeld wordt bij de Fraudehelpdesk Zakelijk. Aan- en verkoopfraude vindt veelal plaats op webshops, terwijl de andere fraudevormen meestal telefonisch of via e-mail gebeuren.

Aanbevelingen

Voor beter zicht op online fraude bij bedrijven is het van belang dat er **in de toekomst meer data wordt verzameld, en dat de beschikbare data van betere kwaliteit is**. Om dit te bereiken bevelen we een aantal zaken aan:

- **De registratiepraktijk bij de politie moet structureel worden verbeterd**. De politie is een belangrijk landelijk meldpunt waar slachtoffers zich melden. Voor inzicht in dit slachtofferschap is het noodzakelijk dat de politie in ieder geval gaat registreren of de melder een bedrijf of particulier is en welke directe financiële schade het fraude-incident tot gevolg had. Het verplicht maken van bepaalde velden in de registratie bij het opnemen van de melding of aangifte, zoals fraudevorm, slachtoffertype en schade, zou hiertoe een eerste stap zijn.
- Bij het maken van een *dark number* schatting zullen meerdere databronnen gecombineerd moeten worden. **Het is daarom van belang dat verschillende organisaties een gezamenlijke taxonomie voor online fraude hanteren**, zoals is voorgesteld in dit rapport. Door gebruik te maken van dezelfde definities en afbakeningen, kan data vergeleken worden en sluit deze op elkaar aan. Door de centrale positie van de Fraudehelpdesk in het landschap kan overwogen worden hen hiervoor verantwoordelijk te maken.[1]
- Voor inzicht in slachtoffertypes zou door de Fraudehelpdesk Zakelijk overwogen kunnen worden **ook informatie over de bedrijven, zoals de bedrijfssector en de bedrijfsgrootte, uit te vragen bij de melders**. Wanneer meer zicht is op slachtoffertypes kunnen beleidsinterventies gericht worden ontwikkeld voor de preventie en bestrijding van online fraude bij bedrijven.
- Ondernemers zijn een notoir lastige doelgroep om te bereiken met een enquête. Het is daarom aan te raden om **inspanningen hiertoe te bundelen en met slachtofferenquêtes aan te sluiten bij lopende monitors.** Een kansrijke monitor voor het in kaart brengen van de omvang van online fraude bij bedrijven is de Monitor Criminaliteit Bedrijfsleven van het CBS, die naar verwachting in 2026 uitgezet zal worden.

[1] Dit is in lijn met één van de opgestelde ontwikkelrichtingen voor de Fraudehelpdesk uit de evaluatie van de organisatie in 2023 (Pro Facto, 2023).

1 Inleiding

1.1 Aanleiding van het onderzoek

In recente jaren is online fraude een steeds belangrijker en actueler onderwerp geworden voor het bedrijfsleven. Technologische ontwikkelingen zorgen ervoor dat ook online fraude steeds gemakkelijker wordt. Zo gebruiken fraudeurs bijvoorbeeld kunstmatige intelligentie (AI) om documenten te vervalsen, waarmee ze (vele) duizenden euro's aan valse claims indienden bij verzekeraars.[2] Echter ontbreekt het momenteel aan kennis van de omvang van deze online fraude in het Nederlandse bedrijfsleven en de omvang van de daarbij geleden schade. De literatuur op het gebied van online fraude kan handvatten en achtergrondinformatie bieden op het onderwerp. Daarentegen biedt het geen concrete informatie over de omvang van online fraude in het Nederlandse bedrijfsleven. Deze kennis is noodzakelijk voor gerichte (beleids)inspanningen om fraude tegen te gaan en om bedrijven die slachtoffer zijn geworden te voorzien van passende hulp. Dit onderzoek moet hier inzicht in geven.

1.2 Doel van het onderzoek en onderzoeksvragen

Dit rapport betreft de uitkomsten van een onderzoek naar de aard en omvang van schade door online fraude bij bedrijven. Om tot een schatting te komen van de aard en omvang zijn een voor- en hoofdonderzoek uitgevoerd. In het vooronderzoek is onderzoek gedaan naar de beschikbaarheid van data op het onderzoek. In het hoofdonderzoek is de beschikbare data geanalyseerd. Het voor- en een hoofdonderzoek proberen daarmee gezamenlijk de hoofdvraag te beantwoorden:

Wat is de aard en omvang van de schade door online fraude bij bedrijven in Nederland?

In het vooronderzoek is een inventarisatie gedaan van de data die beschikbaar is en is geanalyseerd in welke mate deze informatie toereikend is voor het beantwoorden van de hoofdvraag. Dit is gedaan aan de hand van de volgende onderzoeksvragen:

1. Welke databronnen en/of welke data zijn beschikbaar (te maken) over:
    a. Het aantal slachtoffers van online fraude in het Nederlandse bedrijfsleven;
    b. De typen van online fraude waarmee het Nederlandse bedrijfsleven te maken had;
    c. De omvang van de geleden financiële schade als gevolg van deze online fraude?

[2] Zie: [nos.nl]

2. Wat kan er worden gezegd over de volledigheid, validiteit, betrouwbaarheid en actualiteit van de opgeslagen registerdata of in het geval van een panelbevraging van de te verzamelen data?
3. In hoeverre zijn de beschikbaar (te maken) data ook geschikt voor het maken van een betrouwbare actuele schatting van het aantal bedrijven en het type bedrijven dat te maken heeft met online fraude en van de geleden financiële schade in het bedrijfsleven als gevolg van online fraude?
4. Welke methode(n) kom(t)(en) naar voren als geschikte methode(n) om een wetenschappelijk verantwoorde schatting uit te voeren van het aantal en type bedrijven dat te maken heeft met online fraude en van de financiële schade van het bedrijfsleven door online fraude?

Aan de hand van deze databronnen en nieuw verzamelde data proberen we antwoord te geven op de volgende onderzoeksvragen in het hoofdonderzoek:

5. Hoeveel bedrijven waren in 2024 slachtoffer van online fraude?
    a. Zijn hierin verschillen tussen bedrijfstypen (grootte en sector)?
    b. In welke mate gaat het hierbij om enkelvoudig, meervoudig of herhaald slachtofferschap?
6. Met welke online fraudevormen hadden bedrijven in 2024 te maken?
    a. Hoeveel bedrijven werden slachtoffer van de verschillende fraudevormen?
    b. Zijn hierin verschillen tussen bedrijfstypen (grootte en sector)?
7. Welke directe financiële schade ondervonden bedrijven in 2024 als gevolg van online fraude?
8. Welke aannames zijn gemaakt bij het maken van schattingen over de omvang van online fraude en wat kan er worden gezegd over eventuele schending van aannames en de doorwerking hiervan op de omvang van de schatting?
9. Welke zekerheid kan er worden verbonden aan de schattingen in dit onderzoek?
10. Hoe zouden schattingen in de toekomst verbeterd kunnen worden?

1.3 Onderzoeksmethodiek

Zoals al eerder aangegeven bestaat dit onderzoek uit twee delen (het voor- en het hoofdonderzoek) die beide hun eigen onderzoeksmethodiek hadden. Hieronder beschrijven we deze.

1.3.1 Vooronderzoek

Het vooronderzoek bestond uit een literatuuronderzoek gecombineerd met interviews, In totaal zijn er acht interviews gehouden met (vertegenwoordigers van) belangrijke stakeholders en experts op het gebied van (online) fraude en specifiek op het gebied

van online fraude bij bedrijven, zoals de Fraudehelpdesk, het Platform Veilig Ondernemen en VNO-NCW. Een overzicht van alle respondenten is te vinden in Bijlage 1.

In het vooronderzoek zijn we ook tot een taxonomie gekomen die noodzakelijk is voor het maken van een robuuste schatting van de aard en omvang van online fraude bij bedrijven. Met deze taxonomie kunnen we de verschillende vormen van online fraude classificeren. Deze hebben wij opgesteld op basis van het literatuuronderzoek en taxonomieën die we hebben ontvangen van de partners van de Integrale Aanpak Online Fraude[3] en de Fraudehelpdesk. Deze twee hebben wij geanalyseerd en vertaald in een eenduidige taxonomie van online fraude bij bedrijven.

In de tweede fase van het literatuuronderzoek is gezocht naar publicaties en onderzoeken die inzicht geven in het aantal bedrijven dat slachtoffer is geweest van online fraude. Hierbij is gekeken naar zowel wetenschappelijke als andersoortige publicaties. Er zijn ook onderzoeken meegenomen die inzicht geven in online fraude bij particulieren of in online fraude bij niet-Nederlandse bedrijven. Het doel van deze inventarisatie was om inzicht te krijgen in de databronnen die onder deze publicaties liggen en te beoordelen of en in welke mate deze gebruikt zouden kunnen worden in dit onderzoek. Daarnaast geven deze publicaties ook inzichten in mogelijke beperkingen van de databronnen. Een overzicht van de onderzochte publicaties en de beoordeling op volledigheid, betrouwbaarheid, validiteit en actualiteit is te vinden in Bijlage 3. Op basis hiervan zijn we tot een set aan databronnen gekomen die (gezamenlijk) gebruikt kan worden voor het maken van een schatting van online fraude bij bedrijven.

1.3.2 Hoofdonderzoek

Deze databronnen hebben we in het hoofdonderzoek verzameld en geanalyseerd. Het betreft hier een enquête die is uitgezet onder een ondernemerspanel van Ipsos I&O, een analyse van politieregistraties van online fraude en meldingen van online fraude bij de Fraudehelpdesk Zakelijk. De exacte invulling van deze methoden wordt in de respectievelijke hoofdstukken beschreven.

[3] De Integrale Aanpak Online Fraude is een publiek-private samenwerking tussen Politie, het Openbaar Ministerie, VNO-NCW/MKB Nederland, Vodiom, de Consumentenbond, de Nederlandse Vereniging van Banken (NVB), COIN, Thuiswinkel.org, Meta, de Vereniging Nederlandse Gemeenten (VNG), het ministerie van Economische Zaken, het ministerie van Financiën en het ministerie van Justitie en Veiligheid.

Leeswijzer voor dit rapport

In Hoofdstuk 2 definiëren we het begrip online fraude bij bedrijven, beschrijven we de verschillende vormen van online fraude bij bedrijven en stellen we een taxonomie op om deze vormen te classificeren. Deze taxonomie wordt door het volledige rapport gebruikt. Hoofdstuk 3 beschrijft de wijze waarop we online fraude (in theorie) kunnen meten via verschillende. Ook beschrijven we daar hoe we omgaan met niet-geregistreerde online fraude.

Vervolgens bevat Hoofdstuk 4 de inventarisatie van databronnen die mogelijk inzicht kunnen geven in online fraude bij bedrijven. Deze databronnen worden beschreven en beoordeeld op relevantie voor dit onderzoek. Ook worden in dit hoofdstuk aanbevelingen gedaan voor mogelijke verbeteringen met betrekking tot de verzameling van data over online fraude bij bedrijven. In Hoofdstuk 5 schatten we op basis van deze databronnen de aard en omvang van schade door online fraude bij bedrijven.

Afsluitend bevat Hoofdstuk 6 de conclusies, een reflectie op het onderzoek en aanbevelingen.

2 Het begrip online fraude bij bedrijven

In dit hoofdstuk bespreken we het begrip online fraude bij bedrijven. Hiervoor definieren we eerst de begrippen gedigitaliseerde criminaliteit, fraude en bedrijven en komen we tot een classificatie van delicten die onder de noemer online fraude bij bedrijven vallen. Vervolgens geven we op basis van deze definitie een lijst met fraudevormen en stellen we een taxonomie voor om deze fraudevormen te classificeren.

2.1 Definities en afbakening

Om gericht de aard en omvang van de schade van online fraude in kaart te brengen is het voor dit onderzoek van belang om online fraude eenduidig te definiëren. Als we dat niet doen, lopen we namelijk het risico om bijvoorbeeld te generieke cijfers over online criminaliteit te verzamelen – iets wat niet het doel van dit onderzoek is. Het is van belang de gehanteerde begrippen (online, fraude, bedrijven en schade) helder te definiëren en ook vooral helder te stellen welke delicten hier *geen* onderdeel van zijn.

In dit onderzoek definiëren wij een delict als online fraude bij een bedrijf als:

1. De dader ICT als hulpmiddel gebruikt;
2. De dader het slachtoffer opzettelijk en bewust misleidt;
3. Er sprake is van een frauduleuze transactie tussen slachtoffer en dader;
4. Het slachtoffer door de misleiding in zakelijk verband geld is verloren aan de dader.

In onderstaande secties lichten we toe hoe we tot deze voorwaarden zijn gekomen.

2.1.1 Online fraude als vorm van online criminaliteit

Online fraude is een vorm van online criminaliteit. Onder de noemer ‘online criminaliteit’ vallen diverse delicten die kunnen worden onderverdeeld in twee categorieën: cybercriminaliteit en gedigitaliseerde criminaliteit.

- Onder *cybercriminaliteit* vallen delicten waarbij de ICT-infrastructuur doelwit is en waarbij ICT gebruikt wordt als middel voor de uitvoering van het delict (informeel ook wel ‘een aanval op een computer met een computer’ genoemd). Voorbeelden van cybercriminaliteit zijn het platleggen van websites met DDoS-aanvallen, het hacken van databases met persoonsgegevens of het gijzelen van IT-systemen met ransomware (Leukfeldt, Notté, & Malsch, 2018).

- Onder *gedigitaliseerde criminaliteit* vallen traditionele offline delicten die ook online gepleegd worden. Hierbij wordt ICT als hulpmiddel ingezet, maar is ICT niet het doelwit van het delict. Online fraude is een voorbeeld van

gedigitaliseerde criminaliteit, net als bijvoorbeeld het online verspreiden van kinderpornografisch materiaal (Leukfeldt, Notté, & Malsch, 2018).

2.1.2 Fraude

Fraude wordt door het Openbaar Ministerie (OM) gedefinieerd als “opzettelijke misleiding om onrechtmatig voordeel te verkrijgen” (Openbaar Ministerie, n.b.). In de wetenschappelijke literatuur wordt deze definitie verder uitgewerkt naar het “opzettelijk en bewust misleiden van een slachtoffer door feiten over beloofde goederen, diensten of andere voordelen, die niet bestaan, onnodig zijn of nooit geleverd zouden worden, opzettelijk te verdraaien, verkeerd voor te stellen, te verbergen of weg te laten, met als doel het behalen van financieel gewin” (Beals, DeLiema, & Deevy, 2015). Daarnaast is het voor fraude ook van belang dat het slachtoffer actief deelneemt aan de frauduleuze transactie. Dit onderscheidt fraude van andere delicten waarbij slachtoffers niet misleid worden, zoals diefstal of ransomware (Beals, DeLiema, & Deevy, 2015). In onze definitie nemen we daarom op dat de dader het slachtoffer opzettelijk en bewust misleidt en dat er sprake moet zijn van een frauduleuze transactie tussen slachtoffer en dader.

We nemen in dit onderzoek alleen succesvolle fraude mee en geen fraudepogingen. Dit betekent dat het slachtoffer door de fraude daadwerkelijk geld is verloren (Beals, DeLiema, & Deevy, 2015).[4] Bedrijven die slachtoffer worden van online fraude kunnen daar op verschillende manieren schade door ondervinden. In dit onderzoek beperken we ons tot financiële schade. Hierbij zijn alsnog een aantal overwegingen relevant, met name het onderscheid tussen directe en indirecte financiële schade. Binnen dit onderzoek richten we ons op het feitelijke bedrag van de financiële schade op het moment van het misdrijf, oftewel de directe schade (in economische termen ook wel: eerste-orde-effecten). Van deze schade kunnen we het beste aannemelijk maken dat de schade direct gerelateerd is aan het fraudevoorval. Bij indirecte schade (tweede-orde-effecten) is dit minder het geval. Uit de interviews blijkt bijvoorbeeld dat bij beleggingsfraude alleen het bedrag dat door het slachtoffer is geïnvesteerd als (directe) financiële schade wordt aangemerkt, maar dat slachtoffers hier ook het beloofde rendement of misgelopen investeringen opvoeren als (indirecte) financiële schade, evenals de tijd die het fraudevoorval de ondernemer heeft gekost (deze tijd is immers niet besteed aan de bedrijfsvoering). Dergelijke indirecte effecten zijn echter moeilijk vast te stellen en zullen in beschikbare databronnen vermoedelijk niet altijd gemeld zijn door de ondernemer. Daardoor is het lastig de indirecte schade van online fraude in kaart te brengen en wordt in dit onderzoek alleen directe schade meegenomen.

[4] Dit betekent niet dat fraudepogingen niet tot schade kunnen leiden bij het slachtoffer, zoals emotionele schade of reputatieschade.

Verder kan online fraude enkelvoudig, meervoudig en/of herhaald voorkomen. We spreken in dit onderzoek van enkelvoudig slachtofferschap, als een bedrijf één keer slachtoffer is geweest van één vorm van online fraude. Het gaat dan dus om één fraude-incident. Indien een bedrijf meerdere keren slachtoffer is geweest van *dezelfde* vorm van online fraude, spreken we van herhaald slachtofferschap. Hierbij gaat het om meerdere fraude-incidenten. Er is bijvoorbeeld sprake van herhaald slachtofferschap als een bedrijf in 2024 in april, juni en september te maken heeft gehad met aankoopfraude, waarbij er bij elk van deze incidenten geld is verloren. Als laatste spreken we van meervoudig slachtofferschap als een bedrijf meerdere keren slachtoffer is geweest van *verschillende* vormen van online fraude. Hier gaat het dus om verschillende fraude-incidenten van verschillende fraudevormen.

2.1.3 Bedrijven

Dit onderzoek beperkt zich tot online fraude bij bedrijven. Onder bedrijven verstaan we alle typen Nederlandse ondernemingen, van zzp tot aan multinational. Publieke organisaties als overheden en verenigingen vallen hier niet onder.

Er kan overigens wel sprake zijn van overlap tussen de categorie particulieren en de categorie bedrijven. Een zelfstandig ondernemer kan namelijk als particulier persoon bijvoorbeeld slachtoffer worden van online fraude, en daar ook als ondernemer schade ondervinden door bedrijfsgelden over te maken naar de dader. Omdat dit individu geen slachtoffer is vanuit de rol van werknemer van een bedrijf of als ondernemer, nemen wij deze vorm van online fraude niet mee in het onderzoek. We kijken immers specifiek naar online fraude waarbij het slachtoffer in zakelijk verband geld is verloren. In hoeverre dit ook daadwerkelijk mogelijk is in de beschikbare databronnen zal moeten blijken.

2.2 Taxonomie

In dit onderzoek brengen we bronnen in kaart die inzicht (kunnen) geven in de aard en omvang van de schade door online fraude bij bedrijven. Om dit goed te kunnen doen is het noodzakelijk om eerst een duidelijke taxonomie van het fenomeen te ontwikkelen. Zonder deze taxonomie zullen de schattingen beïnvloed worden door overlappende definities en categorieën van online fraude bij verschillende bronnen. Bronnen kunnen bijvoorbeeld rapporteren over online fraude op verschillende abstractieniveaus. Zo is BEC (Businesses E-mail Compromise) fraude een veel genoemde vorm van online fraude in de literatuur en de interviews, maar is dit een verzamelnaam voor fraudevormen waarbij iemand zich in een email voordoet als iemand anders om geld of gevoelige bedrijfsinformatie te ontfutselen. Hiermee is het een benaming voor de wijze waarop ICT als hulpmiddel wordt ingezet en geen goede naam voor de gepleegde fraude (het delict).

2.2.1 Principes van de taxonomie

Om de consistentie en internationale vergelijkbaarheid van misdaadstatistieken te verbeteren en analytische mogelijkheden op zowel nationaal als internationaal niveau te versterken, is de *International Classification of Crime for Statistical Purposes* (ICCS) ontwikkeld. Wij gebruiken diezelfde methode om de verschillende fraudevormen binnen dit onderzoek te classificeren.

Aan deze classificatiemethode liggen vier principes ten grondslag (UNODC/UNECE, 2012; Beals, DeLiema, & Deevy, 2015):

- **Uitputtendheid.** De classificatie moet alle relevante misdrijven dekken, zonder hiaten, zodat elk type misdaad een plaats heeft binnen het systeem.
- **Structuur** De classificatie moet een duidelijke en logische hiërarchische structuur hebben, waardoor gebruikers gemakkelijk kunnen navigeren en misdaden systematisch kunnen indelen.
- **Wederzijdse exclusiviteit.** Elke misdaad moet slechts in één categorie vallen, zonder overlap met andere categorieën, om verwarring en dubbeltelling te voorkomen.
- **Omschrijving.** Elke categorie moet duidelijk omschreven zijn, zodat er geen ruimte is voor verschillende interpretaties van wat een bepaalde misdaad inhoudt.

2.2.2 Vormen van online fraude bij bedrijven

Op basis van de literatuur, de beschrijvingen van fraudevormen die door de partners van de Integrale aanpak online fraude zijn opgesteld, de aangehouden fraudevormen van de Fraudehelpdesk en aanvullende inzichten uit de interviews zijn wij tot een lijst van fraudevormen gekomen die binnen de definitie van online fraude bij bedrijven vallen. Deze lijst is weergegeven in Tabel 3. In deze tabel beschrijven we iedere fraudevorm aan de hand van de acties van de dader (op welke manier misleidt deze het slachtoffer) en de acties van het slachtoffer (via welke frauduleuze transactie verliest het slachtoffer geld).

Tabel 3: Overzicht van fraudevormen

Fraudevorm	Actie dader	Actie slachtoffer
Aankoopfraude	De dader biedt een dienst of product aan zonder de intentie te hebben deze te leveren of levert een product met andere kenmerken.	Het slachtoffer betaalt voor producten of diensten die niet worden ontvangen.

