

pro facta

Eindrapport
Evaluatie Fraudehelpdesk

Groningen, november 2023

www.pro-facto.nl

Colofon

Pro Facto
Ossenmarkt 5
9712 NZ Groningen
www.pro-facto.nl
info@pro-facto.nl
050-3139853

Auteurs	Prof. dr. Heinrich Winter, mr. Christine Veen, mr. Corine Bartlema, Jeanne Cazemier Msc
Adviseur	I. Verkerk
Opdrachtgever	WODC
Datum	17 november 2023
Status	Definitief

Dit onderzoek is – in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum – uitgevoerd door Pro Facto, bureau voor bestuurskundig en juridisch onderzoek, advies en onderwijs.

Begeleidingscommissie: prof. dr. H.J.M. Fenger (Erasmus Universiteit Rotterdam), R.J. Notté Msc (De Haagse Hogeschool), dr. J.H. Bullée (Universiteit Twente), mr. N.S.M. Alberti (ministerie van JenV), dr. H.C.J. van der Veen (WODC).

Voor de inhoud van het rapport zijn de onderzoekers verantwoordelijk. Het leveren van een bijdrage (als medewerker van een organisatie of als lid van de begeleidingscommissie) betekent niet automatisch dat de betrokkene instemt met de gehele inhoud van het rapport. Dat geldt eveneens voor het ministerie van Justitie en Veiligheid en zijn minister.

© 2023 Pro Facto. Auteursrechten voorbehouden.

Inhoud

Gebruikte afkortingen	5
Samenvatting	6
1 Inleiding	15
1.1 Aanleiding	15
1.2 Vraagstelling en onderzoeksthema's	15
1.3 Onderzoeksaanpak	17
1.4 Leeswijzer	20
2 Beleidsreconstructie	21
2.1 Inleiding	21
2.2 Totstandkoming van de Fraudehelpdesk	21
2.3 Veronderstelde doel-middelrelaties en werkzame mechanismen	25
2.4 Evaluatie van de veronderstelde mechanismen	27
2.4.1 Literatuuronderzoek veronderstelde mechanismen	27
2.5 Conclusie	30
3 Organisatie, financiën en activiteiten	32
3.1 Inleiding	32
3.2 Inrichting organisatie	32
3.3 Financiën	34
3.3.1 Subsidievoorwaarden	35
3.4 Activiteiten	37
3.4.1 Registratie van fraudemeldingen	37
3.4.2 Doorverwijzen meldingen	42
3.4.3 Preventie	44
3.5 Overige ontwikkelingen rondom de dienstverlening	45
3.5.1 Verwerken van persoonsgegevens van strafrechtelijke aard	45
3.6 Conclusie	47

4	Bekendheid Fraudehelpdesk	50
4.1	Inleiding	50
4.2	Websiteonderzoek	50
4.3	Naamsbekendheid Fraudehelpdesk	50
4.3.1	Onderzoek naar de naamsbekendheid door de Fraudehelpdesk	50
4.4	Vindbaarheid van de website	53
4.4.1	Vindbaarheid van de website van de Fraudehelpdesk op websites van ketenpartners	55
4.5	Bezoekers website	56
4.6	Conclusie	57
5	Waardering van de Fraudehelpdesk	59
5.1	Inleiding	59
5.2	Respons en verantwoording vragenlijstonderzoek	59
5.3	Waardering door melders	60
5.3.1	Achtergrond respondenten	60
5.3.2	De melding	60
5.3.3	Reactietermijn	61
5.3.4	Tevredenheid dienstverlening	62
5.3.5	Waardering dienstverlening van de medewerkers	63
5.3.6	Advies van de Fraudehelpdesk	63
5.3.7	Doorverwijzingen	64
5.3.8	Suggesties ter verbetering van de dienstverlening	65
5.4	Waardering door ketenpartners	66
5.4.1	Contact met ketenpartners	66
5.4.2	Verhouding taken en werkzaamheden ketenpartners en Fraudehelpdesk	66
5.4.3	Beoordeling dienstverlening en draagvlak in de keten	67
5.4.4	Knelpunten	68
5.4.5	Uitdagingen en neveneffecten	69
5.5	Conclusie	70
6	Landschap van fraudemeldpunten	72
6.1	Inleiding	72
6.2	Verantwoording	72
6.3	Type meldpunten	73
6.4	Doorverwijs- en preventiepunten	75
6.5	Type diensten	76

6.6	Type fraudevormen	78
6.7	Conclusie	79
7	Synthese en conclusie	81
7.1	Inleiding	81
7.2	Beantwoording centrale onderzoeksvragen	81
7.3	Conclusie	91
Bijlage 1:	Deelvragen	94
Bijlage 2:	Geraadpleegde documenten	96
Bijlage 3:	Lijst met gesprekspartners	99
Bijlage 4:	Vragenlijst melders FHD	101
Bijlage 5:	Externe communicatie en projecten	103
Bijlage 6:	Websiteonderzoek	104
Bijlage 7:	Fraudemeldpunten horizontale fraude	109
Bijlage 8:	Subsidievoorwaarden	113
Bijlage 9:	Definities	116
Bijlage 10:	Responsverantwoording naamsbekendheidsonderzoeken	120