Fraudevorm	Actie dader	Actie slachtoffer
Acquisitiefraude	De dader werft opdrachten, maar is niet van plan daar iets mee te doen.	Het slachtoffer betaalt voor producten of diensten die niet worden ontvangen.
Beleggingsfraude[5]	De dader overtuigt het slachtoffer te investeren in valse, niet-bestaande of waardeloze beleggingen of virtuele valuta's (crypto's) waarbij hoge rendementen worden beloofd.	Het slachtoffer maakt geld over om te investeren in verlieslijdende of niet-bestaande producten, aandelen of valuta.
Betaalverzoekfraude	De dader overtuigt het slachtoffer een (klein) bedrag over te maken via een link die lijkt op een legitiem betaalverzoek en vangt via deze link de betaalgegevens van het slachtoffer af.	Het slachtoffer maakt een klein bedrag over en verstrekt de dader daarmee van betaalgegevens.
CEO-fraude	De dader doet zich voor als een hooggeplaatst persoon in de organisatie en vraagt het slachtoffer een geldbedrag over te maken.	Het slachtoffer maakt (in opdracht van de 'CEO') een geldbedrag over naar (vaak een buitenlandse) rekening.
Domeinnaamfraude	De dader overtuigt het slachtoffer een domeinnaam te registreren die sterk lijkt op de domeinnaam van het slachtoffer.	Het slachtoffer betaalt vele malen meer voor een domeinnaam dan nodig.
Factuurfraude	De dader manipuleert een factuur, factureert meervoudig voor dezelfde diensten of goederen of stuurt een (spook)factuur voor niet geleverde diensten of goederen.	Het slachtoffer betaalt een factuur.
Helpdeskfraude	De dader doet zich voor als een medewerker van een helpdesk. Hierbij is onderscheid	Het slachtoffer maakt een overboeking, geeft betaalmiddelen af of installeert een Remote

[5] Beleggingsfraude is met deze definitie een synoniem voor investeringsfraude, boilerroom fraude, ponzifraude en piramidefraude.

Fraudevorm	Actie dader	Actie slachtoffer
	tussen bancaire en niet-bancaire helpdeskfraude.	Access Tool waarmee frauduleuze transacties gedaan kunnen worden.
Identiteitsfraude (werknemer)	De dader doet zich voor als een medewerker van een bedrijf.	Het slachtoffer maakt een bedrag, bijvoorbeeld salaris, over naar de rekening van de fraudeur in de veronderstelling dat die van de werknemer is.
Recovery-fraude	De dader biedt het slachtoffer aan verloren geld door eerdere fraude terug te halen, maar zal deze beloofde hulp niet bieden.	Het slachtoffer betaalt de dader een vergoeding voor het terughalen van het geld.
Verkoopfraude	De dader koopt een product aan of ontvangt een dienst zonder de intentie te hebben hiervoor te betalen.	Het slachtoffer verstuurt het product of levert de dienst, maar ontvangt hier geen betaling voor.

2.2.3 Taxonomie van online fraude bij bedrijven

Aan de hand van principes van een taxonomie en voorgaande lijst met fraudevormen hebben wij een taxonomie opgesteld voor online fraude bij bedrijven. Deze taxonomie heeft drie niveaus en classificeert alle hierboven geïdentificeerde fraudevormen. Voor het opstellen van de taxonomie hebben wij de werkwijze uit Beals, DeLiema, & Deevy (2015) gevolgd. De taxonomie wordt in Figuur 2 geïllustreerd en bevat de volgende niveaus:

1. **Opbrengst voor de dader**. Op het eerste niveau kijken we naar de verwachte opbrengst voor de dader. Hierbij onderscheiden we:
    a. Betalingsfraude (opbrengst voor de fraudeur is een betaling)
    b. Producten- of dienstenfraude (opbrengst voor de fraudeur zijn producten of diensten waar niet voor is betaald)
2. **Modus operandi van de dader**. Op het tweede niveau kijken we naar de *modus operandi* van de fraudeur, de manier waarop de dader het slachtoffer misleidt en het financieel gewin dat het oplevert. Hierbij onderscheiden we:
    a. Niet leveren van beloofde goederen of diensten.
    b. Aannemen van een valse identiteit.
    c. Manipuleren van gegevens.
    d. Niet voldoen aan een betaling.

3. **Specificatie van modus operandi van de dader.** Op het derde niveau wordt de modus operandi verder gespecificeerd en worden de verschillende fraudevormen geplaatst.

Figuur 2: Taxonomie van online fraude bij bedrijven

2.2.4 Type slachtoffer en gebruik van ICT

In het uiteindelijke hoofdonderzoek is het doel om per fraudevorm in de taxonomie het aantal slachtoffers en de omvang van de schade in kaart te brengen. Hierbij spelen nog twee andere aspecten een rol: het *type slachtoffer* en *de wijze waarop ICT wordt gebruikt*. Door de hiërarchische structuur van de taxonomie moet elk lager niveau alle subsets bevatten van het niveau erboven. Het type slachtoffer en het ICT-gebruik zijn echter geen subsets van fraudevormen en worden daarom niet opgenomen in de taxonomie.

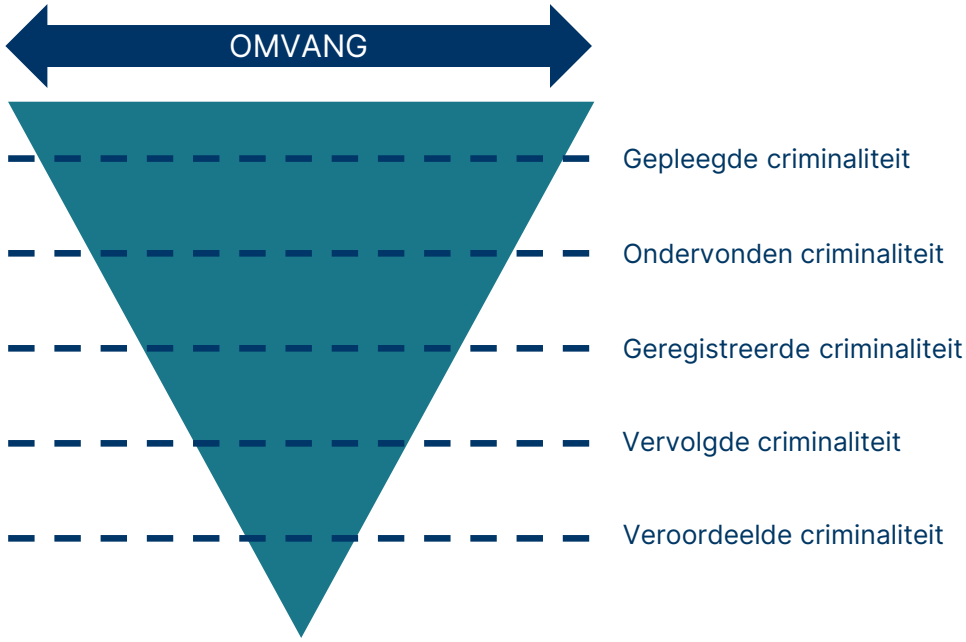
In de analyse van online fraude bij bedrijven zijn het bedrijfstype en het ICT-gebruik wel uitsplitsingen die we per fraudevorm en in totaal willen maken.

3 Het meten van online fraude

In dit hoofdstuk zetten we de (theoretische) kaders voor het meten van online fraude op. We doen dit aan de hand van het trechtermodel van criminaliteit. In dit model maken we onderscheid tussen de gepleegde criminaliteit, de ondervonden criminaliteit en de (niet-)geregistreerde criminaliteit. Vervolgens gaan we in op schattingsmethoden en -technieken die we in dit rapport gebruiken om de grootte van deze niet-geregistreerde criminaliteit te kunnen schatten.

3.1 Het trechtermodel van criminaliteit

Bronnen over online fraude kunnen het fenomeen op verschillende niveaus meten. Om dit in kaart te brengen maken we gebruik van het trechtermodel van criminaliteit, afgebeeld in Figuur 3. Dit trechtermodel is gebaseerd op het model uit Beerthuizen, Sipma, & van der Laan (2020) en aangepast zodat deze aansluit bij de terminologie uit Smit et al. (2018).



Figuur 3. Trechtermodel van criminaliteit.

Bovenaan in de trechter staat de gepleegde criminaliteit. In dit onderzoek scharen we hier alle vormen van online fraude bij bedrijven onder. Het volgende niveau in de trechter is de ondervonden criminaliteit. Tussen de gepleegde en ondervonden criminaliteit zit de online fraude die door het slachtoffer niet als zodanig wordt ervaren, bijvoorbeeld omdat ze (nog) niet doorhebben dat ze geld overmaken aan een fraudeur.

Slachtoffers van online fraude kunnen deze bij verschillende instanties melden. Uit de interviews komen hierbij met name instanties als de politie, de Fraudehelpdesk of hun

bank naar voren. De registraties van deze fraude incidenten wordt de geregistreerde criminaliteit genoemd. Tussen de registraties kan ook overlap bestaan, omdat slachtoffers het incident op meerdere plekken kunnen registreren of omdat er meerdere slachtoffers zijn van een incident (Smit, et al., 2018).

Bij de volgende laag begint de justitiële keten: een (eventuele) vervolging en een (eventuele) veroordeling. Deze niveaus zijn voor inzicht in de gepleegde criminaliteit minder relevant en laten we in dit onderzoek daarom buiten beschouwing. Op basis van inzichten uit de geregistreerde en ondervonden criminaliteit zal geprobeerd worden een schatting te doen van de totale omvang van online fraude bij bedrijven.

3.2 Schattingsmethoden en -technieken voor het dark number

Het *dark number* van criminaliteit bevat de delicten die zijn gepleegd, maar niet geregistreerd. Elk register of databron heeft een eigen *dark number* (Skogan, 1977). De uitdaging is om op basis van een combinatie van geregistreerde criminaliteit en uitgevraagde ondervonden criminaliteit dit *dark number* te benaderen. Omdat we nooit aan alle bedrijven kunnen vragen, of voor alle bedrijven kunnen bepalen, of ze slachtoffer zijn geweest van online fraude zullen we een onderbouwde schatting moeten maken. Hierbij moeten we rekening houden met de beperkingen van de verschillende databronnen. Bepaalde typen bedrijven of slachtoffers van bepaalde fraudevormen kunnen bijvoorbeeld eerder geneigd zijn de fraude aan te geven bij de politie of om te reageren op een enquête. We hebben in dit onderzoek drie relevante methoden ingezet, te weten slachtofferenquêtes, extrapolatie en de multipliermethode. Voor het inschatten van de betrouwbaarheid van de schattingen maken we vervolgens gebruik van triangulatie

3.2.1 Extrapolatie

Om een schatting te maken van de omvang van het slachtofferschap van online fraude op basis van een enquête wordt gebruik gemaakt van extrapolatie. Extrapolatie is het proces waarbij uitkomsten uit een steekproef of deelwaarneming worden doorgetrokken naar een grotere populatie, op basis van aannames over de representativiteit en samenhang tussen steekproef en populatie.

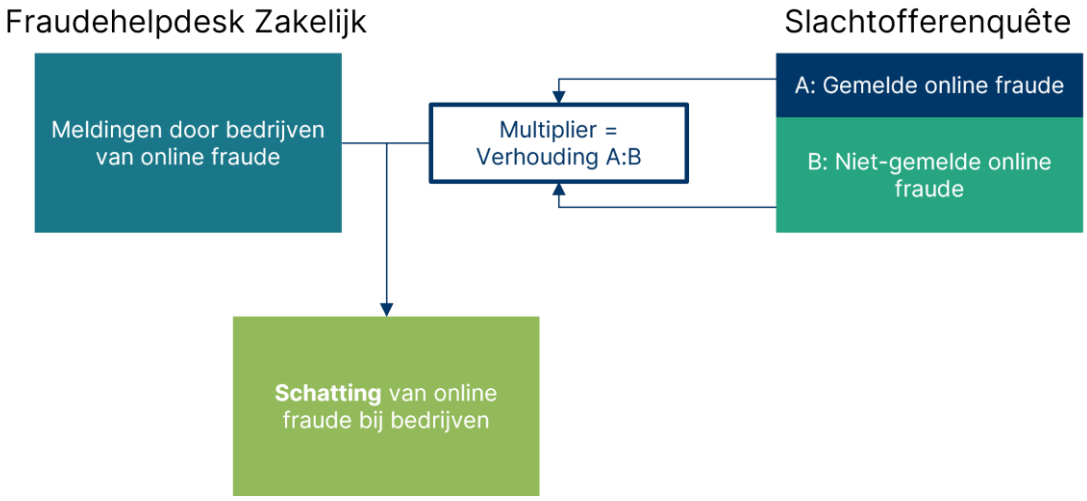
Hierbij maken we gebruik van 95%-betrouwbaarheidsintervallen. Dit interval wordt berekend op basis van het waargenomen aandeel slachtoffers in de steekproef en de steekproefomvang, en geeft een bereik waarbinnen de werkelijke proportie in de populatie met 95% zekerheid wordt verwacht. Het Wilson-interval (wat wij hier zullen gebruiken) biedt daarbij een betrouwbaardere schatting van de onzekerheidsmarge dan het standaardinterval, met name bij proporties en steekproeven van beperkte omvang (Wilson, 1927).

3.2.2 De multipliermethode

De data van verschillende registers die ingezet kunnen worden voor onderzoek naar online fraude zijn op zichzelf beperkt waardevol voor het maken van een schatting, omdat we niet weten welk percentage van slachtoffers het delict registreert. Met de multiplierbenadering kunnen we deze data verrijken en gebruiken voor het maken van een schatting. Door deze schatting te trianguleren met de resultaten van de slachtofferenquête kunnen we tot een meer robuuste schatting komen.

Multipliermethoden maken gebruik van twee databronnen. De ene bron is het geregistreerde deel van de te onderzoeken populatie en de tweede bron levert de vermenigvuldigingsfactor (of multiplier) op. De multiplier wordt bij voorkeur afgeleid uit representatief bevolkingsonderzoek, bijvoorbeeld een slachtofferenquête. Wanneer een dergelijke multiplier niet beschikbaar is, kan de andere bron ook bestaan uit expertinformatie, bijvoorbeeld de mate waarin experts aangeven dat online fraude door bedrijven wordt aangegeven bij de politie. Hierbij geldt uiteraard dat informatie uit representatieve bevolkingsonderzoek te verkiezen is boven een meer subjectieve bron als expertinformatie (Smit, et al., 2018).

De multiplier is de verhouding tussen het deel dat de online fraude heeft gemeld en het deel dat dit niet heeft gedaan. Deze verhouding kan anders zijn voor verschillende type bedrijven en verschillende fraudevormen en daarmee verschillende multipliers opleveren. De multiplier wordt vervolgens toegepast op de geregistreerde data (bijvoorbeeld Fraudehelpdesk Zakelijk) om tot een schatting van het totaal aantal slachtoffers te komen (Smit, et al., 2018).



Figuur 4. Voorbeeld van de werking van de multipliermethode. Bron: Smit, et al. (2018b). Bewerking: Dialogic.

Om de multipliermethode toe te passen moet aan een aantal voorwaarden worden voldaan. De slachtofferenquête moet representatief zijn voor de te onderzoeken

populatie. Ook moeten de gehanteerde definities van online fraude en de bevraagde fraudevormenvormen in de twee bronnen hetzelfde zijn en moeten ze dezelfde tijdsperiode beslaan (Smit, et al., 2018).

Daarnaast moeten alle fraudegevallen in beide databronnen correct geregistreerd zijn (Smit, et al., 2018). Dit is niet altijd het geval. Zo liet eerder onderzoek naar de validiteit van het combineren van politieregistraties en slachtofferenquêtes zien dat een groot deel van gerapporteerde aangiftes in de slachtofferenquête niet terug te vinden is in de politieregistraties. Van slechts 35% van de gerapporteerde aangiftes werd eenduidig een directe tegenhanger in het politieregistratiesysteem aangetroffen (Averdijk & Elffers, 2012; Elffers & van der Kemp, 2016). Dit betekent niet per se dat mensen in enquêtes (bewust of onbewust) niet de waarheid vertellen, het kan bijvoorbeeld ook zijn dat aangiftes of meldingen door de politie niet of onder een andere noemer worden geregistreerd. Idealiter moeten dergelijke vertekeningen ook mee worden genomen in de multiplier.

3.2.3 Triangulatie

Omdat het schattingen van een *dark number* blijven is het van belang om deze te valideren. Met triangulatie worden de uitkomsten van verschillende methoden en (combinaties van) bronnen met elkaar vergeleken om de geldigheid van de schattingen te toetsen (Smit, et al., 2018).

4 Inventarisatie van databronnen

Om inzicht te krijgen in de databronnen die informatie over online fraude bij bedrijven kunnen bieden, hebben we een inventarisatie gemaakt van databronnen die mogelijk inzicht kunnen geven in de verschillende aspecten van online fraude bij bedrijven.

Het doel van deze inventarisatie van databronnen was om tot een onderzoeksaanpak te komen waarmee we tot een representatieve schatting van de aard en omvang van schade door online fraude bij bedrijven kunnen komen.

Hieronder beschrijven we deze databronnen, waarbij we onderscheid maken tussen enerzijds meldpunten en registers en anderzijds slachtofferenquêtes. Per databron bespreken we de mogelijkheden van de bron, de inherente beperkingen van een databron, de beperkingen die voortkomen uit de huidige uitvoeringspraktijk van de databron, de implicaties die deze beperkingen hebben voor het gebruik in dit onderzoek en geven we direct een aantal aanbevelingen om de bruikbaarheid in de toekomst te verhogen. Specifiek bij de slachtofferenquêtes leggen wij uit hoe wij deze in ons hoofdonderzoek hebben ingezet.

We eindigen dit hoofdstuk met een conclusie waarin we beschrijven op welke wijze we de verschillende databronnen zullen combineren om tot een representatieve schatting te komen.

4.1 Meldpunten en registers

In Nederland zijn er vele meldpunten waar slachtoffers van fraude een melding kunnen maken. Tijdens de evaluatie van de Fraudehelpdesk in november 2023 is een lijst van 50 meldpunten geïdentificeerd waar slachtoffers fraude kunnen melden, waaronder de Consumentenbond, Informatiedesk FIOD en Slachtofferhulp Nederland (ProFacto, 2023). Meldingen van online fraude door bedrijven zijn daarom mogelijk dus sterk versnipperd. Uit de interviews en deskstudie kwamen vijf meldpunten naar voren die in dit onderzoek betrokken zouden kunnen worden, omdat ze a) landelijk dekkend zijn, b) zich richten op fraude of de gevolgen van fraude (financiële schade), c) meldingen (kunnen) registreren en d) toegankelijk zijn voor ondernemers.[6] Deze bronnen zijn:

1. Politieregistraties;
2. Fraudehelpdesk Zakelijk;
3. Verzekeraars met cybersecurity- of fraudeverzekeringen;

[6] Deze lijst is mogelijk niet uitputtend. Andere meldpunten of registers zijn in de deskstudie en interviews echter niet naar voren gekomen.

4. Banken met zakelijke klanten;
5. Landelijk Meldpunt Internetoplichting (LMIO).

Na gesprekken met deze bronhouders bleven alleen de politieregistraties en de Fraudehelpdesk Zakelijk over als databronnen, ieder met eigen beperkingen die we hieronder zullen toelichten. Daarnaast bespreken we in de hierop volgende secties uitgebreider waarom de verzekeraars, banken en het LMIO uiteindelijk niet over relevante data beschikten of deze konden leveren en hoe dat in de toekomst mogelijk wel gedaan kan worden.

4.1.1 Politieregistraties

Aard van de bron

De politie is een instantie waar slachtoffers aangifte of een melding kunnen doen van online fraude en het incident kunnen laten registreren.

Mogelijkheden van de bron

- **Registraties van fraude-incidenten.** Slachtoffers kunnen melding maken van hun fraude-incident waarmee dit incident in de politieregistraties geregistreerd wordt.

Beperkingen van de bron

- **Aangiftebereidheid**. Niet alle slachtoffers weten dat ze slachtoffer zijn of doen aangifte van online fraude-incidenten bij de politie. Daarnaast is niet duidelijk of hierin verschillen zitten tussen type bedrijven (zzp, mkb of groot) of tussen verschillende vormen van online fraude. Uit eerdere onderzoeken blijkt dat tussen de 6% en 14% van slachtoffers van cybercriminaliteit of gedigitaliseerde criminaliteit aangifte doet, maar ook dat de aangiftebereidheid van onlinecriminaliteit het grootst is onder eenmanszaken (CBS, 2018; van der Weijer, Leukfeldt, & van der Zee, 2020).

Beperkingen door de huidige uitvoeringspraktijk

- **Wijze van registreren**. De meldingen en aangiften die van online fraude worden gedaan kunnen niet eenduidig uit de politiesystemen worden gehaald. Ook kan niet van alle meldingen en aangiften worden vastgesteld of het een particulier slachtoffer of een ondernemer betrof en staat ook niet voor elke melding of aangifte een schadebedrag genoteerd. Hierdoor is niet altijd duidelijk of het poging tot fraude betreft of een daadwerkelijk fraude-incident met schade.
- **Inzicht in slachtoffer**. Als bekend is dat het slachtoffer een bedrijf is, dan kunnen wij alleen informatie ontvangen of het een zzp'er, mkb'er of ander bedrijf betrof. Er is geen verdere informatie beschikbaar over bijvoorbeeld bedrijfsgrootte of bedrijfssector.

- **Inzicht in fraudevormen**. Tot slot bevatten de politieregistraties niet alle fraudevormen. Zo worden aan- en verkoopfraude beperkt geanalyseerd omdat dit al door het Landelijk Meldpunt Internetoplichting wordt gedaan (waarover later meer).

Implicaties voor het onderzoek

Ondanks de beperkingen is de politie een groot landelijk meldpunt voor slachtoffers. De politieregistraties zijn daarmee een belangrijke bron voor inzichten over online fraude die we in dit onderzoek meenemen.

De inzichten over de omvang van online fraude bij bedrijven op basis van politieregistraties hebben een hoge mate van onzekerheid. Met de huidige uitvoeringspraktijk is niet met zekerheid vast te stellen welk deel van de meldingen en aangiften binnen de gehanteerde definitie van online fraude bij bedrijven vallen. Daarnaast wordt schade niet (consistent) geregistreerd.

Schattingen op basis van de politieregistraties zullen onzeker zijn en ook incompleet – over schade door online fraude die door bedrijven gemeld is bij de politie zullen we niks kunnen zeggen.

Aanbevelingen

Om in de toekomst meer en betrouwbaardere inzichten te kunnen halen uit de politieregistraties is het voor de politie aan te bevelen om:

- De registratiepraktijk te verbeteren door fraude op eenduidige wijze te registreren, bijvoorbeeld aan de hand van de in dit onderzoek voorgestelde taxonomie, en ook verplicht de mogelijke schade te registreren.
- Wanneer het slachtoffer een bedrijf is additionele informatie te registreren, zoals het type bedrijf (bijvoorbeeld zzp, mkb of grootbedrijf) en de bedrijfssector.

4.1.2 Fraudehelpdesk Zakelijk

Aard van de bron

De Fraudehelpdesk is een instantie waar slachtoffers melding kunnen doen van online fraude en het incident kunnen registreren. De Fraudehelpdesk heeft ook een zakelijk kanaal; de Fraudehelpdesk Zakelijk.

Mogelijkheden van de bron

- **Registraties van fraude-incidenten.** Zakelijke slachtoffers kunnen melding maken van hun fraude-incident waarmee dit incident bij de Fraudehelpdesk Zakelijk geregistreerd wordt.

- **Inzicht in de verschillende fraudevormen.** De Fraudehelpdesk Zakelijk classificeert elk fraude-incident waarmee inzicht wordt gekregen in de specifieke vorm van het fraude-incident.

Beperkingen van de bron

- **Meldingsbereidheid**. Niet alle ondernemers weten dat ze slachtoffer zijn en zullen melding maken van online fraude bij de Fraudehelpdesk. Daarnaast is niet duidelijk of hierin verschillen zitten tussen type bedrijven (zzp, mkb of groot) of tussen verschillende vormen van online fraude.

Beperkingen door de huidige uitvoeringspraktijk

- **Inzicht in slachtoffer**. Van zakelijke melders is geen verdere informatie beschikbaar over bijvoorbeeld bedrijfsgrootte of bedrijfssector.

Implicaties voor het onderzoek

De Fraudehelpdesk Zakelijk heeft waardevolle en omvangrijke informatie over fraude-incidenten, waardoor ze voor dit onderzoek waardevolle registraties bevatten. Deze registraties bevatten echter geen verdere informatie over de bedrijven die slachtoffer zijn geworden.

Daarnaast is niet duidelijk of de typen slachtoffers en geregistreerde fraude-incidenten bij de Fraudehelpdesk Zakelijk representatief zijn voor alle slachtoffers en fraude-incidenten. Het is bijvoorbeeld voorstelbaar dat slachtoffers met veel (directe) financiële schade eerder melding maken bij de Fraudehelpdesk Zakelijk dan slachtoffers met beperkte schade. Een schatting op basis van deze meldingen zou dan kunnen leiden tot een overschatting van de totale schade bij Nederlandse bedrijven door online fraude. Tegelijkertijd kan het ook zijn dat slachtoffers van fraude-incidenten met (zeer) hoge schade juist naar de politie gaan in plaats van een melding maken bij de Fraudehelpdesk Zakelijk, waardoor de schatting van de totale schade juist weer een onderschatting zou zijn.

Aanbevelingen

Meldingen bij de Fraudehelpdesk Zakelijk zouden in de toekomst nog waardevoller zijn voor wetenschappelijk onderzoek als:

- De Fraudehelpdesk Zakelijk meer gedetailleerde informatie over het slachtoffer zou vragen, zoals het type bedrijf (bijvoorbeeld zzp, mkb of grootbedrijf) en de bedrijfssector.

4.1.3 Verzekeraars met cybersecurity- of fraudeverzekeringen

Aard van de bron

Bedrijven kunnen bij verschillende partijen een cyber- of een fraudeverzekering afsluiten. Bij schade door online fraude kunnen deze bedrijven een claim indienen voor vergoeding van de schade.

Mogelijkheden van de bron

- **Inzicht in schade door online fraude**. Verzekeraars hebben inzicht in de aantallen claims van bedrijven met een dergelijke verzekering die ook dekking biedt voor online fraude.[7]

Beperkingen van de bron

- **Representativiteit van slachtoffers**. Uit eerdere onderzoeken weten we ook dat bedrijven die een cyberverzekering afsluiten vaak niet representatief zijn voor alle bedrijven – om aan de voorwaarden te voldoen moet de ICT en de beveiliging van een dermate hoog niveau zijn dat de kans veel kleiner is om slachtoffer te worden van een cyberaanval (Blom, et al., 2023).

Beperkingen door de huidige uitvoeringspraktijk

- **Variatie in polisvoorwaarden**. De polisvoorwaarden van de verzekeringen verschillen dermate dat het niet altijd duidelijk is of en in hoeverre online fraude gedekt wordt.
- **Beschikbaarheid data**. Data wordt niet centraal verzameld door bijvoorbeeld het Verbond van Verzekeraars. Inzichten moeten daarom bij iedere individuele verzekeraar opgevraagd worden.

Implicaties voor het onderzoek

De beperkingen van de bron zijn dermate groot dat ze niet opwegen tegen de mogelijkheden. De representativiteit van de slachtoffers is hierbij een beperking, maar met name het feit dat de data op dit moment niet beschikbaar is voor wetenschappelijk onderzoek maakt dat deze databron niet verder is meegenomen.

Aanbevelingen

Om in de toekomst wel verdiepende inzichten te krijgen in het verloop van fraude-incidenten en de daaruit voortvloeiende schade, zowel direct als indirect, zou het volgende gedaan kunnen worden:

[7] NB: hier zullen AVG technisch nog veel haken en ogen aan zitten.

- Verzekeraars die online fraude bij bedrijven dekken moeten geïdentificeerd worden door een analyse van de polisvoorwaarden of omdat verzekeraars dit expliciteren.
- Een centrale partij als het Verbond van Verzekeraars moet deze informatie gaan verzamelen.

4.1.4 Banken met zakelijke klanten

Aard van de bron

Zakelijke klanten bij de meeste Nederlandse banken kunnen bij een vorm van service-desk melding maken van fraude om ondersteuning te krijgen bij een fraude-incident.

Mogelijkheden van de bron

- **Registraties van fraude-incidenten.** Zakelijke slachtoffers kunnen hun bank om hulp vragen bij een fraude-incident waardoor dit incident in theorie geregistreerd kan worden.[8]
- **Inzicht in de verschillende fraudevormen.** Indien de banken een uniforme taxonomie adopteren zouden deze meldingen ook inzicht kunnen geven in de verschillende vormen van online fraude.
- **Inzicht in schade door online fraude**. Banken zijn bij uitstek de partij die inzicht zou kunnen geven in de schade die door slachtoffers wordt geleden.

Beperkingen van de bron

- **Meldingsbereidheid**. Niet alle ondernemers weten dat ze slachtoffer zijn en zullen dit melden bij hun bank. Daarnaast is niet duidelijk of hierin verschillen zitten tussen type bedrijven (zzp, mkb of groot) of tussen verschillende vormen van online fraude.

Beperkingen door de huidige uitvoeringspraktijk

- **Beschikbaarheid data**. Data over online fraude bij bedrijven wordt momenteel niet door banken verzameld.

Implicaties voor het onderzoek

Doordat deze data momenteel niet wordt verzameld kunnen we deze ook niet meenemen in dit onderzoek.

Aanbevelingen

De aanbeveling voor deze databron is eenduidig:

[8] NB: hier zullen AVG technisch nog veel haken en ogen aan zitten.

- Banken met zakelijke klanten moeten middels een uniforme taxonomie fraude-incidenten en schade gaan registreren.

4.1.5 Landelijk Meldpunt Internetoplichting (LMIO)

Aard van de bron

In het Landelijk Meldpunt Internetoplichting (LMIO) van de politie werkt de politie samen met het Openbaar Ministerie, banken, Marktplaats en internetserviceproviders. Deze samenwerking heeft als doel het terugdringen van internetoplichting (fraude bij online handel). Mensen die via online verkoopsites zijn opgelicht, kunnen dit melden via LMIO.

Mogelijkheden van de bron

- **Inzicht in aan- en verkoopfraude**. Meldingen en aangiften van aan- en verkoopfraude bij de politie verlopen via het LMIO. Het LMIO heeft ook inzicht in deze fraudevorm.

Beperkingen van de bron

- **Aangiftebereidheid**. Niet alle slachtoffers weten dat ze slachtoffer zijn en doen aangifte van online aan- en verkoopfraude bij de politie. Daarnaast is niet duidelijk of hierin verschillen zitten tussen type bedrijven (zzp, mkb of groot).

Beperkingen door de huidige uitvoeringspraktijk

- **Registratie van slachtoffer.** Het LMIO geeft aan geen onderscheid te maken tussen particuliere slachtoffers en bedrijven.

Implicaties voor het onderzoek

Omdat het LMIO überhaupt niet registreert of een melding of aangifte afkomstig is van een bedrijf kunnen we deze bron niet meenemen in dit onderzoek.

Aanbevelingen

De aanbeveling voor deze databron is eenduidig:

- LMIO zou bij meldingen van aan- en verkoopfraude moeten registreren of de melding afkomstig is van een bedrijf, en idealiter ook verdere informatie verzamelen over het type bedrijf.

4.2 Slachtofferenquêtes

Bij delicten met slachtoffers is het gangbaar om een representatieve slachtofferenquête te gebruiken als basis voor de schatting van de omvang (Groot, de Hoop, Houkes, & Sikkel, 2007). De vertaling van de uitkomsten van een representatieve

enquête naar de hele populatie gebeurt hierbij op basis van extrapolatie. Mocht de enquête niet (volledig) representatief zijn dan wordt dit gecorrigeerd op basis van weegfactoren.

In deze sectie beschrijven we drie type slachtofferenquêtes die binnen de kaders van dit onderzoek gebruikt kunnen worden voor het in kaart brengen van online fraude bij bedrijven:

1. Bestaande enquêtes over aanpalende onderwerpen of doelgroepen;
2. Een enquête onder een representatief ondernemerspanel;
3. Een enquête breed verspreid onder ondernemers.

Hieronder bespreken we deze drie.

4.2.1 Bestaande enquêtes

Aard van de bron

Partijen als banken, verzekeraars, wetenschappers en het CBS zetten regelmatig enquêtes uit onder hun klanten of de Nederlandse bevolking, ook op het gebied van online fraude. Een overzicht van de beschikbare slachtofferenquêtes van over online fraude is te vinden in Bijlage 3.

Mogelijkheden van de bron

- **Inzicht in de mate van online fraude bij bepaalde groepen/sectoren**. Bestaande enquêtes kunnen inzicht geven in de mate van online fraude bij een bepaalde doelgroep of sector die in de enquête is bevraagd.

Beperkingen van de bron

- **Slachtofferbias**. Bij de meeste slachtofferenquêtes moet rekening worden gehouden met een slachtofferbias. Slachtofferbias houdt in dat slachtoffers eerder geneigd zijn deel te nemen aan onderzoeken en enquêtes dan niet-slachtoffers. Dit bemoeilijkt een representatieve schatting (Gomes, Farrington, Maia, & Krohn, 2019; Cantor & Lynch, 2000).

Beperkingen door de huidige uitvoeringspraktijk

- **Aansluiting bij onderzoeksdoel en doelgroep**. Er is momenteel geen bestaande enquête die aansluit bij het onderwerp van dit onderzoek. Zo maakte een fraudeonderzoek van Allianz Trade bijvoorbeeld geen onderscheid tussen online en offline fraude (Allianz Trade, 2025) en een onderzoek van ABN AMRO naar cyberaanvallen nam alleen CEO-fraude mee als vorm van online fraude (ABN AMRO, 2024). De CBS Veiligheidsmonitor bevat wel vragen over online fraude, maar richt zich dan weer niet specifiek op bedrijven. Ook wordt in

bestaande enquêtes niet altijd duidelijk of een slachtoffer daadwerkelijk schade heeft opgelopen of dat er alleen een poging tot fraude is gedaan.

- **Onderzoeksverantwoording**. De onderzoeksverantwoording is bij enquêtes die banken en verzekeraars bijvoorbeeld uitzetten onder hun klanten beperkt. Zo is het niet duidelijk wat de definitie van slachtoffer is (is er alleen sprake van een poging of heeft iemand ook daadwerkelijk schade?), wat precies onder fraude wordt verstaan en hoe verschillende fraudevormen gedefinieerd zijn in de vragenlijst. Daarnaast is niet te achterhalen of de respondenten representatief zijn voor een bepaalde groep. Daarnaast kan een commerciële partij er baat bij hebben om een gevaar zo groot mogelijk te laten lijken, zodat mensen bijvoorbeeld meer geneigd zijn om een verzekering af te sluiten.

Implicaties voor het onderzoek

Doordat bestaande enquêtes niet aansluiten bij de in dit onderzoek gehanteerde definities van online fraude en niet specifiek gericht zijn op de doelgroep die in dit onderzoek centraal staat (bedrijven) nemen wij deze niet mee in dit onderzoek.

Aanbevelingen

Bestaande enquêtes zouden bij een volgend onderzoek naar online fraude bij bedrijven meegenomen kunnen worden als:

- De doelgroep en gehanteerde definities overeenkomen;
- Er transparantie is over de onderzoeksverantwoording.

De Monitor Criminaliteit Bedrijfsleven

We willen hier wel graag de Monitor Criminaliteit Bedrijfsleven van het CBS uitlichten, die vanaf 2026 wordt uitgevoerd. Online fraude zal ook onderdeel zijn van deze enquête onder ondernemers. Omdat online fraude slechts één van de vormen van criminaliteit is waar in deze enquête naar gevraagd zal worden zullen andere inzichten vergaard worden, maar kan de mate van online fraude onder ondernemers de komende jaren wel gevolgd worden.

4.2.2 Enquête onder ondernemerspanel

Aard van de bron

Bij een ondernemerspanel kan een enquête worden uitgezet onder ondernemers over of ze slachtoffer zijn geweest van online fraude, van welke vorm ze slachtoffer zijn geweest, welke schade ze daarvan hebben ondervonden en of ze hier melding van

hebben gemaakt. In dit onderzoek kiezen we voor deze aanpak en maken we gebruik van het ondernemerspanel van Ipsos I&O en hebben we een enquête uitgezet onder een representatieve steekproef (op basis van bedrijfsgrootte en -sector) van 600 Nederlandse bedrijven.

Mogelijkheden van de bron

- **Controle over definities en vraagstelling**. Bij het opstellen van een eigen enquête garanderen we dat de vraagstelling en de gehanteerde definities van online fraude bij bedrijven aansluiten bij de opgestelde taxonomie, zodat we de uitkomsten van de enquête ook volgens onze taxonomie kunnen analyseren.
- **Representatieve groep ondernemers.** Ondernemerspanels bevatten (vaak op basis van sector en bedrijfsgrootte) een representatieve groep ondernemers voor de volledige populatie van ondernemers. De uitkomsten van de steekproef kunnen daarmee geëxtrapoleerd worden naar de volledige populatie.
- **Gegarandeerde reactiegraad.** Uit verschillende interviews komt naar voren dat ondernemers, en met name mkb-bedrijven, niet graag enquêtes invullen: ze hebben er geen tijd voor en zien er het nut niet van in. Het voordeel van het gebruik van een ondernemerspanel is dat er een gegarandeerde reactiegraad is. Deze reacties kunnen vervolgens worden gewogen op basis van sector en bedrijfsgrootte.

Beperkingen van de bron

- **Slachtofferbias.** Ondernemers worden uitgenodigd om plaats te nemen in het ondernemerspanel van Ipsos I&O en hebben de keuze om mee te doen aan een specifieke enquête. Slachtoffers zijn mogelijk eerder geneigd deel te nemen aan deze enquête over slachtofferschap. Bij extrapolatie naar de gehele populatie zou dit daarmee leiden tot een overschatting van het totale aantal slachtoffers van online fraude.
- **Representativiteit ondernemers.** Eerder gaven we aan dat de representativiteit van de steekproef op basis van bedrijfsgrootte en sector het mogelijk maakt om de uitkomsten te extrapoleren naar de gehele populatie van ondernemers. We gaven daarnaast echter ook aan dat eerder onderzoek liet zien dat ondernemers niet graag enquêtes invullen. De groep die dat middels een ondernemerspanel wél doet, is daarmee mogelijk een bijzonder type ondernemer. Of dit ook invloed heeft op de representativiteit met betrekking tot slachtofferschap van online fraude is niet bekend.
- **Zelfrapportage**. Ondernemers moeten zelf rapporteren of ze in een bepaalde periode slachtoffer zijn geweest van online fraude. Men is hier niet altijd toe in staat is, bijvoorbeeld doordat ze zaken door elkaar halen, zijn vergeten of omdat ze het incident toeschrijven aan de verkeerde periode. Daarnaast kunnen mensen zich ook schamen voor het incident en hier niet over willen

rapporteren. Daarnaast is het mogelijk dat de ondernemer niet op de hoogte is van de online fraude die heeft plaatsgevonden binnen het bedrijf.

Beperkingen door de huidige uitvoeringspraktijk

- **Beperkt tot geen inzicht in verschillende fraudevormen.** Alhoewel de reactiegraad gegarandeerd is, is de reactie in absolute aantallen in dit onderzoek beperkt. Hierdoor kan een dergelijke enquête gebruikt worden om de algehele mate van online fraude bij bedrijven in kaart te brengen, maar niet om inzicht te krijgen in de verschillende fraudevormen. De respons is te laag om uitsplitsingen naar verschillende fraudevormen te maken.

Implicaties voor het onderzoek

We gebruiken de enquête onder het ondernemerspanel bij Ipsos I&O om inzicht te krijgen in de mate van online fraude bij bedrijven: hoeveel ondernemers hebben hier in 2024 mee te maken gehad? Bij de extrapolatie naar de populatie werken we met een 95% betrouwbaarheidsinterval. Omdat de grootte van de steekproef beperkt is, zijn de bandbreedtes van de schattingen relatief groot.

Naast grote bandbreedtes spelen er ook verschillende factoren mee die invloed hebben op de betrouwbaarheid van de schattingen. Slachtofferbias en zelfrapportage (waarbij mensen bijvoorbeeld ook delicten rapporteren uit een andere tijdsperiode) kunnen leiden tot een overschatting van het aantal fraude-incidenten in de gehele ondernemerspopulatie. Tegelijkertijd is het ook mogelijk dat de enquête leidt tot een onderschatting van het daadwerkelijke aantal slachtoffers doordat ondernemers niet op de hoogte kunnen zijn van online fraude binnen het bedrijf, (minder ernstige) fraude-incidenten zijn vergeten of niet hebben gemerkt dat ze slachtoffer zijn geweest van online fraude. Hoe deze factoren, die enerzijds kunnen leiden tot overschattingen en anderzijds tot onderschattingen, zich tot elkaar verhouden en wat dit exact betekent voor de schattingen weten we niet. Echter is het wel belangrijk deze mee te nemen bij het interpreteren van de betrouwbaarheid van de schattingen.

We gebruiken de enquête ook voor het bepalen van de multiplier voor de meldingen van online fraude in de politieregistraties en bij de Fraudehelpdesk Zakelijk. Eerdergenoemde factoren kunnen ook een rol spelen bij de schattingen op basis van de multipliermethode. De multipliermethode veronderstelt namelijk dat het type ondernemer dat plaatsneemt in een ondernemerspanel slachtoffer is dezelfde is als het type ondernemer dat slachtoffer wordt van online fraude en daar melding van maakt bij de politie of de Fraudehelpdesk Zakelijk. We weten niet in hoeverre dit waar is. Ook dit is belangrijk mee te nemen bij het interpreteren van de betrouwbaarheid van de schattingen op basis van de multipliermethode.

Aanbevelingen

De inherente beperkingen van slachtofferenquêtes onder panels zijn lastig te mitigeren. Wel is een het voor een toekomstige slachtofferenquête aan te raden om:

- Een grotere steekproef te trekken, zodat de enquête ook inzichten over fraudevormen en slachtoffertypen kan geven en de betrouwbaarheidsintervallen kleiner worden.

4.2.3 Enquête onder brede ondernemerspopulatie

Aard van de bron

Een enquête onder een ondernemerspanel geeft een gegarandeerde respons. Deze respons is (in dit onderzoek) in absolute aantallen beperkt en kan daarmee beperkt inzicht geven in de verschillende fraudevormen waar ondernemers slachtoffer van worden en het type ondernemer dat hier slachtoffer van wordt. Een breed uitgezette enquête onder de volledige ondernemerspopulatie kan hier meer inzicht in geven.

De slachtofferbias bij een dergelijke enquête zal echter dermate groot zijn dat deze enquête niet gebruikt kan worden voor het maken van schattingen over de omvang van slachtofferschap van online fraude. Een brede enquête en een enquête onder een ondernemerspanel kunnen daarmee complementair aan elkaar zijn.

In dit onderzoek is samen met VNO-NCW geprobeerd een brede groep ondernemers te bereiken met een enquête.[9] VNO-NCW heeft de aangesloten brancheverenigingen gevraagd de enquête te verspreiden onder hun leden. Na dit verzoek heeft de enquête twee maanden opengestaan en heeft VNO-NCW een reminder gestuurd aan de brancheverenigingen. Desalniettemin bleef de reactie van ondernemers beperkt tot enkele responses.

Mogelijkheden van de bron

- **Controle over definities en vraagstelling**. Bij het opstellen van een eigen enquête kan worden gegarandeerd dat de vraagstelling en de gehanteerde definities van online fraude bij bedrijven aansluiten bij de opgestelde taxonomie, zodat we de uitkomsten van de enquête ook volgens onze taxonomie kunnen analyseren.
- **Inzicht in respondenten/slachtoffers**. Beschikbare databronnen geven zeer beperkt inzicht in het slachtoffer zelf, zowel wat betreft bedrijfsgrootte als bedrijfssector. Met een eigen enquête kunnen we de achtergrond van de

[9] De enquête is dezelfde als door Ipsos I&O is voorgelegd aan het ondernemerspanel.

respondenten uitvragen zodat we de uitkomsten ook uit kunnen splitsen naar de verschillende typen slachtoffer.

- **Potentieel groot bereik.** VNO-NCW vertegenwoordigt 300.000 kleine, middelgrote en grote ondernemingen, waarmee het een grote dekking heeft onder het Nederlandse bedrijfsleven. Via haar dochtervereniging MKB-Nederland is dit bereik nog verder groter.
- **Inzicht in fraude-incidenten en sectorspecifieke verschillen.** Een groot aantal responses betekent dat we voldoende dekking en celvulling hebben om uitsplitsingen te maken naar fraudevormen en slachtoffertypes.