Gebruikte afkortingen

ACM	Autoriteit Consument & Markt
AFM	Autoriteit Financiële Markten
AP	Autoriteit Persoonsgegevens
AVG	Algemene Verordening Gegevensbescherming
BFT	Bureau Financieel Toezicht
CCV	Centrum voor Criminaliteitspreventie en Veiligheid
CMI	Centraal Meldpunt Identiteitsfraude
DUO	Dienst Uitvoering Onderwijs
ECC	Europees Consumenten Centrum
EZK	Ministerie van Economische Zaken
IGZ	Inspectie Gezondheidszorg en Jeugd
JenV	Ministerie van Justitie en Veiligheid
KIFID	Klachteninstituut Financiële Dienstverlening
LMIO	Landelijk Meldpunt Internetoplichting
OM	Openbaar Ministerie
SHN	Stichting Slachtofferhulp Nederland
UAVG	Uitvoeringswet Algemene Verordening Gegevensbescherming
VbbV	Veiligheid begint bij Voorkomen

Samenvatting

Aanleiding

Ons land kent verschillende informatie- en meldpunten waar burgers en bedrijven informatie kunnen inwinnen over (nieuwe) vormen van horizontale fraude, waarbij burgers en bedrijven worden benadeeld en waar fraude en oplichting kunnen worden gemeld.¹ Een van die fraudemeldpunten – het meldpunt dat in dit onderzoek centraal staat en dat zich op alle vormen van fraude richt – is de Fraudehelpdesk. De Fraudehelpdesk is opgericht door de Stichting SafeCin, nadat het ministerie van Justitie en Veiligheid (hierna: JenV) daarvoor eind 2010 een subsidie beschikbaar stelde. Het ministerie van JenV is op dit moment de enige subsidieverstrekker. Dit evaluatieonderzoek beoogt de besluitvorming over de verdere subsidiëring, de hoogte van de toe te kennen subsidie, de doelen van de subsidie en daarbij te stellen voorwaarden te ondersteunen.

Vraagstelling en deelonderzoeken

De volgende hoofdvragen stonden in het onderzoek centraal:

1. In hoeverre kunnen de doelen die de Fraudehelpdesk nastreeft in theorie via de geldende subsidievoorwaarden en het inrichtingsplan van de Fraudehelpdesk worden bereikt?
2. In welke mate volstaat de praktische invulling van het inrichtingsplan van de Fraudehelpdesk in het bereikbaar maken van deze doelen?
3. Welke bijdrage heeft de Fraudehelpdesk geleverd aan de preventie en bestrijding van horizontale fraude?
4. Welke positie bekleedt de Fraudehelpdesk in het veld van de Nederlandse fraudepreventie en -bestrijding?
5. Hoe zou de toekomstige doelbereiking van de Fraudehelpdesk (verder) kunnen worden verbeterd? Zijn er structurele of procesmatige aanpassingen nodig om de

¹ Met de nota Zicht op fraude expliciteerde het Openbaar Ministerie in 1997 het onderscheid tussen verticale en horizontale fraude. Bij verticale fraude is de overheid de benadeelde partij. Bij horizontale fraude wordt een burger of bedrijf benadeeld.

toekomstige bijdrage van de Fraudehelpdesk aan fraudepreventie en -bestrijding in Nederland te verbeteren?

Het onderzoek is uitgevoerd aan de hand van vier deelonderzoeken.

I. Planevaluatie

In de planevaluatie stond de vraag waarom een beleidsinterventie (het oprichten van een helpdesk) zou *kunnen* werken centraal. We hebben daarvoor de beleidstheorie in beeld gebracht en op basis daarvan een doelenboom opgesteld. De gereconstrueerde beleidstheorie is voorgelegd aan experts op het gebied van fraude(bestrijding) en er is gekeken of er in de wetenschappelijke literatuur onderbouwing kan worden gevonden voor de veronderstelde werkzame mechanismen.

II. Procesevaluatie

De mogelijke effectiviteit van de Fraudehelpdesk wordt niet alleen bepaald door de kwaliteit van de beleidstheorie, maar ook door de uitvoering en de organisatie van de Fraudehelpdesk. Dat stond centraal in de procesevaluatie, die zich richtte op werkzaamheden van de Fraudehelpdesk in de praktijk. Daarnaast zijn knelpunten in de uitvoering in kaart gebracht. Omdat de uitvoering meerdere aspecten raakt richtte de procesevaluatie zich op vier onderdelen: de uitvoering, de bekendheid van de Fraudehelpdesk, de waardering van de Fraudehelpdesk, en de knelpunten. De onderzoeksactiviteiten voor de procesevaluatie zijn uitgevoerd in de eerste helft van 2023.