Beperkingen van de bron

- **Slachtofferbias**. Bedrijven die slachtoffer zijn geworden van online fraude zijn vermoedelijk eerder geneigd de enquête in te vullen, waarmee de steekproef niet meer representatief is voor de volledige populatie van bedrijven.
- **Zelfrapportage**. Bedrijven moeten zelf rapporteren of ze in een bepaalde periode slachtoffer zijn geweest van online fraude. Uit eerdere onderzoeken blijkt dat men hier niet altijd toe in staat is, bijvoorbeeld doordat ze zaken door elkaar halen of omdat ze het incident toeschrijven aan de verkeerde periode.

Beperkingen door de huidige uitvoeringspraktijk

- **Reactiegraad bij ondernemers**. Ondanks het feit dat de enquête is verspreid via VNO-NCW en de brancheverenigingen bleven de reacties van ondernemers beperkt tot enkele responses. Dit bevestigt nogmaals dat de doelgroep van ondernemers niet snel geneigd is deel te nemen aan dergelijke onderzoeken en hun tijd te besteden aan het invullen van enquêtes.

Implicaties voor het onderzoek

Doordat de respons zo beperkt was, kunnen we de resultaten van deze enquête niet verder meenemen in dit onderzoek.

Aanbevelingen

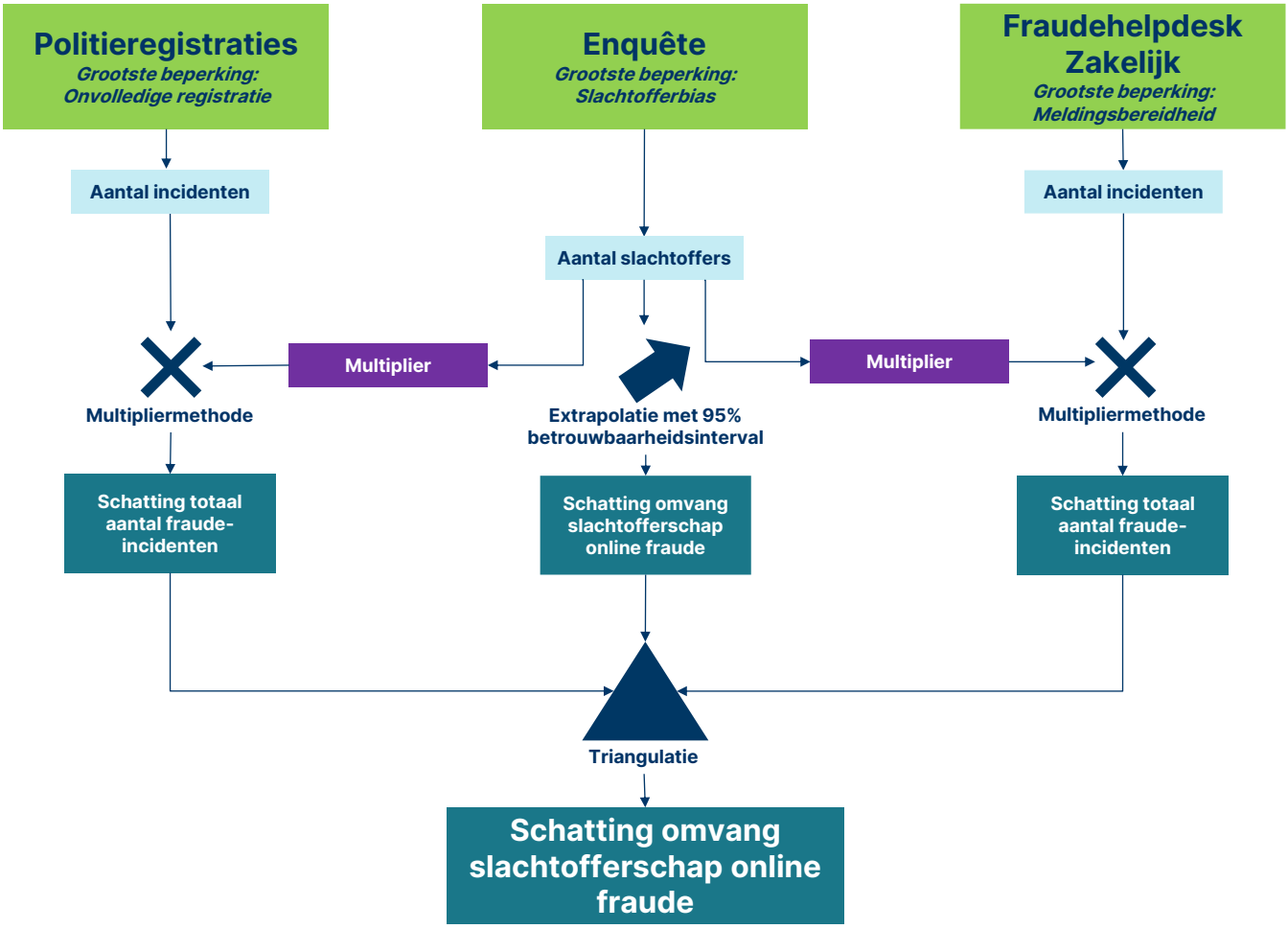
Wij verwachten niet dat ondernemers met een andere benaderingswijze wél *en masse* een enquête ingevuld zouden hebben. Om toch meer inzicht te krijgen in de aard van online fraude bij bedrijven is het daarom aan te bevelen om:

- Inspanningen te bundelen en aan te sluiten bij lopende slachtofferenquêtes. Een kansrijke monitor voor het in kaart brengen van de omvang van online fraude bij bedrijven is de Monitor Criminaliteit Bedrijfsleven van het CBS, die naar verwachting in 2026 uitgezet zal worden.
- Informatie over de aard van online fraude-incidenten bij ondernemers op een andere manier te verkrijgen dan via een brede enquête. Richt de inspanningen bijvoorbeeld op het verhogen van de meldingsbereidheid bij de politie of de

Fraudehelpdesk, zodat ondernemers deze informatie zelf (laten) registreren, of vergroot het bereik van een ondernemerspanel.

4.3 Conclusie

Het doel van de inventarisatie van databronnen was om tot een onderzoeksaanpak te komen waarmee we tot een representatieve schatting van de aard en omvang van schade door online fraude bij bedrijven kunnen komen. **De in dit hoofdstuk besproken beperkingen van de verschillende databronnen en de huidige uitvoeringspraktijk laten zien dat dit met de beschikbare data lastig is.** Onderstaande figuur toont desalniettemin hoe we, alle beperkingen in acht nemend, op basis van extrapolatie en de multipliermethode proberen te komen tot een drietal schattingen van het totale aantal fraude-incidenten en de omvang van het slachtofferschap. Deze schattingen kunnen we vervolgens trianguleren om de betrouwbaarheid van deze schattingen te toetsen.



Figuur 5. Overzicht databronnen en methoden om tot een schatting van de omvang van slachtofferschap door online fraude te komen.

De voor dit onderzoek beschikbare data bestaat uit politieregistraties, meldingen bij de Fraudehelpdesk Zakelijk en een enquête onder een ondernemerspanel van Ipsos I&O. Deze databronnen hebben allen beperkingen die van grote invloed zijn op de betrouwbaarheid van schattingen en mogelijk leiden tot over- en/of onderschattingen:

- Bij de politie zijn meldingen en aangiftes van online fraude onvolledig, waardoor het aantal incidenten van online fraude bij bedrijven in de registraties al een schatting is.
- De grootste beperking van de enquête is een mogelijke slachtofferbias. Dit zou bij extrapolatie naar de totale populatie tot een overschatting van de omvang van het aantal slachtoffers leiden. Daarnaast beperkt dit mogelijk ook de betrouwbaarheid van de multipliers die op basis van de enquête worden bepaald.
- Tot slot is de grootste beperking van de Fraudehelpdesk Zakelijk de meldingsbereidheid van slachtoffers, waardoor het aantal meldingen in absolute zin beperkt is.

5 Online fraude bij bedrijven

In het vorige hoofdstuk beschreven we alle beschikbare databronnen, de bijbehorende beperkingen en de methodologie om toch tot inzichten te komen in de totale omvang van online fraude bij bedrijven en de bijbehorende schade. Door alle beperkingen die met de beschikbare databronnen komen is de betrouwbaarheid van deze schattingen beperkt. Desalniettemin hopen we dat ze wel een indicatie geven van de omvang van en financiële schade door online fraude. De beschrijvingen van de politieregistraties, meldingen bij de Fraudehelpdesk Zakelijk en een enquête onder een ondernemerspanel van Ipsos I&O en de wijze waarop de data verwerkt is, zijn te vinden in respectievelijk Bijlage 4, Bijlage 5 en Bijlage 6.

5.1 Omvang slachtofferschap

De omvang van online fraude bij bedrijven brengen we in kaart aan de hand van het aantal bedrijven dat in 2024 slachtoffer was van online fraude en het aantal fraude-incidenten. Van de beschikbare databronnen geeft alleen de enquête onder een ondernemerspanel van Ipsos I&O inzicht in het aantal bedrijven dat slachtoffer was van online fraude in 2024. De Fraudehelpdesk Zakelijk vraagt geen specifieke gegevens uit over het slachtoffer, waardoor de meldingen van fraude-incidenten niet te ontdubbelen zijn en te achterhalen is of er sprake is van herhaald of meervoudig slachtofferschap. Ditzelfde geldt voor de dataset die door de politie aangeleverd is.

5.1.1 Enquête

Uit de enquête onder 600 bedrijven bleek dat 21 bedrijven slachtoffer waren van online fraude met directe financiële schade in 2024. Daarmee was 3,5% van de bedrijven uit de steekproef slachtoffer van online fraude. Om op basis hiervan een schatting te maken van het aantal bedrijven in Nederland dat in 2024 slachtoffer was van online fraude moeten we dit percentage uit de steekproef wegen naar de totale populatie van bedrijven. Een weging op basis van sector en bedrijfsgrootte zorgt voor een geschat percentage van 3,76% van alle Nederlandse bedrijven. Met een betrouwbaarheidsinterval van 95% rondom deze schatting betekent dit dat tussen de 2,24% en 5,28% van de Nederlandse bedrijven in 2024 naar schatting slachtoffer is geweest van online fraude.

Nederland kende in totaal 2.359.330 bedrijven in 2024[10], wat op basis van extrapolatie zou kunnen betekenen dat tussen de 52.849 en 124.573 bedrijven in 2024 slachtoffer waren van online fraude.

[10] Zie: [opendata.cbs.nl]

Gezamenlijk hebben de 21 slachtoffers uit de steekproef in 2024 te maken gehad met 32 incidenten van online fraude. Dertien bedrijven waren één keer slachtoffer geweest (enkelvoudig slachtoffer). Zeven slachtoffers gaven aan twee keer slachtoffer te zijn geweest van dezelfde fraudevorm en één bedrijf gaf zelfs aan vijf keer of meer slachtoffer te zijn geweest van dezelfde fraudevorm (herhaald slachtofferschap). Meervoudig slachtofferschap, waarbij hetzelfde bedrijf slachtoffer is van verschillende vormen van online fraude, kwam niet voor in de steekproef.

Op basis van extrapolatie van de steekproef (waarin 21 ondernemers samen slachtoffer waren van 32 fraude-incidenten) naar de volledige populatie zouden in 2024 tussen de 80.532 en 189.825 incidenten van online fraude bij bedrijven zijn geweest.[11]

5.1.2 Fraudehelpdesk Zakelijk

In totaal waren er in 2024 4.831 meldingen van fraude bij de Fraudehelpdesk Zakelijk. Na filtering van de data op meldingen van *online* fraude, blijkt dat er 2.924 meldingen van online fraude waren door bedrijven (de methode staat beschreven in Bijlage 5). Bij 14% van deze meldingen registreerde de Fraudehelpdesk Zakelijk directe schade (N = 420).

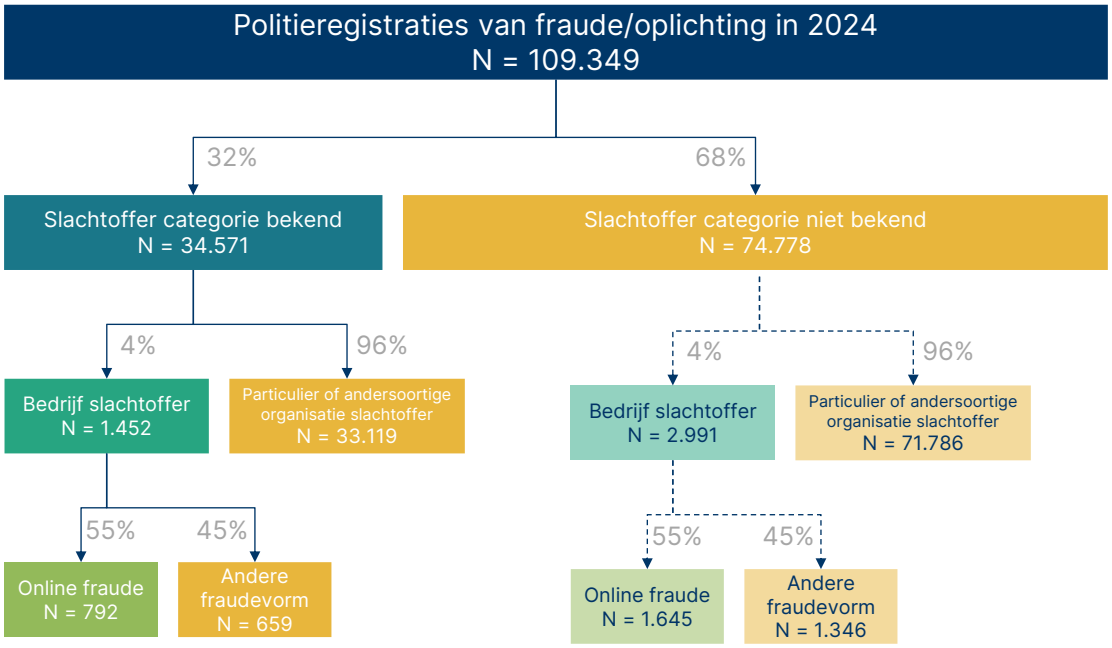
Uit de enquête onder ondernemers komt naar voren dat 10% van de incidenten door de slachtoffers gemeld is bij de Fraudehelpdesk Zakelijk, met een 95%-betrouwbaarheidsinterval van 3,6% tot 25%. In een interview met de Fraudehelpdesk Zakelijk gaven zij ook aan zelf uit te gaan van een meldingspercentage van ongeveer 10%. Dit meldingspercentage uit de enquête gebruiken we als multiplier om met behulp van de multiplier methode tot een schatting van het totale aantal incidenten te komen. **Dit zou op basis van de multipliermethode betekenen dat er in totaal tussen de 1.680 en 11.667 incidenten van online fraude met directe schade bij bedrijven waren in 2024.**

5.1.3 Politieregistraties

In totaal bevatte de dataset van politieregistraties in 2024 109.349 meldingen en aangiftes van fraude en oplichting. Van deze registraties is van 34.571 registraties (32%) de slachtoffercategorie bekend. Bij de opname van de melding of aangifte kan de desbetreffende agent in het aangifteformulier aangeven tot welke categorie het slachtoffer behoort. 1.452 van deze registraties (4%) vallen onder de categorie ‘Bedrijf’. Aan de

[11] Het is mogelijk dat onze steekproef een *outlier* bevat (de ondernemer die meer dan vijf keer slachtoffer werd van dezelfde vorm van online fraude), waardoor deze schatting van fraude-incidenten een overschatting is. Omdat de andere bronnen geen inzicht geven in herhaald of meervoudig slachtofferschap kunnen we echter niet met zekerheid zeggen of deze respondent een *outlier* is of niet.

hand van de eerder vastgestelde taxonomie classificeren wij vervolgens 792 registraties (55%) van deze meldingen/aangiftes als online fraude (zie Figuur 6).[12,13]



Figuur 6. Links: Het aantal registraties van online fraude bij bedrijven. Rechts: Een schatting van het aantal registraties van online fraude waarbij de slachtoffer categorie niet bekend is.

In totaal weten we van 792 politieregistraties dus dat het online fraude bij bedrijven betreft. Van een groot gedeelte van de in totaal 109.349 politieregistraties van fraude/oplichting is echter het type slachtoffer niet bekend. Echter zullen hier ook bedrijven tussen zitten en daarmee relevante meldingen/aangiftes. Als we ervanuit gaan dat 1) de verhouding tussen bedrijven en particulieren gelijk is bij politieregistraties waar de slachtoffer categorie bekend is en waar de slachtoffer categorie onbekend is en dat 2) de verhouding tussen online fraude en andere fraudevormen gelijk is bij politieregistraties waar de slachtoffer categorie bekend is en waar deze niet bekend is. Dan schatten we dat het totale aantal meldingen en aangiftes van online fraude door bedrijven bij de politie in 2024 2.437 is (N = 792 + 1.645), zie Figuur 6.

Niet alle fraude-incidenten worden door bedrijven geregistreerd bij de politie. Voor het maken van een schatting van de totale omvang gebruiken we daarom wederom de multipliermethode. In onze eigen enquête onder ondernemers hebben we slachtoffers gevraagd of zij melding hebben gemaakt of aangifte hebben gedaan bij de politie.

[12] Hierbij merken wij dus expliciet aan dat dit voor aan- en verkoopfraude een onderschatting is omdat deze bij het LMIO worden geclassificeerd.

[13] Andere fraudevormen zijn door de politie geregistreerd onder bijvoorbeeld ransomware, hacken, afpersing en overige fraude

Daaruit bleek dat 41% van de incidenten, met een 95%-betrouwbaarheidsinterval van tussen de 25% en 60%, uit 2024 door de slachtoffers gemeld was bij de politie of dat daar aangifte van was gedaan. **Op basis van de multipliermethode zou dit betekenen dat er in totaal tussen de 4.061 en 9.748 incidenten van online fraude bij bedrijven waren in 2024.** Een beperking hier is dat de multiplier gebaseerd is op slachtoffers van incidenten *met directe schade*, terwijl we bij de politieregistraties niet weten of het fraude-incident ook daadwerkelijk geleid heeft tot directe financiële schade.

5.1.4 Conclusie

Onderstaande tabel toont dat de schattingen van het aantal slachtoffers en het aantal incidenten op basis van de verschillende databronnen sterk uiteenlopen. **Het is daarmee niet mogelijk om een eenduidige, robuuste schatting van de omvang van online fraude bij bedrijven vast te stellen.**

Tabel 4. Overzicht van schattingen van aantal slachtoffers en aantal fraude-incidenten voor de verschillende databronnen.

Databron	Schatting (95% betrouwbaarheidsinterval)
Enquête ondernemerspanel	**Tussen de 52.849 en 124.573 *slachtoffers*** **Tussen de 80.532 en 189.825 *incidenten met directe schade***
Fraudehelpdesk Zakelijk	**Tussen de 1.680 en 11.667 *incidenten met directe schade***
Politieregistraties	**Tussen de 4.061 en 9.748 *incidenten***

De hoge schattingen op basis van de representatieve enquête kunnen duiden op slachtofferbias. Het verschil in schattingen op basis van meldingen bij de Fraudehelpdesk Zakelijk en de politie komt ook doordat we bij de politie niet kunnen selecteren op incidenten met schade, waardoor de registraties vermoedelijk ook incidenten bevatten zonder schade. De schattingen liggen echter dermate uit elkaar dat er niet op een betekenisvolle manier getrianguleerd kan worden.

5.2 Aard

In deze sectie kijken we ook naar de aard van online fraude bij bedrijven. Hierbij kijken we naar de slachtoffers, de verschillende vormen van online fraude en de wijze waarop slachtoffers door de fraudeurs zijn benaderd.

5.2.1 Slachtoffers

De politieregistraties en de meldingen bij de Fraudehelpdesk Zakelijk geven geen verdere inzichten in de kenmerken van bedrijven die in 2024 slachtoffer waren van online fraude en worden hier daarom niet verder beschreven.

Over de bedrijven die deelnamen aan de enquête, en slachtoffer waren van online fraude, is wel meer bekend. Onderstaande tabel toont bijvoorbeeld het percentage van bedrijven dat slachtoffer was van online fraude op basis van bedrijfsgrootte.

Tabel 5. Percentage slachtoffers per bedrijfsgrootte in steekproef ondernemerspanel.

Aantal medewerkers	Aantal in steekproef	Aantal slachtoffers	Percentage slachtoffer (95%-betrouwbaarheidsinterval)
0 t/m 1 medewerker	333	14	4,2% (2,9% - 6,1%)
2 t/m 4 medewerkers	133	4	3% (1,9% – 4,7%)
5 of meer medewerkers	134	3	2,2% (1,3% - 3,7%)

Zzp'ers en eenmanszaken lijken daarmee vaker slachtoffer te worden van online fraude dan bedrijven met meerdere werknemers. Onderstaande tabel toont daarnaast dat bedrijven in de steekproef uit de sector Industrie, bouw en nutsbedrijven (op basis van SBI-code) vaker slachtoffer lijken te worden dan bedrijven in de andere sectoren.

Tabel 6. Percentage slachtoffers per bedrijfssector op basis van SBI-code in steekproef ondernemerspanel

Sector	Aantal in steekproef	Aantal slachtoffers	Percentage slachtoffer (95%-betrouwbaarheidsinterval)
Landbouw/visserij (A)	21	0	-
Industrie, bouw en nutsbedrijven (BCDEF)	59	3	5% (3,5% - 7,0%)

Sector	Aantal in steekproef	Aantal slachtoffers	Percentage slachtoffer (95%-betrouwbaarheidsinterval)
Handel en logistiek, horeca (GHI)	87	2	2,3% (1,4% - 3,8%)
Financiële en zakelijke dienstverlening (JKLMN)	254	9	3,5% (2,3% - 5,3%)
Overheid, onderwijs, zorg en overig (OPQRSTU)	179	7	3,9% (2,6% - 5,8%)

5.2.2 Fraudevormen

De fraude-incidenten uit de verschillende databronnen hebben wij aan de hand van de door ons opgestelde taxonomie opnieuw geclassificeerd om hopelijk tot (een eenduidig) inzicht te komen over de fraudevormen die bij bedrijven in 2024 het meest voorkwamen. Tabel 7 toont per databron het aantal incidenten per fraudevorm en het aandeel van deze fraudevorm binnen de databron.

Bij de politie registreerden bedrijven die slachtoffer waren van online fraude het vaakst factuurfraude (30,1%), gevolgd door CEO-fraude (21,7%), identiteitsfraude (13,6%) en helpdeskfraude (13,1%). Hierbij merken we op dat aan- en verkoopfraude niet volledig mee zijn genomen in de analyse, omdat deze grotendeels registreert worden bij het LMIO. Bij de Fraudehelpdesk Zakelijk wordt daarentegen minder vaak melding gemaakt van factuurfraude (5,7%), maar het vaakst van aan- en verkoopfraude (34,3%) en acquisitiefraude (25,7%).[14] Ook in de enquête onder het ondernemerspanel geven respondenten aan het vaakst slachtoffer te zijn van aankoopfraude (37,9%) en verkoopfraude (27,6%).

[14] De verdeling van het aantal meldingen zonder directe financiële schade is te vinden in Bijlage 4.

Tabel 7. Aantal geregistreerde of rapporteerde incidenten per fraudevorm en databron.

Fraudevormen	Enquête		Politieregistraties		Fraudehelpdesk Zakelijk	
	N	%	N	%	N	%
1.1 Niet leveren van beloofde goederen of diensten						
1.1.a Aankoopfraude	11	37,9%	-	-	-	-
1.1.b Acquisitiefraude	3	10,3%	-	-	108	25,7%
1.1.c Beleggingsfraude	1	3,4%	13	1,6%	9	2,1%
1.1d. Recoveryfraude	-	-	-	-	2	0,5%
1.2 Aannemen van een valse identiteit						
1.2.a CEO-fraude	2	6,9%	172	21,7%	57	13,6%
1.2.b Helpdeskfraude	-	-	104	13,1%	19	4,5%
1.2.c Identiteitsfraude (werknemer)	-	-	108	13,6%	10	2,4%
1.3 Manipuleren van gegevens						
1.3.a Domeinnaamfraude	3	10,3%	-	-	-	-
1.3.b Factuurfraude	1	3,4%	238	30,1%	24	5,7%
1.3.c Betaalverzoekfraude	-	-	-	-	-	-
Misbruik bedrijfsgegevens	-	-	-	-	38	9,0%
Fraude bankgegevens	-	-	59	7,4%		
2.1 Niet voldoen aan betaling						
2.1.a Verkoopfraude	8	27,6%	-	-	-	-
Overig						
Aan- en verkoopfraude	-	-	46	5,8%	144	34,3%
Telecomfraude	-	-	13	1,6%	3	0,7%
Betaalmiddelfraude	-	-	39	4,9%	6	1,4%
Totaal	**29**	**100%**	**792**	**100%**	**420**	**100%**

Noot: Schuingedrukt staan de fraudevormen die niet één op één te koppelen zijn met een specifieke fraudevorm uit de taxonomie, maar wel binnen een categorie van online fraude vallen.

De meeste geregistreerde en gerapporteerde incidenten van online fraude bij bedrijven betreffen aan- en verkoopfraude. In de enquête zijn aankoopfraude en verkoopfraude gezamenlijk goed voor 66% van de gerapporteerde fraude-incidenten. Ook bij de Fraudehelpdesk betreft aan- en verkoopfraude met 34% de grootste categorie. Bij de politieregistraties is het aandeel van aan- en verkoopfraude lager (6%), maar wordt dit verklaart door het feit dat deze meldingen met name bij het LMIO worden geregistreerd.

Ten opzichte van de Fraudehelpdesk worden incidenten van factuurfraude, CEO-fraude, identiteitsfraude en helpdeskfraude relatief vaker gemeld bij de politie. Het aandeel van deze meldingen bij de politie is ook hoger dan in de enquête. Dit zou kunnen betekenen dat slachtoffers van deze fraudevormen dit als dusdanig ernstig ervaren dat ze dit melden bij de politie. Bij factuurfraude en CEO-fraude kan ook nog meespelen dat dit alleen tegen bedrijven gepleegd kan worden. In de politieregistraties is het voor deze fraudevormen dus duidelijk dat het slachtoffer een bedrijf is. Andere

fraudevormen kunnen ook gericht zijn tegen particulieren, waardoor deze mogelijk niet correct geregistreerd worden in de politieregistraties als online fraude bij bedrijven.

Acquisitiefraude wordt daarentegen juist vaker geregistreerd bij de Fraudehelpdesk dan bij de politie. Dit zou dan kunnen betekenen dat slachtoffers dit wel als fraude herkennen, maar niet als dusdanig ernstig dat ze ermee naar de politie gaan. Dit is echter speculatief, aangezien we de slachtoffers zelf niet hebben gevraagd.

5.2.3 Benadering van slachtoffers

Slachtoffers van online fraude kunnen op verschillende manieren benaderd worden door fraudeurs. Wanneer slachtoffers een fraude-incident registreren bij de Fraudehelpdesk Zakelijk wordt ook uitgevraagd hoe zij zijn benaderd. Bij deze meldingen was de benaderingswijze met name telefonisch[15] (29,8%) of via e-mail (28,6%). Bijlage 8 toont ook de benaderingsvormen bij fraude-incidenten zoals gerapporteerd in de enquête. Deze komen grotendeels overeen met de meldingen bij de Fraudehelpdesk Zakelijk. In de enquête was e-mail de meest voorkomende benaderingswijze (37,9%), gevolgd door webshop (24,1%) en telefonisch (17,2%).

In de dataset van de Fraudehelpdesk Zakelijk kunnen we ook kijken naar meldingen zonder directe schade. Waar de meeste benaderingen telefonisch gedaan worden door fraudeurs, wordt daar relatief minder vaak ook daadwerkelijk (directe) schade geregistreerd: maar in 8% van de gevallen.

De benaderingstechniek van de fraudeurs blijkt ook te verschillen per fraudevorm. Een telefonische benadering is bij bijna de helft van de fraudevormen de populairste manier om slachtoffers te benaderen. Bij Helpdeskfraude, Acquisitiefraude en Recoveryfraude gebruiken fraudeurs zelfs in 85% of meer van de gevallen deze benaderingsvorm. Daarnaast vindt aankoopfraude vaak plaats op een webshop (59%) en worden slachtoffers bij CEO-fraude en Factuurfraude het vaakst benaderd via de email (respectievelijk 70% en 67%). Met uitzondering van Misbruik bedrijfsgegevens is één benaderingsvorm voor iedere fraudevorm dominant (mimimaal 30% van de incidenten). Dit kan betekenen dat er voor elke fraudevorm een voorkeursbenadering is of dat fraudeurs een voorkeursbenadering hebben en daar de meest geschikte fraudevorm voor gebruiken

5.2.4 Conclusie

Deze sectie ging over de aard van online fraude bij bedrijven, waarbij we hebben gekeken naar verschillende typen slachtoffers, fraudevormen en benaderingswijzen. Over

[15] N.B. in sommige (wetenschappelijke) studies wordt fraude via de telefoon niet gezien als online fraude.

de aard van de slachtoffers (zoals bedrijfsgrootte of -sector) kunnen we op basis van de in dit onderzoek ontsloten databronnen beperkt inzichten geven.

Van de fraudevormen die wij hebben opgenomen in de taxonomie van online fraude bij bedrijven komt aan- en verkoopfraude het vaakst voor. Bij aan- en verkoopfraude wordt veelal gebruik gemaakt van webshops (in 52% van de incidenten). Over het algemeen gezien vindt het merendeel van de online fraude-incidenten echter plaats via de telefoon of e-mail. Bij een telefonische benadering is het slagingspercentage (waarbij het slachtoffer daadwerkelijk geld overmaakt aan de fraudeur) echter het laagst.

Er zijn verschillen zichtbaar in de geregistreerde fraudevormen tussen de verschillende databronnen. Dit kan komen door de verschillende wijze van registreren of doordat slachtoffers andere overwegingen maken bij het melden van een fraude-incident. We zien bijvoorbeeld dat factuurfraude, CEO-fraude, identiteitsfraude en helpdeskfraude meer bij de politie worden geregistreerd dan bij de Fraudehelpdesk Zakelijk, terwijl acquisitiefraude juist weer vaker wordt gemeld bij de Fraudehelpdesk Zakelijk. Dit kan onderliggende oorzaken hebben in perceptie van de ernst van het incident of toegankelijkheid van het meldpunt, maar ook worden toegeschreven aan de wijze van registratie. Hier kunnen we op basis van deze data geen uitspraken over doen.

5.3 Omvang schade

Tot slot kijken we verder naar de omvang van de directe financiële schade bij bedrijven door online fraude in 2024.

5.3.1 Fraudehelpdesk Zakelijk

In totaal zijn er 420 meldingen van online fraude waarbij bedrijven directe schade hebben gemeld.[16] De totale schade van deze 420 meldingen is €3.415.972. **Gemiddeld betaalden de bedrijven per incident €8.919 aan de fraudeur, met een mediaan van €720.** Het hoogste schadebedrag voor een enkel incident is €353.925 en het kleinste €2. Deze brede spreiding blijkt ook uit de standaarddeviatie van € 29.601. Onderstaande tabel toont de schade per fraudevorm.

[16] In 39 gevallen gaven ondernemers aan wel te hebben betaald aan de tegenpartij, maar is het schadebedrag € 0,-. Het kan hierbij zijn dat de ondernemer het exacte schadebedrag niet weet of niet wil doorgeven. Deze meldingen nemen we niet mee in de schattingen van de omvang van de directe financiële schade.

Tabel 8: Overzicht meldingen en schade door online fraude gemeld bij de Fraudehelpdesk Zakelijk in 2024.

Fraudevormen	Aantal incidenten	Totaal schade-bedrag	Gemiddeld schade-bedrag	Mediaan	Min.	Max.
1.1 Niet leveren van beloofde goederen of diensten	**134**	**€ 273.022**	**€ 2.703**	**€ 478**	**€ 12**	**€ 63.000**
1.1.b Acquisitiefraude	108	€ 95.402	€ 1.048	€ 478	€ 12	€ 15.000
1.1.c Beleggingsfraude	9	€ 113.620	€ 14.203	€ 2.810	€ 250	€ 53.000
1.1d. Recoveryfraude	2	€ 64.000	€ 32.000	€ 1.000	€1.000	€ 63.000
1.2 Aannemen van een valse identiteit	**86**	**€ 424.717**	**€ 5.243**	**€ 1.200**	**€ 6**	**€ 173.064**
1.2.a CEO-fraude	57	€ 71.998	€ 1.309	€ 800	€ 150	€ 11.000
1.2.b Helpdeskfraude	19	€ 325.784	€ 18.099	€ 4.055	€ 6	€ 173.064
1.2.c Identiteitsfraude (werknemer)	10	€ 26.935	€ 3.367	€ 3.383	€ 1.500	€ 5.000
1.3 Manipuleren van gegevens	**62**	**€ 2.019.291**	**€ 37.394**	**€ 14.795**	**€ 12**	**€ 353.925**
1.3.b Factuurfraude	24	€ 924.507	€ 44.024	€ 25.163	€ 300	€ 180.895
Misbruik Bedrijfsgegevens	38	€ 1.094.784	€ 33.176	€ 10.800	€ 12	€ 353.925
2.1 Niet voldoen aan betaling	**0**	-	-	-	-	-
Overig	**153**	**€ 698.942**	**€ 4.857**	**€ 380**	**€ 2**	**€ 125.000**
Aan- en verkoopfraude	144	€ 669.188	€ 4.800	€ 369	€ 13	€ 125.000
Telecomfraude	3	€ 152	€ 76	€ 76	€ 2	€ 150
Betaalmiddelfraude	6	€ 29.602	€ 5.920	€ 1.371	€ 860	€ 25.000
Totaal	**420**	**€ 3.415.972**	**€ 8.919**	**€ 720**	**€ 2**	**€ 353.925**

Noot: Schuingedrukt staan de fraudevormen die niet één op één te koppelen zijn met een specifieke fraudevorm uit de taxonomie, maar wel binnen een categorie van online fraude vallen. Fraudevormen zonder meldingen zijn niet opgenomen in de tabel.

Met ruim €2 miljoen schade zorgen misbruik van bedrijfsgegevens en factuurfraude (fraudecategorie 'Manipuleren van gegevens') gezamenlijk voor 59% van de geregistreerde schade door online fraude bij de Fraudehelpdesk Zakelijk. Voor deze twee fraudevormen ligt het gemiddelde schadebedrag ook relatief hoog, met respectievelijk €33.176 en €44.024. Wat opvalt is dat het schadebedrag voor bijna elke fraudevorm sterk uiteenloopt. Slachtoffers van helpdeskfraude hebben bijvoorbeeld of €6 of €173.064, - betaald aan de fraudeur.

Ook hier kunnen we op basis van de multipliermethode een schatting maken van de totale omvang van de schade door online fraude. Uit de enquête onder ondernemers komt naar voren dat 10% van slachtoffers de incidenten gemeld heeft bij de Fraudehelpdesk Zakelijk, met een 95%-betrouwbaarheidsinterval van 3,6% tot 25%. **Dit betekent dat de totale omvang van de schade door online fraude bij ondernemers op basis van meldingen bij de Fraudehelpdesk Zakelijk in 2024 tussen de €14 miljoen en €95 miljoen lag.**

5.3.2 Enquête

Ook in de enquête zijn slachtoffers gevraagd naar het directe schadebedrag. Onderstaande tabel toont deze antwoorden. **Het gemiddelde schadebedrag is €1.360 en de mediaan €575.** Onderstaande tabel toont de schade per fraudevorm.

Tabel 9: Overzicht meldingen en schade door online fraude bij respondenten in de steekproef.

Fraudevormen	Aantal incidenten	Totaal schade-bedrag	Gemiddeld schade-bedrag	Mediaan	Min.	Max.
1.1 Niet leveren van beloofde goederen of diensten	**15**	**€ 14.475**	**€ 965**	**€ 325**	**€ 32**	**€ 5.000**
1.1a. Aankoopfraude	11	€ 3.845	€ 350	€ 300	€ 32	€ 750
1.1.b Acquisitiefraude	3	€ 5.630	€ 1.877	€ 350	€ 280	€ 5.000
1.1.c Beleggingsfraude	1	€ 5.000	€ 5.000	€ 5.000	€ 5.000	€ 5.000
1.2 Aannemen van een valse identiteit	**2**	**€ 800**	**€ 400**	**€ 400**	**€ 400**	**€ 400**
1.2.a CEO-fraude	2	€ 800	€ 400	€ 400	€ 400	€ 400
1.3 Manipuleren van gegevens	**4**	**€ 4.835**	**€ 1.208**	**€ 700**	**€ 185**	**€ 700**
1.3.a Domeinnaamfraude	3	€ 1.585	€ 528	€ 700	€ 185	€ 700
1.3.b Factuurfraude	1	€ 3.250	€ 3.250	€ 3.250	€ 3.250	€ 3.250
2.1 Niet voldoen aan betaling	**8**	**€ 15.250**	**€ 3.250**	**€ 1.500**	**€ 250**	**€ 11.000**
2.1a Verkoopfraude	5	€ 15.350	€ 3.250	€ 1.500	€ 250	€ 11.000
Totaal	**26**	**€ 35.360**	**€ 1.360**	**€ 575**	**€ 32**	**€ 11.000**

Bij drie incidenten van verkoopfraude is het schadebedrag niet gerapporteerd door de respondent en deze zijn daarom niet meegenomen. Fraudevormen die in de steekproef niet voorkwamen zijn niet opgenomen in de tabel.

Als we deze schadebedragen in de steekproef extrapoleren naar de Nederlandse populatie van ondernemers, dan lag de directe financiële schade door online fraude in 2024, met een betrouwbaarheidsinterval van 95%, tussen de €90 miljoen en €211 miljoen.

5.3.3 Conclusie

Op basis van extrapolatie en de multipliermethode komen we met een 95%-betrouwbaarheidsinterval voor respectievelijk de enquête onder ondernemers en meldingen bij de Fraudehelpdesk tot onderstaande schattingen van de omvang van schade door online fraude bij bedrijven (zie onderstaande tabel).

Tabel 10. Overzicht van schattingen van omvang van de schade voor de verschillende databronnen.

Databron	Schatting (95% betrouwbaarheidsinterval)
Enquête ondernemerspanel	**Tussen de €90 miljoen en €211 miljoen directe financiële schade**
Fraudehelpdesk Zakelijk	**Tussen de €14 miljoen en €95 miljoen directe financiële schade**

De schatting van de totale omvang van de schade ligt op basis van de enquête hoger dan op basis van meldingen bij de Fraudehelpdesk Zakelijk. Dit terwijl zowel de mediaan als het gemiddelde schadebedrag van meldingen bij de Fraudehelpdesk Zakelijk hoger ligt (zie Tabel 11).

Tabel 11. Overzicht van gemiddeld schadebedrag en de mediaan van de gerapporteerde schadebedragen van de verschillende databronnen.

Databron	Gemiddeld schadebedrag	Mediaan schadebedrag
Enquête ondernemerspanel	€1.360	€575
Fraudehelpdesk Zakelijk	€8.919	€720

Dit verschil kan deels worden verklaard doordat de fraudevormen met de hoogste schadebedragen bij de Fraudehelpdesk Zakelijk (factuurfraude en misbruik bedrijfsgegevens) beperkt voorkwamen in de steekproef (slechts één keer). Daarnaast kan het zijn dat slachtoffers met hoge schade eerder geneigd zijn dit te melden bij de Fraudehelpdesk, waardoor het gemiddelde schadebedrag hoger ligt bij deze meldingen.

6 Conclusies, reflecties en aanbevelingen

Dit onderzoek laat zien dat de op dit moment beschikbare databronnen ontoereikend zijn voor een eenduidige, robuuste en betrouwbare schatting van de aard en omvang van de schade door online fraude bij bedrijven. In dit hoofdstuk bespreken we de belangrijkste conclusies en beperkingen en geven we een aantal aanbevelingen om in de toekomst mogelijk tot betere schattingen te komen.

6.1 Conclusies en reflecties

Een eenduidige taxonomie is een randvoorwaarde om de aard en omvang van online fraude in het Nederlandse bedrijfsleven in kaart te kunnen brengen. Er bestond nog geen taxonomie voor het classificeren van verschillende fraudevormen bij bedrijven. Zonder taxonomie zullen schattingen beïnvloed worden door overlappende definities en categorieën van online fraude bij verschillende bronnen. De taxonomie opgesteld in dit onderzoek biedt een basis voor classificatie en registratie van online fraude.

Figuur 7: Taxonomie van online fraude bij bedrijven.

De momenteel beschikbare databronnen hebben allen beperkingen die van invloed zijn op de betrouwbaarheid van mogelijke schattingen. In dit onderzoek hebben we een inventarisatie gedaan van databronnen met informatie over online fraude bij bedrijven. Daarbij zijn een viertal bronnen naar voren gekomen:

1. *Politieregistraties*. Politieregistraties vormen een belangrijke bron voor inzichten over online fraude door doordat zij een groot landelijk meldpunt zijn voor slachtoffers. **De registratiepraktijk bij de politie is echter onvoldoende voor het in kaart brengen van slachtofferschap van online fraude**. Meldingen en aangiftes zijn vaak onvolledig, waarbij niet duidelijk is of het slachtoffer een bedrijf of een particulier is, er geen eenduidige definities zijn voor verschillende fraudevormen en schadebedragen ontbreken.
2. *Fraudehelpdesk Zakelijk*. De Fraudehelpdesk Zakelijk is een online meldpunt voor bedrijven voor fraude. **Data van de Fraudehelpdesk Zakelijk bevat uitgebreide en consistente informatie over fraude-incidenten en fraudevormen**. Bij de Fraudehelpdesk Zakelijk wordt echter geen informatie verzameld over de kenmerken van bedrijven die melding maken, waardoor deze databron geen verdere inzichten kan bieden over het type bedrijven dat slachtoffer wordt.
3. *Enquête onder ondernemerspanel.* We hebben een enquête uitgezet onder een representatief panel van 600 ondernemers van Ipsos I&O. In deze enquête hebben we succesvol gebruik gemaakt van de opgestelde taxonomie voor online fraude. Middels extrapolatie hebben we een schatting kunnen maken van online fraude bij bedrijven en multipliers vast kunnen stellen voor gebruik van de multipliermethode op de registerdata. **Het aantal slachtoffers in de steekproef is echter te klein om inzicht te krijgen in de aard van online fraude bij bedrijven en het is aannemelijk dat er sprake is van slachtofferbias in de steekproef.**
4. *Enquête onder ondernemerspopulatie.* We hebben via VNO-NCW en MKB-Nederland een enquête uitgezet bij de aangesloten brancheverenigingen. **Hier hebben we (nogmaals) ondervonden dat ondernemers niet graag enquêtes invullen.** De respons was dermate beperkt dat deze databron niet gebruikt kon worden.

De schattingen van de aard en omvang van schade door online fraude verschillen sterk tussen de verschillende databronnen. Onderstaande tabellen laten de schattingen van het aantal slachtoffers, het aantal incidenten van online fraude en de omvang van de schade zien. Doordat we werken met betrouwbaarheidsintervallen en een kleine steekproef van slachtoffers, zijn de bandbreedtes van de schattingen groot.

Tabel 12. Overzicht van schattingen van aantal slachtoffers en aantal fraude-incidenten voor de verschillende databronnen. De politieregistraties bevatten geen (betrouwbare) informatie over financiële schade door fraude-incidenten.

Databron	Schatting (95% betrouwbaarheidsinterval)
Enquête ondernemerspanel	**52.849 - 124.573** ***slachtoffers*** **80.532 - 189.825** ***incidenten met directe schade***
Fraudehelpdesk Zakelijk	**1.680 - 11.667** ***incidenten met directe schade***
Politieregistraties	**4.061 - 9.748** ***incidenten***

Tabel 13. Overzicht van schattingen van omvang van de schade voor de verschillende databronnen. De politieregistraties bevatten geen (betrouwbare) informatie over financiële schade door fraude-incidenten.

Databron	Schatting (95% betrouwbaarheidsinterval)
Enquête ondernemerspanel	**€90 miljoen - €211 miljoen** ***directe financiële schade***
Fraudehelpdesk Zakelijk	**€14 miljoen - €95 miljoen** ***directe financiële schade***

De schattingen op basis van extrapolatie van de responses uit de steekproef zijn hoger dan de schattingen op basis van de multipliermethode met de politieregistraties en meldingen bij de Fraudehelpdesk Zakelijk. Dit doet vermoeden dat er bij de enquête sprake is van slachtofferbias, dat leidt tot een overschatting, maar het laat ook de beperkingen van de multipliermethode zien. We weten dat ondernemers niet graag enquêtes invullen. Het is dus de vraag hoe representatief het type ondernemer is dat plaatsneemt in een panel voor enquêtes. Als deze ondernemers bijvoorbeeld eerder geneigd zijn om een fraude-incident te melden bij de politie of de Fraudehelpdesk Zakelijk, dan is het meldingspercentage in de steekproef hoger dan in de gehele populatie. Een te hoog meldingspercentage leidt met de multipliermethode leidt vervolgens tot een onderschatting van het totaal aantal fraude-incidenten.

De meeste geregistreerde en gerapporteerde incidenten van online fraude bij bedrijven betreffen aan- en verkoopfraude. Incidenten van factuurfraude, CEO-fraude, identiteitsfraude en helpdeskfraude worden relatief vaker gemeld bij de politie, acquisitiefraude wordt daarentegen juist vaker geregistreerd bij de Fraudehelpdesk. Aan- en verkoopfraude vindt veelal plaats op webshops, terwijl de andere fraudevormen veelal telefonisch of via e-mail plaatsvinden.

Het schatten van het *dark number* van online fraude blijft een zeer uitdagende exercitie. Dit is een conclusie die algemeen bekend is, maar dit onderzoek laat nogmaals

zien dat een goede registratiepraktijk essentieel is voor het in kaart brengen van een dergelijk fenomeen. Desalniettemin blijven de schattingsmethoden zeer gevoelig voor inherente beperkingen van bronnen, zoals slachtofferbias en meldingsbereidheid.

6.2 Aanbevelingen

Voor beter zicht op online fraude bij bedrijven is het van belang dat er in de toekomst meer data wordt verzameld, en dat de beschikbare data van betere kwaliteit is. Om dit te bereiken bevelen we een aantal zaken aan:

- **De registratiepraktijk bij de politie moet structureel worden verbeterd**. De politie is een belangrijk landelijk meldpunt waar slachtoffers zich melden. Voor inzicht in dit slachtofferschap is het noodzakelijk dat de politie in ieder geval gaat registreren of de melder een bedrijf of particulier is en welke directe financiële schade het fraude-incident tot gevolg had. Het verplicht maken van bepaalde velden in de registratie zoals slachtoffertype en schade bij het opnemen van de melding of aangifte zou hiertoe een eerste stap zijn.
- Bij het maken van een *dark number* schatting zullen meerdere databronnen gecombineerd moeten worden. **Het is daarom van belang om een gezamenlijke taxonomie voor online fraude bij bedrijven te hanteren, zoals is voorgesteld in dit rapport.** Door gebruik te maken van dezelfde definities en afbakeningen, kan data vergeleken worden en sluit het op elkaar aan. Door de centrale positie van de Fraudehelpdesk in het landschap kan overwogen worden hen hiervoor verantwoordelijk te maken.[17]
- Voor inzicht in slachtoffertypes zou door de Fraudehelpdesk Zakelijk overwogen kunnen worden ook informatie over de bedrijven, zoals de bedrijfssector en de bedrijfsgrootte, uit te vragen bij de melders. Wanneer meer zicht is op slachtoffertypes kunnen **beleidsinterventies gericht worden ontwikkeld voor de preventie en bestrijding van online fraude**.
- Ondernemers zijn een notoir lastige doelgroep om te bereiken met een enquête. Het is daarom aan te raden om **inspanningen te bundelen en aan te sluiten bij lopende slachtofferenquêtes.** Een kansrijke monitor voor het in kaart brengen van de omvang van online fraude bij bedrijven is de Monitor Criminaliteit Bedrijfsleven van het CBS, die naar verwachting in 2026 uitgezet zal worden.

[17] Dit is in lijn met één van de opgestelde ontwikkelrichtingen voor de Fraudehelpdesk uit de evaluatie van de organisatie in 2023 (Pro Facto, 2023).

7 Verwijzingen

ABN AMRO. (2024). *Steeds verfijndere cyberaanvallen schudden ondernemers nog lang niet altijd wakker. Sectorrapport 2024.*

Allianz Trade. (2025). *Jaarlijks fraudeonderzoek in Nederland en België. Trendrapport 2025.*

Averdijk, M., & Elffers, H. (2012). The discrepancy between survey-based victim accounts and police reports revisited. *International review of victomology*, pp. 91-107.

Beals, M., DeLiema, M., & Deevy, M. (2015). Framework for a taxonomy of fraud. *Financial Fraud Research Center*.

Bloem, B., & Harteveld, A. (2024). *Online fraude in beeld: Fenomeenbeeld 2024.* Driebergen: Nationale politie, Eenheid Landelijke Expertise en Operaties (LX).

Blom, T., Sahebali, W., Deppe, K., Romijn, P., Donath, F., & Brennenraedts, R. (2023). *Ransomware-aanvallen op instellingen en bedrijven in Nederland.* Den Haag: WODC.

Bullée, J.-W., & Junger, M. (2020). *Social engineering: digitale fraude en misleiding.* WODC. Opgehaald van https://repository.wodc.nl/bitstream/handle/20.500.12832/817/JV202002-artikel8.pdf?sequence=10&isAllowed=y

Cantor, D., & Lynch, J. (2000). Self-report surveys as measures of crime and criminal victimization. *Criminal Justice*, pp. 85-138.

CBS. (2018). *Cybersecuritymonitor 2018: Een verkenning van dreigingen, incidenten en maatregelen.* Den Haag: Centraal Bureau voor de Statistiek.

Elffers, H., & van der Kemp, J. (2016, 4). Als je nou politiecijfers combineert met slachtofferenquêtes, dan... ben je nog nergens. Wat nu? *preprintversie Cahiers Politiestudies Meten is Weten*, pp. 43-55.

Gomes, H., Farrington, D., Maia, A., & Krohn, M. (2019). Measurement bias in self-reports of offending: a systematic review of experiments. *Journal of Experimental Criminology*.

Groot, I., de Hoop, T., Houkes, A., & Sikkel, D. (2007). *De kosten van criminaliteit. Een onderzoek naar de kosten van criminaliteit voor tien verschillende delicttypen. .* Den Haag: WODC.

Leukfeldt, R., Notté, R., & Malsch, M. (2018). *Slachtofferschap van online criminaliteit. Een onderzoek naar behoeften, gevolgen en verantwoordelijkheden na slachtofferschap van cybercrime en gedigitaliseerde criminaliteit.* Den Haag: WODC.

Openbaar Ministerie. (n.b.). *Fraude*. Opgehaald van Openbaar Ministerie: https://www.om.nl/onderwerpen/fraude

Pro Facto. (2023). *Evaluatie Fraudehelpdesk.* Opgehaald van https://open.overheid.nl/documenten/dpc-8b4cea33f8c62c933880eafdaf09121c22c42cf2/pdf

ProFacto. (2023). *Evaluatie Fraudehelpdesk.* Groningen: Pro Facto.

Skogan, W. (1977). Dimensions of the dark figure of unreported crime. *Crime & Delinquency 23.1*, pp. 41-50.

Smit, P., Ghauharali, R., van der Veen, H., Willemsen, F., Steur, J., te Velde, R., . . . Bongers F. (2018). *Tasten in het duister. Deel 2: Technisch rapport.* Den Haag: WODC.

UNODC/UNECE. (2012). *Principles and Framework for an International Classification of Crimes for Statistical Purpose.* Conference of European Statistics.

van der Weijer, S., Leukfeldt, E., & van der Zee, S. (2020). *Slachtoffer van onlinecriminaliteit, wat nu? Een onderzoek naar de aangiftebereidheid onder burgers en ondernemers.* Den Haag: Sdu Uitgevers.

Wilson, E. (1927). *Probable Inference, the Law of Succession, and Statistical Inference.* Journal of the American Statistical Association.

Bijlage 1. Overzicht interviewrespondenten en gesproken personen

Organisatie	Positie
Avans Hogeschool	Lector Cyberweerbare Organisaties van het Centre of Expertise Veiligheid & Veerkracht
Centrum voor Criminaliteitspreventie en Veiligheid (CCV)	Teamleider ondernemen
Fraudehelpdesk	Adviseur
Nationale politie	Projectleider Datagedreven Werken
Nederlandse Vereniging van Banken	Beleidsadviseur integrale fraude
Platform Veilig Ondernemen (PVO)	Themaspecialist cyberweerbaarheid
Regionaal Informatie- en Expertisecentrum (RIEC) Noord-Nederland	Aanjager digitale weerbaarheid
Verbond van Nederlandse Ondernemingen - Nederlands Christelijk Werkgeversverbond (VNO-NCW)	Beleidsadviseur

Bijlage 2. Vragenlijst

Introductie

Voor u ligt een enquête over **online fraude** bij bedrijven in **2024**. Deze enquête is onderdeel van een onderzoek dat in opdracht van het WODC wordt uitgevoerd en waarbij VNO-NCW en MKB-Nederland zijn betrokken.

Wat bedoelen we met online fraude bij bedrijven?

Bij online fraude wordt uw bedrijf door een fraudeur benaderd (via telefoon, mail, WhatsApp, etc.) of komt op een online platform in contact met een fraudeur die u misleidt om zakelijk geld over te maken, betaalgegevens af te staan of producten te leveren waarvoor niet wordt betaald.

Het invullen van de enquête duurt ongeveer 5 minuten en is anoniem. **Als uw bedrijf geen slachtoffer is geweest van online fraude vragen we u ook om de enquête in te vullen.** Deze informatie is nodig om te bepalen hoe vaak online fraude bij bedrijven voorkomt.

Onderdeel 1: Achtergrondkenmerken

1. **Hoeveel mensen zijn er werkzaam in uw bedrijf (inclusief uzelf)? [Dropdown]**
    a. ZZP
    b. Microbedrijf: minder dan 10 werkzame personen
    c. Kleinbedrijf: 10 tot 50 werkzame personen
    d. Middenbedrijf: 50 tot 250 werkzame personen
    e. Grootbedrijf: Meer dan 250 werkzame personen

In het geval van Ipsos I&O de indeling: 0 t/m 1 medewerker, 2 t/m 4 medewerkers 5 of meer medewerkers.

2. **Wat is uw functie in dit bedrijf?**

[Open veld]

In het geval van Ipsos I&O de indeling: Zelfstandige/directeur/eigenaar/manager vestiging, HRM-contactpersoon, Anders, namelijk:

3. **In welke sector is uw bedrijf actief? [Dropdown]**
    - A. Landbouw, bosbouw en visserij
    - B. Winning van delfstoffen
    - C. Industrie
    - D. Productie en distributie van en handel in elektriciteit, gas, stoom en gekoelde lucht
    - E. Winning/distributie van water; afval/ en afvalwaterbeheer en sanering
    - F. Bouwnijverheid

- G. Groot- en detailhandel
- H. Vervoer en opslag
- I. Logies-, maaltijd- en drankverstrekking
- J. Activiteiten van uitgeverijen, omroepactiviteiten, en activiteiten op het gebied van productie en distributie van inhoud
- K. Telecommunicatie, computerprogrammering en consultancy, informatica-infrastructuur en overige activiteiten op het gebied van informatiediensten
- L. Activiteiten op het gebied van financiële dienstverlening en verzekeringen
- M. Exploitatie van en handel in onroerend goed
- N. Wetenschappelijke en technische activiteiten en specialistische zakelijke dienstverlening
- O. Verhuur van roerende goederen en overige zakelijke dienstverlening
- P. Openbaar bestuur, overheidsdiensten en verplichte sociale verzekeringen
- Q. Onderwijs
- R. Gezondheids- en welzijnszorg
- S. Kunst, cultuur, sport en recreatie activiteiten
- T. Overige dienstverlening
- U. Activiteiten van huishoudens als werkgever en niet-gedifferentieerde productie van goederen en diensten door huishoudens voor eigen gebruik
- U. Activiteiten van extraterritoriale organisaties en instanties

Ispos I&O voegt deze sectoren samen in de volgende clusters: A Landbouw/visserij; BCDEF Industrie, bouw en nutsbedrijven; GHI Handel en logistiek, horeca; JKLMN Financiële en zakelijke dienstverlening; OPQRSTU Overheid, onderwijs, zorg en overig.

Onderdeel 2: Zakelijk slachtofferschap online fraude

4. **Van welke vormen van online fraude was uw bedrijf <u>in 2024</u> slachtoffer?** *(Meerdere antwoorden mogelijk)*
    a. **Aankoopfraude**: Uw bedrijf heeft zakelijk iets online gekocht en is opgelicht
    b. **Verkoopfraude**: Uw bedrijf heeft zakelijk iets online verkocht en is opgelicht
    c. **Factuurfraude**: Een fraudeur heeft aan uw bedrijf een gemanipuleerde of valse digitale factuur verstuurd en deze is aan de fraudeur betaald
    d. **Acquisitiefraude**: Uw bedrijf werd digitaal benaderd voor het plaatsen van advertenties of het werven van opdrachten en heeft hiervoor betaald, maar dit is nooit, of niet zoals beloofd, gebeurt
    e. **Beleggingsfraude**: Uw bedrijf heeft belegd in iets waarbij hoge rendementen werden beloofd, maar de investering bleek vals, niet te bestaan of waardeloos te zijn

f. **CEO-fraude:** Een fraudeur deed zich voor als hooggeplaatst persoon (bijvoorbeeld de CEO) bij uw bedrijf en op diens verzoek is een bedrag overgemaakt aan de fraudeur
g. **Identiteitsfraude (werknemer):** Een fraudeur deed zich digitaal voor als een medewerker van uw bedrijf en op diens verzoek is een betaling, zoals een salaris, overgemaakt
h. **Bankhelpdeskfraude:** Een fraudeur deed zich voor als medewerker van een bank en uw bedrijf heeft betaalgegevens afgegeven of een overboeking gedaan aan deze fraudeur
i. **Helpdeskfraude:** Een fraudeur deed zich voor als medewerker van een andere helpdesk en uw bedrijf heeft betaalgegevens afgegeven of een overboeking gedaan aan deze fraudeur
j. **Betaalverzoekfraude**: Een fraudeur stuurde uw bedrijf een betaalverzoek die is betaald en via dit betaalverzoek heeft de fraudeur uw betaalgegevens afgevangen
k. **Domeinnaamfraude**: Een fraudeur heeft uw bedrijf overtuigd een domeinnaam te registreren die sterk op die van uw bedrijf lijkt, maar waar vele malen te veel voor is betaald
l. **Recoveryfraude:** Uw bedrijf heeft betaald om eerder verloren geld uit fraude terug te krijgen, maar deze hulp werd niet geboden of leidde tot extra geldverlies
m. **Mijn bedrijf is op een andere manier online opgelicht**
n. **Mijn bedrijf was in 2024 geen slachtoffer van online fraude**

Onderdeel 3: Beschrijving [FRAUDEVORM]

5. **[Als 4 != n] Hoe vaak was uw bedrijf slachtoffer van [FRAUDEVORM] in 2024?**
    a. 1 keer
    b. 2 keer
    c. 3 keer
    d. 4 keer
    e. 5 keer of meer

[Afhankelijk van vraag 5 onderstaande vragen meerdere keren doorlopen] Per incident beantwoordt u onderstaande vragen.
Bij meerdere vormen van fraude max 2 vormen uitvragen (willekeurig) en vragen naar laatste 2 incidenten.

6. **Hoe heeft uw bedrijf contact gehad met de fraudeur?** *[Meerdere antwoorden mogelijk]*
    a. Telefonisch (bellen)
    b. SMS
    c. E-mail

d. Online chat dienst (zoals Whatsapp of Signal)
e. Social media (zoals LinkedIn, Instagram, X of Facebook)
f. Online handelsplaats (zoals Marktplaats of Ebay)
g. Webshop
h. Weet ik niet
i. Anders, namelijk:

7. Kunt u het incident hieronder beschrijven? Probeer daarbij zoveel mogelijk identificeerbare gegevens te vermijden.

a. [Open veld]

8. Heeft uw bedrijf door de fraude geld verloren?

a. Ja
b. Nee
c. Weet ik niet

9. **[Als 9 = a] Heeft uw bedrijf nog andere financiële schade ondervonden als gevolg van het fraude-incident?** Bijvoorbeeld: verloren tijd, nieuwe systemen, advocaten, etc.

a. Ja
b. Nee

10. [Als 10 = a] Waar bestond deze schade uit en hoe groot was deze?

a. Open veld + geen antwoord / weet ik niet

11. Heeft uw bedrijf het fraude-incident ergens gemeld?

Meerdere antwoorden mogelijk.

a. Aangifte en ondertekend bij Politie
b. Melding maar geen aangifte bij Politie
c. Fraudehelpdesk particulier
d. Fraudehelpdesk zakelijk
e. Landelijk Meldpunt Internetoplichting
f. Melding bij de Bank
g. Anders, namelijk:
h. Nee, ik heb het fraude-incident niet gemeld
i. Weet ik niet

13. Welke acties zijn er binnen uw bedrijf ondernomen ten behoeve van veilig online gedrag?

a. Er zijn adviezen/richtlijnen/regels over online veilig gedrag van medewerkers
b. De toegang tot bepaalde websites en/of socialmediakanalen is geblokkeerd

c. Er is binnen mijn organisatie/bedrijf een digitale hulpverlener waar je terecht-kunt
d. Er wordt getoetst op veilig online gedrag door bijvoorbeeld op willekeurige momenten nep phishingmails te sturen
e. Er zijn afspraken gemaakt over het gebruik van zakelijke apparaten smartphones, laptops en/of tablets voor privé en/of zakelijk gebruik
f. Alleen de systeembeheerders kunnen software installeren
g. Twee-staps-inloggen is verplicht voor toegang
h. Er worden trainingen gegeven binnen mijn organisatie over online veiligheid
i. Anders, namelijk:
j. Weet ik niet
k. In mijn bedrijf of organisatie is geen actie ondernomen ten behoeve van veilig online gedrag

Onderdeel 4: Afsluiting

Heeft u nog verdere opmerkingen over het incident of deze vragenlijst?

[open invulveld]

Bedankt voor het invullen van de vragenlijst!

Bijlage 3. Onderzochte slachtofferenquêtes

Om meer inzicht te krijgen in online fraude in het Nederlandse bedrijfsleven worden door partijen als banken en verzekeraars regelmatig enquêtes uitgezet onder hun klanten. In totaal zijn tien slachtofferenquêtes onderzocht om te inventariseren welk inzicht zij kunnen geven in de aard en omvang van online fraude bij bedrijven.

De slachtofferenquêtes zijn beoordeeld op volledigheid, validiteit, betrouwbaarheid en actualiteit. Deze analyse is uitgewerkt via een stoplichtmodel: groen = toereikend, oranje = deels toereikend en rood = niet toereikend. In het geval van volledigheid is een bron bijvoorbeeld toereikend als het inzicht biedt in online fraude bij alle Nederlandse bedrijven. Een bron is deels toereikend als het inzicht biedt een subset van Nederlandse bedrijven of fraudevormen en een bron is niet toereikend als deze niet toeziet op Nederlandse bedrijven, maar bijvoorbeeld op Nederlandse particulieren of bedrijven in het buitenland.

De uitkomsten van slachtofferenquêtes worden meestal gepubliceerd in rapportages en vormen de meest voorkomende databron voor online fraude. Echter, veel van de gevonden enquêtes **sluiten niet geheel aan bij de onderzoeksvraag** van het huidige onderzoek. Zo gaan sommige enquêtes wel over online fraude maar niet over bedrijven, terwijl andere enquêtes wel over bedrijven gaan maar niet specifiek over financiële schade. In de onderstaande tekst beschrijven we de dikgedrukte selectie uit de onderstaande tien gevonden slachtofferenquêtes aan de hand van het stoplichtmodel. De overige enquêtes zijn op voorhand al aangewezen als niet toereikend doordat de niet over online fraude gaan of niet over bedrijven.

1. **Jaarlijks fraudeonderzoek in Nederland en België (2025) Alianz Trade**
2. **Steeds verfijndere cyberaanvallen schudden ondernemers nog lang niet altijd wakker (2024) ABN AMRO**
3. **Global Fraud trends (2024) Ravelin**
4. **CBS veiligheidsmonitor**
5. **CBS ICT gebruik bij bedrijvenOnline veiligheid en criminaliteit (2024) CBS**
6. **Online veiligheid en criminaliteit (2024) CBS**
7. Cybercriminaliteit in de coronacrisis (2023) NSCR
8. Cybersecurity onderzoek Alert Online (2024) Ipsos I&O
    - Deelrapport bedrijfsleven
9. ESET mkb Digital Security Sentiment Report (2022) ESET
10. Fraudevictimisatie in Nederland (2022) Junger et al.

Fraude Trendrapport van Allianz Trade

Allianz Trade maakt een voert jaarlijks een onderzoek uit naar fraude in het bedrijfsleven in Nederland en België en rapporteerd hierover in een trendrapport. Het rapport

beschrijft op basis van een enquête verschillende vormen van fraude, de schade die bedrijven lijden en maatregelen die worden genomen. Omdat deze enquête beperkingen heeft op gebied van volledigheid, validiteit en betrouwbaarheid, is het geen geschikte databron om mee te nemen in het hoofdonderzoek.

Volledigheid	Alleen bedrijven/organisaties met een jaaromzet van minstens €10 miljoen en minimaal 50 medewerkers
Validiteit	Allianz Trade definieert fraude in het rapport als opzettelijke misleidingen om onrechtmatig voordeel te verkrijgen. Dit sluit aan bij onze definitie van fraude. Echter worden verschillende fraudevormen generieker beschreven dan in onze taxonomie, bijvoorbeeld als het 'ontvreemden van documenten'. Daarentegen sluit het onderzoek wel aan bij andere fraudevormen, zoals factuurfraude, kopersfraude (vergelijkbaar met aankoopfraude) en betalingsfraude (vergelijkbaar met betaalverzoekfraude).
Betrouwbaarheid	In de rapportage van het onderzoek is de methodologische verantwoording zeer beperkt. De respondenten (type bedrijf en functie respondent binnen bedrijf) worden wel beschreven, maar het ontbreekt aan transparantie over de wijze waarop deze zijn benaderd, de exacte vraagstelling en de wijze waarop de antwoorden op de vragen zijn geanalyseerd.
Actualiteit	Jaarlijks terugkerende enquête

ABN AMRO onderzoek cyberaanvallen

ABN AMRO heeft is samenwerking met onderzoeksbureau MWM2 een enquêteonderzoek gedaan naar het aantal cyberaanvallen onder Nederlandse bedrijven. Het onderzoek gaat met name over cybercrime. Omdat deze enquête veel beperkingen heeft op gebied validiteit en actualiteit, is het geen geschikte databron om mee te nemen in het hoofdonderzoek.

Volledigheid	In totaal werden 895 ondernemers ondervraagd, waarvan 139 zzp'ers, 524 mkb-bedrijven (jaaromzet tot 25 miljoen euro) en 232 grote bedrijven (jaaromzet vanaf 25 miljoen euro).
Validiteit	Het onderzoek gaat over cyberaanvallen in alle vormen en is dus niet specifiek gericht op online fraude. Het onderzoek richt zich met name op cybercrime (malware, datalekke, randsomeware, etc.), hoewel phising en CEO fraude ook benoemd worden. Het

	rapport doet alleen generieke uitspraken over de omvang van de financiële schade.
Betrouwbaarheid	De methode is toereikend beschreven.
Actualiteit	Een eenmalige enquête uit 2024.

Ravelin Global fraud trends

Deze internationale enquête is uitgevoerd onder 1457 deskundigen die werken in bedrijven die online producten en diensten aanbieden. Verschillende veelvoorkomende vormen van fraude in de ecommerce worden besproken. Omdat deze enquête beperkingen heeft op gebied van volledigheid, validiteit en betrouwbaarheid, is het geen geschikte databron om mee te nemen in het hoofdonderzoek.

Volledigheid	(Wereldwijde) Bedrijven met een jaaromzet van meer dan $50 miljoen en/of meer dan 500 werknemers. Het onderzoek is gericht op ecommerce bedrijven, die online producten en diensten verkopen (retail, reissector, digitale middelen, markplaatsen).
Validiteit	Data wordt uitgesplitst naar sector. Financiële schade wordt op een ordinale schaal benoemd. De vormen van fraude die benoemd worden zijn: fraude met online betalingen, 'chargeback' (terugbetaling) fraude, misbruik van promoties, vouchers en polissen, misbruik van terugbetalingen, leverancier-, partner- en verkopersfraude. In hoeverre deze begrippen overlap hebben met de taxonomie van het huidige onderzoek is niet geheel duidelijk.
Betrouwbaarheid	De methode is toereikend beschreven.
Actualiteit	Jaarlijkse enquête.

CBS Veiligheidsmonitor

De Veiligheidsmonitor is een landelijke monitor waarmee zowel op landelijk als regionaal/lokaal niveau informatie over de veiligheid in Nederland wordt verzameld. Omdat deze enquête beperkingen heeft op gebied van volledigheid en validiteit, is het geen geschikte databron om mee te nemen in het hoofdonderzoek.

Volledigheid	De veiligheidsmonitor is een bevolkingsonderzoek en daarmee niet gericht op bedrijven, maar op personen. Tegen betaling zou de enquête in de CBS-microdata gekoppeld kunnen worden om te achterhalen of de personen ondernemer zijn. Dit zou interessant kunnen zijn in het kader van de zzp'er. De bron zelf geeft echter geen inzicht in bedrijven.
Validiteit	Geeft alleen inzicht in aan- en verkoopfraude
Betrouwbaarheid	Er zijn geen zorgen over de betrouwbaarheid van het CBS
Actualiteit	Tweejaarlijks terugkerende enquête

CBS ICT-gebruik bij bedrijven

De enquête 'ICT-gebruik bij bedrijven' meet jaarlijks gegevens over de automatisering en de toepassing van informatie- en communicatietechnologie (ICT) bij bedrijven in Nederland. In de vragenlijst wordt niet specifiek gevraagd naar online fraude. Wel wordt er gevraagd naar de mate waarin bedrijven incidenten melden, waardoor het voor triangulatie een nuttige databron kan zijn. Omdat deze enquête veel beperkingen heeft op het gebied van validiteit, is het geen geschikte databron om mee te nemen in het hoofdonderzoek.

Volledigheid	In Nederland gevestigde bedrijven met 10 en meer werkzame personen, bedrijven met 2 tot 10 werknemers en zzp'ers. De opgehaalde informatie kan op bedrijfsniveau tegen betaling beschikbaar worden gesteld in de CBS-microdata omgeving.
Validiteit	De vragenlijst haalt informatie op over ICT-veiligheidsincidenten bij bedrijven, en vraagt daarbij specifiek naar incidenten die 'door externen' zijn veroorzaakt, en welke kosten daarmee gemoeid gingen. Fraude is een subset van incidenten 'door externen', maar daar wordt niet specifiek naar gevraagd.
Betrouwbaarheid	Er zijn geen zorgen over de betrouwbaarheid van het CBS
Actualiteit	Jaarlijks terugkerende enquête

CBS-onderzoek Veiligheid en Criminaliteit (OVeC)

In 2022 heeft het CBS een onderzoek uitgevoerd naar online veiligheid en criminaliteit onder de Nederlandse bevolking. In de OVeC vragenlijst wordt onderscheid gemaakt naar vier soorten online fraude (aan- en verkoopfraude, fraude bij betalingsverkeer & identiteitsfraude).

De opgehaalde informatie kan op persoonsniveau tegen betaling beschikbaar worden gesteld in de CBS-microdataomgeving. Daarmee kan het gekoppeld worden aan persoons- en bedrijfskenmerken. Omdat deze enquête veel beperkingen heeft op gebied van volledigheid en actualiteit, is het geen geschikte databron om mee te nemen in het hoofdonderzoek.

Volledigheid	Het betreft een bevolkingsonderzoek en is daarmee niet gericht op bedrijven, maar op personen. Tegen betaling zou de enquête in de CBS-microdata gekoppeld kunnen worden om te achterhalen of de personen ondernemer zijn. Dit zou interessant kunnen zijn in het kader van de zzp'er. De bron zelf geeft echter geen inzicht in bedrijven.
Validiteit	Geeft inzicht in aan- en verkoopfraude, betalingsverkeer fraude en identiteitsfraude. Het onderzoek maakt echter geen onderscheid tussen online en offline fraude.
Betrouwbaarheid	Er zijn geen zorgen over de betrouwbaarheid van het CBS
Actualiteit	Het onderzoek is drie jaar oud en niet terugkerend

Bijlage 4. Politieregistraties

Wanneer bedrijven weten dat ze slachtoffer zijn van online fraude kunnen ze hiervan aangifte of melding doen bij de politie. De politie beschikt daarmee over relevante data met betrekking tot online fraude bij bedrijven. In dit hoofdstuk beschrijven we deze politieregistraties en de beperkingen van de dataset die we hebben ontvangen en analyseren we deze.

7.1.1 Beschrijving

Aangiften en meldingen worden door de politie geregistreerd in de Basisvoorziening Handhaving (BVH). Om inzicht te krijgen in de cyberincidenten die in de BVH staan geregistreerd is door de Dienst Landelijke Informatieorganisatie (DLIO) de Landelijke Cybercrime Query (LCQ) ontwikkeld (Bloem & Harteveld, 2024). Voor iedere verschijningsvorm is op basis van literatuur en in samenspraak met experts een tekstquery[18] opgesteld. De resultaten van de LCQ worden vervolgens handmatig geclassificeerd naar de verschijningsvorm van cybercriminaliteit in een specifieke en gestandaardiseerde database genaamd BlueIntel. *Fraude/oplichting* is één van de categorieën die hier wordt aangehouden (Bloem & Harteveld, 2024). Deze meldingen zijn binnen de hoofdcategorie ingedeeld in verschillende thema's (subcategorieën) en type benadeelde. Politieregistraties in BlueIntel bevatten alleen fraude-incidenten die als zodanig succesvol geregistreerd worden. Omdat de politieregistraties op geaggregeerd niveau aangeleverd zijn, kunnen we in de data niet achterhalen hoeveel bedrijven achter de meldingen zitten, en of dit unieke slachtoffers zijn of dat er sprake is van meervoudig slachtofferschap.

Deze dataset bevat echter een aantal beperkingen in relatie tot dit onderzoek:

1) Dit onderzoek focust zich op online fraude bij bedrijven. Uit de interviews en eerdere onderzoeken aan de hand van politieregistraties blijkt echter dat lang niet altijd geregistreerd wordt dat een bedrijf slachtoffer is, ook door capaciteit en prioritering van de politie. Ook wanneer wel bekend is dat het slachtoffer een bedrijf is, is in een groot deel geen verdere informatie beschikbaar over bedrijfsgrootte of bedrijfssector.
2) Mogelijk zijn er meldingen gedaan bij de politie die niet in de BVH terecht zijn gekomen. Dit kan voorkomen als iemand zich meldt bij de politie aan de balie maar de meldingen niet geregistreerd wordt door de medewerker. Hier heeft dit onderzoek geen zicht op.
3) In de politiedata is het onduidelijk of de meldingen gaan over pogingen tot fraude of geslaagde fraude (met directe financiële schade) doordat de data op

[18] Met een tekstquery kunnen teksten op automatische wijze worden geanalyseerd en geclassificeerd.

geaggregeerd niveau aangeleverd zijn. Daardoor is het bijvoorbeeld onduidelijk of er sprake is van meervoudig/herhaald slachtofferschap. Echter heeft dit ook implicaties voor de extrapolatie van de politiedata.

4) Uit de interviews blijkt dat meldingen en aangiften van aan- en verkoopfraude beperkt worden geregistreerd worden in BlueIntel. Deze meldingen worden namelijk verzameld door het Landelijk Meldpunt Internetoplichting (LMIO). Dit meldpunt is opgericht vanwege de toename aan marktplaats oplichting, wat in ons onderzoek gezien wordt als aan- en verkoopfraude. Door een gebrek aan capaciteit bij de politie wordt de data van LMIO niet overgenomen in BlueIntel. Daardoor is er sprak van onderschatting in het aantal meldingen van aan- en verkoopfraude in de dataset.

7.1.2 Verwerking

Fraudevormen

Niet alle subcategorieën van fraude die de politie hanteert binnen de hoofdcategorie fraude/oplichting zijn van toepassing op dit onderzoek, omdat ze geen online fraude betreffen, zoals sextortion en DDoS. De data die we hebben ontvangen van de politie is daarom gefilterd op de relevante subcategorieën en vertaald naar de taxonomie voor dit onderzoek. Zeven subcategorieën kunnen we één-op-één vertalen naar een specifieke fraudevorm in onze taxonomie. Drie subcategorieën kunnen alleen vertaald worden naar een hoger niveau in de taxonomie, wat betekent dat we de subcategorie niet kunnen toewijzen aan een specifieke fraudevorm, dit geven we aan middels de nummering. De vertaling en relevantie subcategorieën uit de politieregistraties zijn te zien in Tabel 14.

Tabel 14. Vertaling van subcategorieën in politieregistraties naar de fraudevormen uit de opgestelde taxonomie.

Subcategorie uit politieregistraties	Fraudevorm in taxonomie
Aan- en verkoopfraude	Overig
Bankhelpdeskfraude	1.2.b Helpdeskfraude
Beleggingsfraude	1.1.c Beleggingsfraude
CEO-fraude	1.2.a CEO-fraude
Creditcardfraude	Overig
Factuurfraude (loon, salaris)	1.3.b Factuurfraude
Fraude bankgegevens/internetbankieren	1. Betalingsfraude
Helpdeskfraude (tech support scam)	1.2.b Helpdeskfraude
Misbruik accounts voor bestellingen	1.2c Identiteitsfraude
Telecomfraude	Overig

De politie maakt in zijn registraties geen onderscheid tussen aan- en verkoopfraude. Daarom wordt in de verwerking van de dataset de combinatie van aan- en verkoopfraude als fraudevorm opgenomen en gecategoriseerd onder de kop Overig. Aan- en verkoopfraude wordt daarmee niet alvorens de taxonomie opgesplitst in twee categorieën.

Type slachtoffer

Naast een aantal irrelevante subcategorieën zijn ook een aantal slachtoffer categorieën niet relevant omdat de slachtoffers geen bedrijven zijn, zoals particulieren en scholen of is in onvoldoende mate duidelijk of dit alleen om bedrijven gaat, zoals Zorg Daarom zijn van de onderstaande slachtoffer categorieën die bij een aangifte of melding geregistreerd zijn alleen de dikgedrukte meegenomen in het onderzoek:

- **Bank**;
- **Bedrijf – eenmanszaak/zzp**;
- **Bedrijf – MKB**;
- **Bedrijf – overig**;
- **Bedrijf – onbekend**;
- Overheid/gemeente;
- Overige benadeelde;
- **Overige financiële instelling**;
- Particulier;
- School;
- Stichting/vereniging;
- Zorg.

Schadebedragen

Daarnaast bleek bij de analyse van de schadebedragen dat deze niet zodanig staan opgenomen in de dataset dat we deze mee kunnen nemen in de analyse. Dit heeft twee redenen:

1. Niet elke melding of aangifte bevat een schadebedrag. Dit kan of betekenen dat dit simpelweg niet (goed) geregistreerd of geclassificeerd is, maar het kan ook betekenen dat de aangever geen schade heeft opgelopen. In het eerste geval leidt dit vooral tot vertekeningen in de (gemiddelde) geregistreerde schade door online fraude bij bedrijven. In het tweede geval leidt het ook tot problemen in cijfers over het aantal slachtoffers, omdat deze gevallen mee worden genomen als geregistreerd fraudegeval terwijl het een mislukte poging betreft.
2. Er zijn geen standaardregels voor het rapporteren van schadebedragen. Tijdens een interview bleek bijvoorbeeld dat bij een enkele melding/aangifte de aangegeven valuta niet Euro was, maar een cryptomunt. Omdat wij

geaggregeerde data ontvangen, en niet de individuele meldingen/aangiften, kunnen wij ook niet valideren of het vermelde schadebedrag alleen directe financiële schade betreft, of ook indirecte.

Op basis van de politieregistraties zullen wij daarom helemaal geen uitspraken doen over de omvang de schade.

Bijlage 5. Fraudehelpdesk Zakelijk

Bij de Fraudehelpdesk kunnen particulieren en ondernemers informatie vinden over fraude, persoonlijk advies krijgen en fraude melden via de telefoon of de website. De Fraudehelpdesk heeft ook een zakelijk kanaal, specifiek gericht op fraude bij ondernemers. Van de Fraudehelpdesk Zakelijk hebben wij alle meldingen van 2024 ontvangen en geanalyseerd.

7.1.3 Beschrijving

Bij de Fraudehelpdesk Zakelijk kunnen bedrijven via een formulier op de website van de Fraudehelpdesk melding maken van een fraude incident. Hierbij zijn specifiek voor bedrijven meldingsformulieren beschikbaar naast de formulieren voor particuliere slachtoffers. Slachtoffers beschrijven de meldingen onder andere in een open tekstveld. Deze wordt vervolgens zowel automatisch als door een medewerker gecategoriseerd naar een specifieke fraudevorm.

De Fraudehelpdesk slaat geen persoonsgegevens over het slachtoffer op en registreert ook niet de kenmerken van bedrijven die melding doen. Daardoor kunnen we in het kader van dit onderzoek alleen data gebruiken over meldingen die via het zakelijke kanaal binnenkomen bij de Fraudehelpdesk – bij meldingen die binnenkomen via het generieke kanaal is (achteraf) niet meer vast te stellen of het een bedrijf betreft. De Fraudehelpdesk geeft aan dat ze geen inzicht hebben op het percentage ondernemers dat melding maakt van online fraude. Omdat de Fraudehelpdesk geen gegevens over het slachtoffer opslaat, kunnen we in de data niet achterhalen hoeveel bedrijven achter de meldingen zitten, en of dit unieke slachtoffers zijn of dat er sprake is van meervoudig slachtofferschap. Ook kunnen we daardoor geen uitspraken doen over het type bedrijf dat melding van online fraude heeft gedaan bij de Fraudehelpdesk. De Fraudehelpdesk heeft voor dit onderzoek alle zakelijke meldingen in 2024 anoniem beschikbaar gesteld.

7.1.4 Verwerking

Fraudevormen

Niet alle fraudevormen gemeld bij de Fraudehelpdesk behoren tot vormen van online fraude, zoals cybercrime en datingfraude, waardoor een filtering nodig is. De gecategoriseerde meldingen van Fraudehelpdesk Zakelijk hebben we gefilterd en geclassificeerd binnen de taxonomie van dit onderzoek, zie onderstaande tabel.

Tabel 15. Vertaling van fraudecategorieën bij de Fraudehelpdesk naar de fraudevormen uit de opgestelde taxonomie.

Fraudecategorie	Fraudevorm in taxonomie
Aan- en verkoopfraude	Overig
Acquisitiefraude	1.1.b Acquisitiefraude
Beleggingsfraude	1.1.c Beleggingsfraude
Betaalmiddelfraude	Overig
CEO-fraude	1.2.a CEO-fraude
Factuurfraude	1.3.b Factuurfraude
Helpdeskfraude	1.2.b Helpdeskfraude
Identiteitsfraude	1.2 Aannemen van een valse identiteit
Misbruik bedrijfsgegevens	1.3 Manipuleren van gegevens
Misleidende verkoop	1.1 Niet leveren van beloofde goederen of diensten
Recovery-fraude	1.1.d Recoveryfraude
Spooknota (Zakelijk)	1.3.b Factuurfraude
Telecomfraude	Overig

Zeven vormen kunnen één-op-één gekoppeld worden aan een specifieke fraudevorm uit de taxonomie, terwijl vijf vormen, net als bij de politieregistraties, betrekking hebben op online fraude op een hoger niveau in de taxonomie. Identiteitsfraude, misbruik bedrijfsgegevens en misleidende verkoop zijn in onze taxonomie namelijk geen specifieke fraudevormen maar zijn onderdeel van een specifieke *modus operandi* waar meerdere fraudevormen onder vallen. Betaalmiddelfraude is geen specifieke modus operandi, maar beschrijven de opbrengst voor de dader (een betaling). Telecomfraude is geen modus operandi en beschrijft ook niet de opbrengst voor de dader, maar alleen het ICT-hulpmiddel dat is gebruikt om de fraude te plegen. Daarom kunnen de fraudegevallen die onder telecomfraude geregistreerd staan alleen worden meegenomen in de totale omvang van online fraude bij bedrijven. De Fraudehelpdesk Zakelijk maakt in zijn registraties geen onderscheid tussen aan- en verkoopfraude. Daarom wordt in de verwerking van de dataset de combinatie van aan- en verkoopfraude als fraudevorm opgenomen onder de kop Overig.

Schade

Bij meldingen van online fraude ondervindt de ondernemer niet altijd directe financiële schade. Bij een melding geven ondernemers aan of ze direct geld hebben betaald aan de tegenpartij, dat ze indirecte schade hebben geleden (financiële schade als gevolg van het incident) of dat de poging helemaal geen schade heeft opgeleverd. In de verdere analyses maken wij onderscheid tussen meldingen met directe schade en meldingen zonder directe schade.

Benaderingsvormen

Daarnaast bevat de dataset niet alleen meldingen van *online* fraude, maar ook fraude-incidenten waarbij het slachtoffer niet online is benaderd. Meldingen waarbij het slachtoffer persoonlijk of via de post is benaderd zijn daarom ook uit de dataset gehaald.

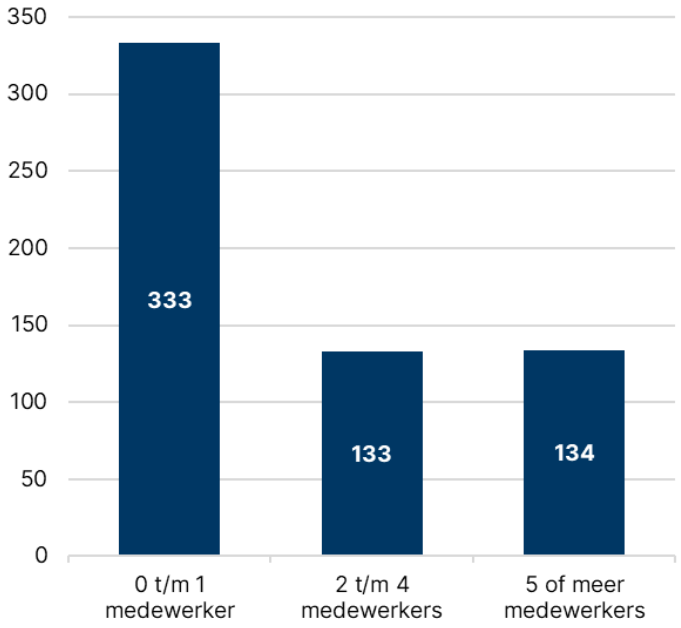
Bijlage 6. Enquête ondernemerspanel Ipsos I&O

Ipsos I&O heeft voor ons een enquête uitgezet onder een representatieve steekproef van 600 Nederlandse bedrijven uitgezet. In de enquête vroegen we Nederlandse bedrijven of ze in 2024 slachtoffer waren van online fraude en zo ja, van welke fraudevormen. Ook werden o.a. het schadebedrag, de benaderingsvorm en het wel of niet melden van het fraude-incident uitgevraagd.

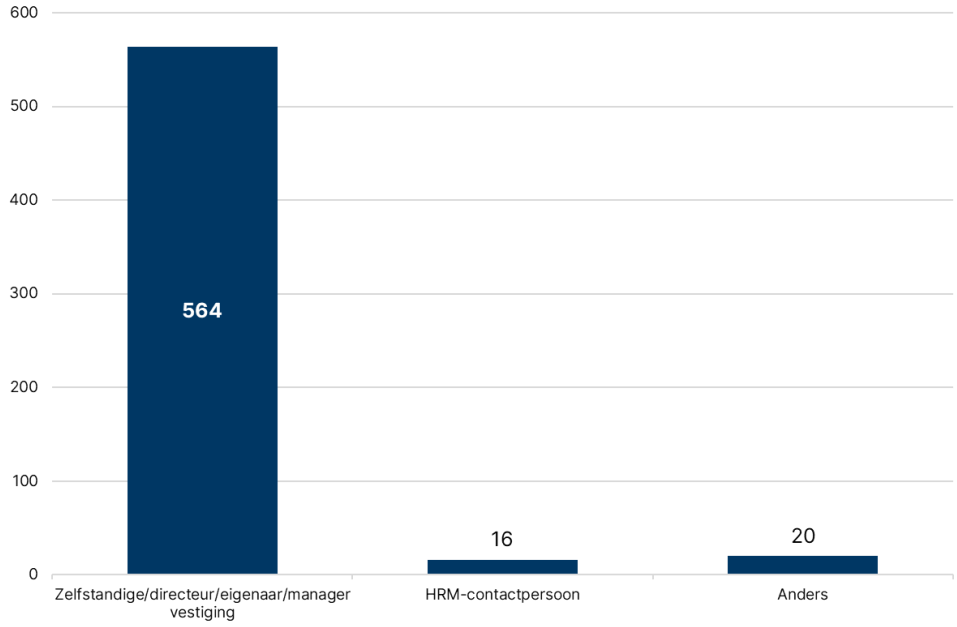
7.1.5 Beschrijving

Ipsos I&O beschikt over een panel bestaande uit 3.200 zzp'ers (60%), 1.350 ondernemers met 2-10 medewerkers (26%) en 750 ondernemers met 10+ medewerkers (14%). De bedrijfsgrootte, sector en functie in het bedrijf is van alle personen in het panel bekend voor Ipsos I&O en hoefde in de enquête dus niet te worden uitgevraagd. De vragenlijst is in Bijlage 2 te vinden.

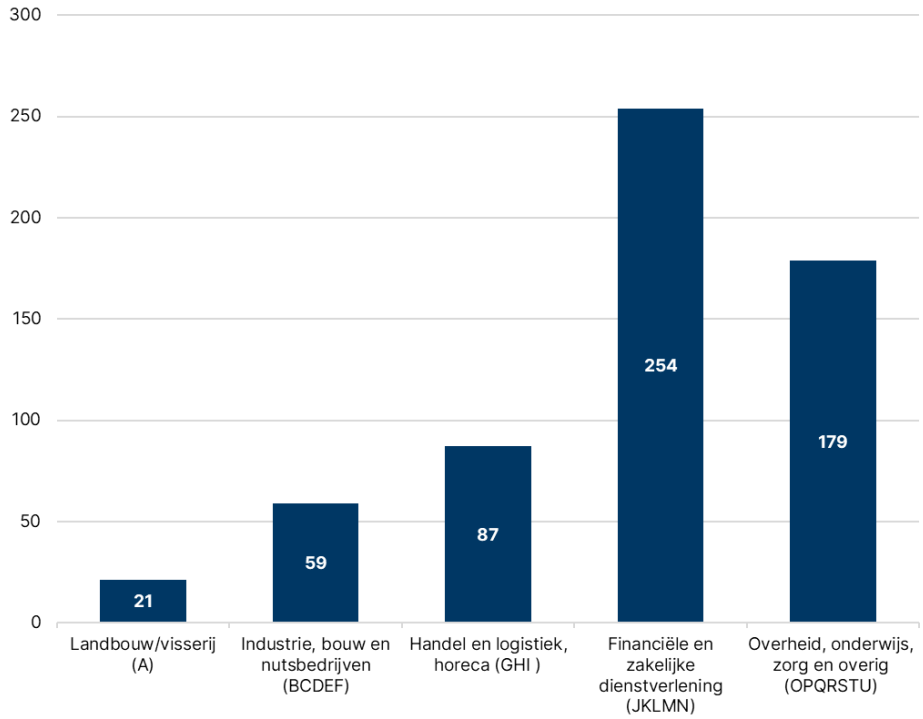
De steekproef bestaat netto uit 600 respondenten (N = 600). De steekproef bestaat uit 333 bedrijven met 0-1 medewerkers, 133 bedrijven met 2-4 medewerkers en 134 bedrijven met 5 of meer medewerkers (zie Figuur 8). Voor dit onderzoek is specifiek gekozen voor deze drie groottecategorieën voor een voldoende representatieve verdeling. De respondenten in de steekproef bestaan grotendeels uit eigenaren, directeuren of managers van een vestiging. Ipsos I&O gaat ervan uit dat de mensen die *geen* eigenaar, directeur of manager zijn, toch een hoge positie binnen het bedrijf bekleden en daardoor voldoende kennis hebben over eventuele slachtofferschap (zie Figuur 9). Verder zit er spreiding in sectoren (SBI-codes) van de bedrijven (zie Figuur 10).



Figuur 8: Bedrijfsgrootte (gehele steekproef)



Figuur 9: Bedrijfsfunctie respondent (gehele steekproef)



Figuur 10: Bedrijfssectoren (gehele steekproef)

7.1.6 Verwerking

Ipsos I&O heeft zowel de ruwe data van alle respondenten, als de aantallen en percentages per vraag aangeleverd. Verder is er een weging gemaakt naar bedrijfsgrootte en sector om de resultaten van de enquête representa

tief te maken voor het Nederland bedrijfsleven. We hebben de aantallen en percentages zowel ongewogen als gewogen ontvangen, samen met een document dat inzicht geeft in de berekening van de wegingsfactoren. De weging maakt het mogelijk om de steekproef representatief te maken voor de populatie van bedrijven in Nederland en zijn te vinden in Bijlage 7. Ipsos I&O heeft daarnaast gezorgd voor het opschonen van de data middels het verwijderen van *straight-lining* antwoorden, waarbij respondenten consistent dezelfde antwoordoptie kiezen in een vragenreeks, en er is een controlevraag in de enquête bijgevoegd.

Wanneer respondenten slachtoffer waren van online fraude is gevraagd om het incident te beschrijven via een open antwoordveld. Van alle incidenten van online fraude die in de data voorkwamen, is deze beschrijving van het incident (open antwoordveld) doorgenomen om te controleren voor inconsistenties en verkeerde interpretatie van de vragen door respondenten. Op basis hiervan hebben we een aantal correcties doorgevoerd. Omwille van de lengte van de vragenlijst, konden respondenten maximaal twee incidenten van online fraude per fraudevorm in zijn volledigheid beschrijven. Onder de slachtoffers van online fraude kwam het één keer voor dat een respondent met meer

dan twee incidenten te maken had gehad (in dit geval was er '5 keer of meer' ingevuld). Van drie incidenten is dus geen beschrijving beschikbaar.

Incorrect gecategoriseerde fraudevormen

In verschillende gevallen is een fraudevorm, ondanks de gepresenteerde definities, verkeerd gecategoriseerd door respondenten. Zo is aankoopfraude bijvoorbeeld een aantal keer gecategoriseerd als verkoopfraude. Op basis van de beschrijving van het fraude incident, die opgegeven is door het slachtoffer, zijn een aantal incidenten gecorrigeerd in de data, zodat alle fraude-incidenten volgens onze taxonomie op de juiste wijze zijn gecategoriseerd. Dit betrof negen incidenten.

Fraude-incidenten zonder financiële schade

In 49% van de incidenten van online fraude die zijn beschreven in de vragenlijst bleek er, op basis van de beschrijving, dat er geen geld was verloren als direct gevolg van het incident. In dit onderzoek nemen we alleen fraude-incidenten met directe financiële schade mee in de analyse. Daarom zijn alle fraude-incidenten waar geen sprake was van directe financiële schade uitgesloten.

Incorrecte definiëring van herhaald slachtofferschap

In twee gevallen gaven respondenten aan twee keer slachtoffer te zijn geweest van dezelfde vorm van online fraude, maar is er op basis van de beschrijving van het incident beoordeeld dat het om één incident ging. In beide gevallen was er in de beschrijving van het tweede incident aangegeven dat het om hetzelfde incident ging als eerder beschreven. Hiervoor is gecorrigeerd door in deze gevallen herhaald slachtofferschap te vervangen door enkelvoudig slachtofferschap.

Bijlage 7. Weegfactoren enquête Ipsos I&O

Om tot een representatieve schatting van de Nederlandse bedrijven te komen weegt Ipsos I&O zijn uitkomsten. Dit doet het door zowel op bedrijfsgrote als op sector te wegen. Daarbij zijn er drie grootteklasse en zes sectoren. Per klasse en sector is bepaald hoeveel Nederlandse bedrijven aanwezig zijn waarna onderstaande berekening uitgevoerd is. Dit is gedaan op basis van de 2023 Landelijk Informatiesysteem van Arbeidsplaatsen (LISA).

Weging = (Totale steekproef/ Steekproef grootklasse en sector) * (Populatie grootteklassen en sector/ Totale populatie).

Tabel 16: Weegfactoren Ipsos I&O

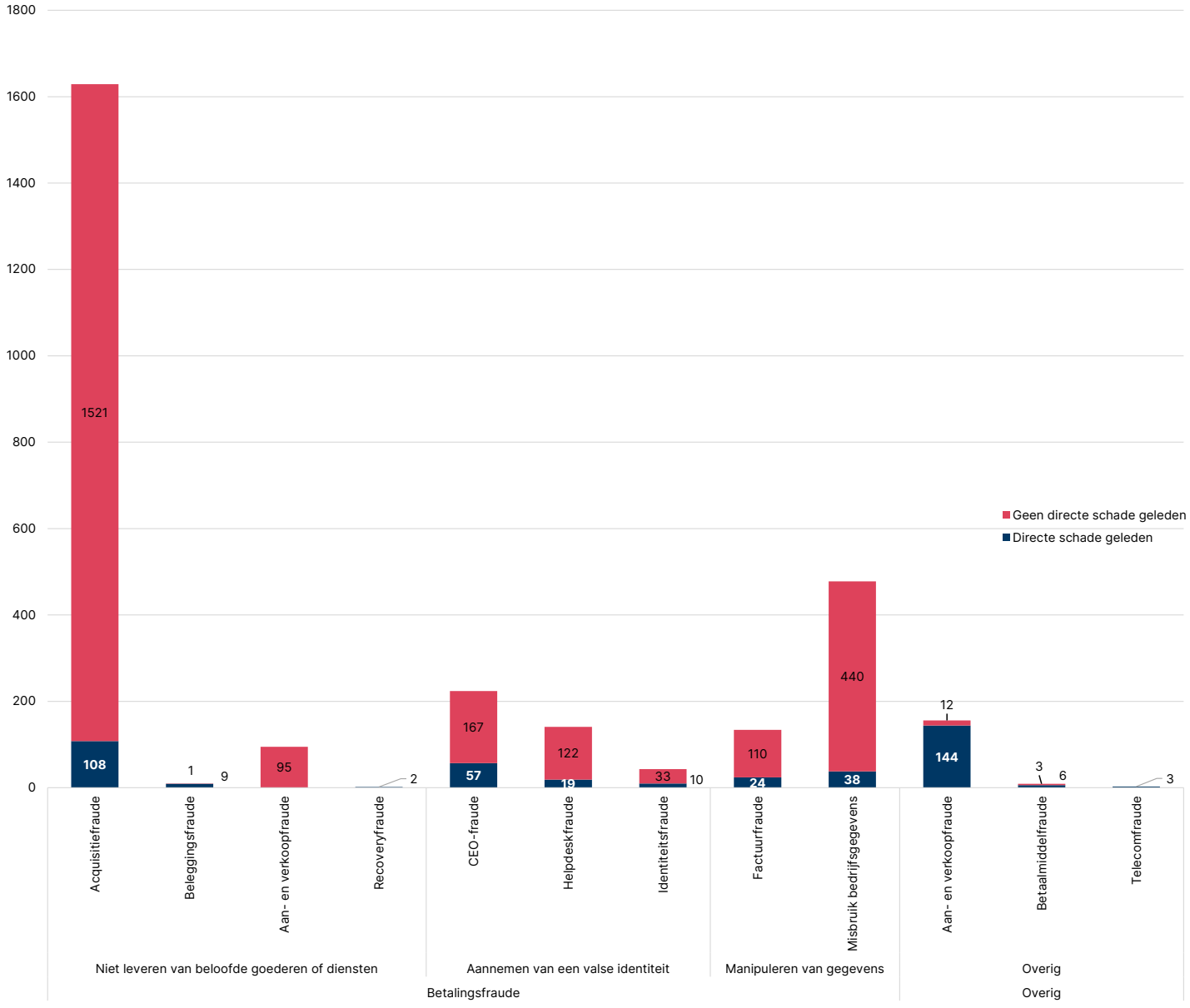
Grootteklasse	Sector	Populatie	Steekproef	Weegfactor
0 t/m 1 medewerkers	Landbouw/visserij	44.145	8	1,53
	Industrie, bouw en nutsbedrijven	270.234	22	3,41
	Handel en logistiek, horeca	286.993	18	4,43
	Financiële en zakelijke dienstverlening	574.417	174	0,91
	Overheid, onderwijs, zorg en overig	508.812	111	1,3
2 t/m 4 medewerkers	Landbouw/visserij	28.556	9	0,89
	Industrie, bouw en nutsbedrijven	30.405	8	1,06
	Handel en logistiek, horeca	101.688	38	0,74
	Financiële en zakelijke dienstverlening	62.918	48	0,36
	Overheid, onderwijs, zorg en overig	52.942	30	0,50
5 en meer medewerkers	Landbouw/visserij	4.900	4	0,34
	Industrie, bouw en nutsbedrijven	29.245	29	0,28
	Handel en logistiek, horeca	70.006	31	0,63

Grootteklasse	Sector	Populatie	Steekproef	Weegfactor
	Financiële en zakelijke dienst-verlening	41.577	32	0,36
	Overheid, onderwijs, zorg en overig	52.990	38	0,39
Totaal		2.159.828	600	

Bijlage 8. Additionele analyses

Meldingen met directe en zonder directe schade bij de Fraudehelpdesk Zakelijk

Veruit de meeste meldingen bij de Fraudehelpdesk Zakelijk van online fraude door bedrijven gaan over Acquisitiefraude (N=1.629 in totaal). Ook wordt er relatief vaak melding gemaakt van Misbruik van bedrijfsgegevens (N=478) en Aankoop- en CEO-fraude (N=224 en N=224 respectievelijk). Echter is bij een groot deel van de meldingen geen sprake van directe financiële schade.



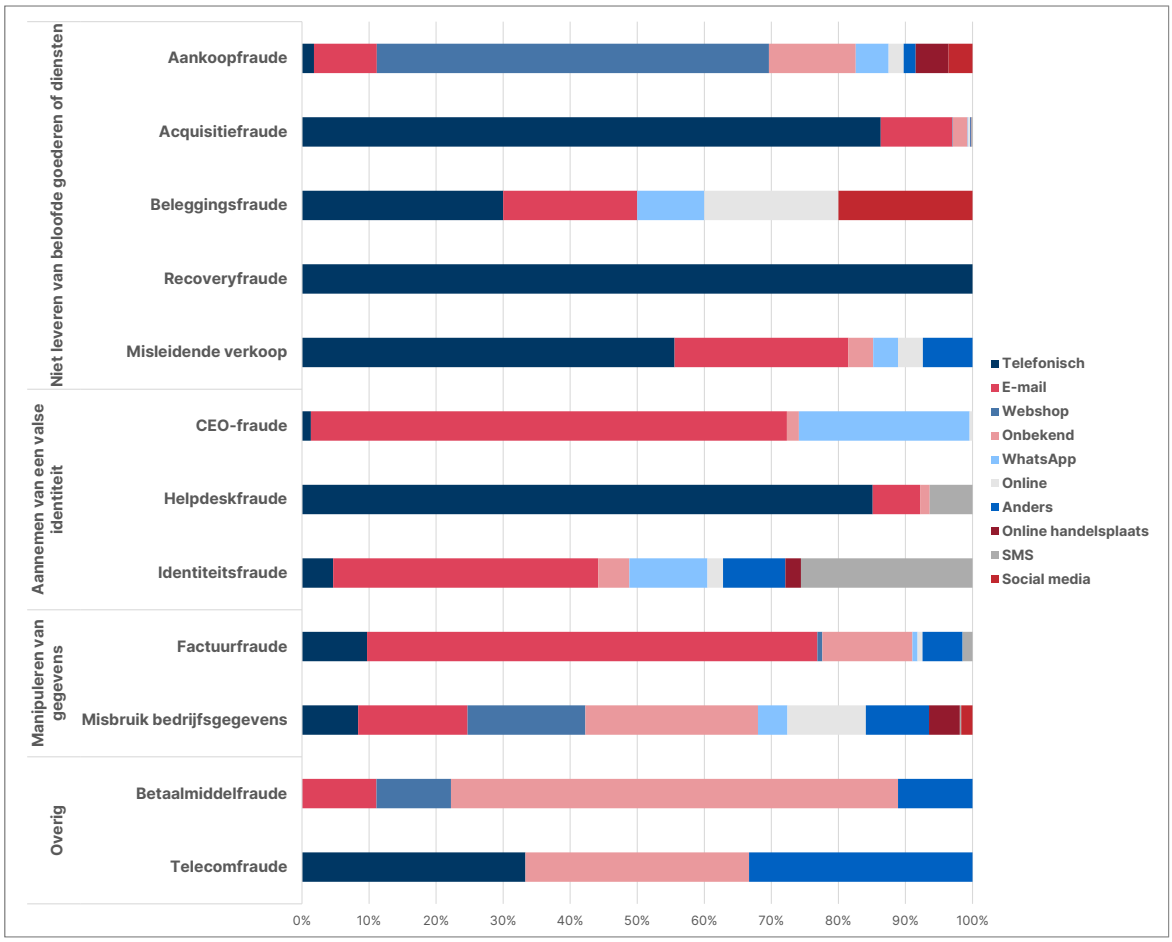
Figuur 11. Aantal meldingen van online fraude bij de Fraudehelpdesk Zakelijk in 2024 per fraudevorm.

Waar de meeste meldingen gaan over Acquisitiefraude of Misbruik van bedrijfsgegevens, wordt daar relatief minder vaak ook directe schade geregistreerd. Aan- en verkoopfraude is een fraudevorm waarbij relatief vaak schade wordt geregistreerd door de Fraudehelpdesk Zakelijk (in 58% van de gevallen). Bij Acquisitiefraude is dat slechts het geval in 7% van de meldingen (N=108). Het percentage van meldingen met directe schade ligt bij Recovery- en Beleggingsfraude het hoogst, met respectievelijk 100% en 91% van de gemelde gevallen (kanttekening daarbij wel is dat het totaal aantal meldingen beperkt is).

Deze verschillen in geregistreerde schade bij meldingen kan een aantal dingen betekenen. Het kan zijn dat ondernemers bepaalde fraudevormen makkelijker herkennen dan andere en zich ertegen kunnen verweren, waardoor een poging niet tot schade leidt, maar er wel melding van wordt gemaakt. Daarnaast kunnen fraudeurs met bepaalde fraudevormen ook succesvoller zijn, waardoor een poging ook vaker tot directe schade leidt bij het slachtoffer. Tot slot kan het ook te maken hebben met de meldingsbereidheid, waarbij ondernemers vaker melding maken van bepaalde fraudevormen.

Benaderingswijze per fraudevorm bij meldingen met directe schade bij de Fraudehelpdesk Zakelijk

In onderstaande figuur tonen we per fraudevorm het percentage van meldingen met directe schade waarbij een bepaalde benaderingsvorm is gebruikt.

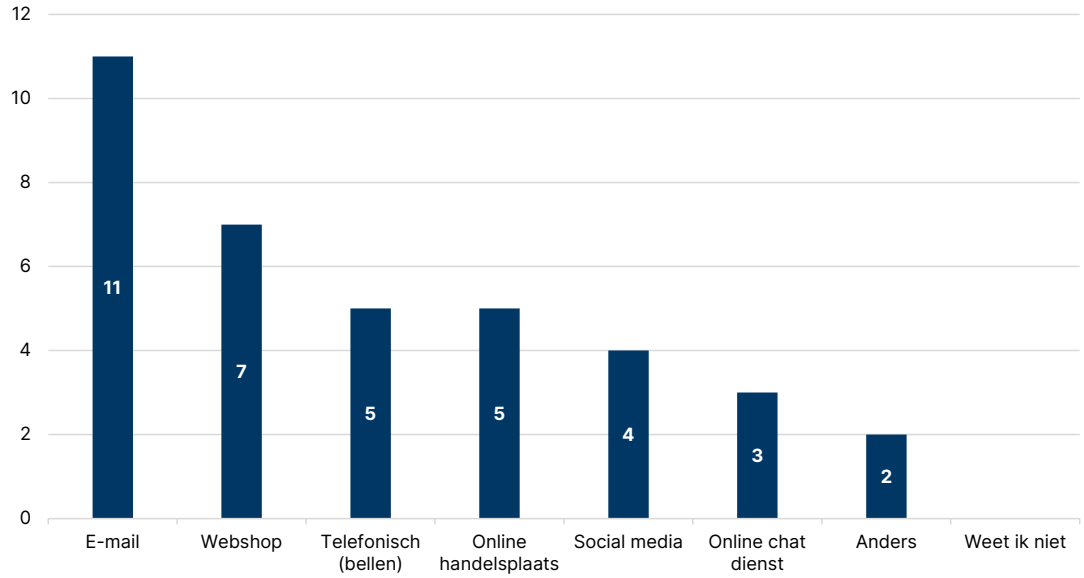


Figuur 12: Benaderingsvorm per melding uitgesplitst per fraudevorm

Benaderingswijze bij fraude-incidenten uit de enquête onder ondernemers

Het onderstaande diagram geeft weer op welke manier een slachtoffer contact had met een dader. Bij een fraude-incident kan het slachtoffer op meerder manieren contact hebben gehad met de dader. Bij 8 van de 29 incidenten heeft de fraudeur gebruik gemaakt van meerdere benaderingsvormen.

Over alle incidenten komt e-mail als benaderingsvorm het meeste voor: bij een derde van de incidenten worden slachtoffers per e-mail benaderd (soms naast andere benaderingsvormen).



Figuur 13: Benaderingsvormen bij fraude-incidenten