III. Het landschap van fraudemeldpunten

In de loop der jaren is een veelheid aan fraudemeldpunten ontstaan. In dit deelonderzoek zijn bestaande fraudemeldpunten voor horizontale fraude geïnventariseerd. Horizontale fraude gaat over fraude die is gericht tegen burgers, financiële instellingen of bedrijven. We hebben gekeken met welke meldpunten er overlap in diensten bestaat en waarin de Fraudehelpdesk zich onderscheidt van de diensten van andere meldpunten.

IV. Synthese

Het onderzoek is afgesloten met een synthesefase. Daarin zijn alle bevindingen uit de drie deelonderzoeken samengevat en vertaald naar conclusies over de Fraudehelpdesk in het algemeen en worden de onderzoeksvragen beantwoord.

Aanpak

Startgesprek

Het onderzoek ging van start met een startgesprek met de directeur van de Fraudehelpdesk. In dit gesprek zijn de onderzoeksactiviteiten die we wilden uitvoeren en waarbij medewerking van de Fraudehelpdesk nodig was toegelicht. Onder meer zijn afspraken gemaakt over het uitzetten van een vragenlijst onder melders en het aanleveren van documenten.

Deskresearch

Bij aanvang van het onderzoek is informatie over de totstandkoming van de Fraudehelpdesk verzameld en bestudeerd. Daarbij ging het in de eerste plaats om parlementaire stukken, zoals Kamerstukken en (voortgangs)brieven van de minister aan de Tweede Kamer. Op basis van

het bestuderen van deze stukken is de beleidstheorie in beeld gebracht en een doelenboom opgesteld. Daarnaast is gezocht naar relevante literatuur en documenten met informatie over de veronderstellingen waarop de beleidstheorie is gebaseerd. Ten slotte zijn ook de jaarverslagen van de Fraudehelpdesk bestudeerd.

Interviews

Om een beeld te krijgen van onder andere de (ontwikkeling van) diensten die de Fraudehelpdesk verleent en de knelpunten en uitdagingen, is met vijf medewerkers van de Fraudehelpdesk en met twee leden van de Raad van Toezicht gesproken. Daarnaast is ook een verdiepend gesprek gevoerd met de directeur van de Fraudehelpdesk. Voor het in beeld brengen van de waardering van de dienstverlening door ketenpartners hebben we met zeventien gesprekspartners bij veertien verschillende ketenpartners gesproken. Ten slotte is gesproken met twee experts op het gebied van fraude.

Registratieonderzoek

Informatie uit de jaarverslagen is benut om het aantal doorverwijzingen, telefonische en digitale meldingen en kosten van de gemelde schade in beeld te brengen. Daarnaast is informatie aangeleverd door de Fraudehelpdesk over het aantal websitebezoekers.

Websiteonderzoek

De vindbaarheid van de website van de Fraudehelpdesk is in kaart gebracht met een websiteonderzoek. Hiervoor is een lijst met voor de hand liggende zoektermen opgesteld, die vervolgens met synoniemen zijn aangevuld. Per zoekterm is gekeken op welke positie in Google de website van de Fraudehelpdesk verscheen. Daarnaast is gekeken in hoeverre de website van de Fraudehelpdesk eenvoudig vindbaar is via websites van ketenpartners, door daarnaar op die websites te zoeken.

Vragenlijst en telefonische interviews melders

Om de waardering van de Fraudehelpdesk door melders te onderzoeken hebben we een digitale vragenlijst uitgezet onder bijna tweeduizend melders. Dit heeft geleid tot in totaal 412 (deels en volledig) ingevulde vragenlijsten. Na afronding van het vragenlijstonderzoek is met een aantal respondenten contact opgenomen voor het stellen van een aantal aanvullende vragen. We spraken met tien respondenten die aangaven dat ze bereid waren om een aanvullende toelichting te geven.

Landschap fraudemeldpunten

Voor het in kaart brengen van het landschap van fraudemeldpunten voor horizontale fraude is gebruik gemaakt van een eerdere inventarisatie van fraudemeldpunten uit 2015 van Homburg en Van den Tillaart.² De inventarisatie uit dat onderzoek is geactualiseerd en aangevuld met nieuwe meldpunten. Voor het in kaart brengen van nieuwe meldpunten is gebruik gemaakt van de lijst met zoektermen die in het kader van het websiteonderzoek is opgesteld.

Expertmeeting

Het onderzoek is afgesloten met een expertmeeting waarin we onze voorlopige bevindingen hebben voorgelegd aan ketenpartners en hebben besproken hoe de toekomstige doelbereiking van de Fraudehelpdesk (verder) kan worden verbeterd.

² Homburg, G. en Van den Tillaart, J. (2015) *Fraudemeldpunten: synergie en samenwerking*. Amsterdam: Regioplan.

Wederhoor

De laatste versie van het concepteindrapport (zonder de analyse) is voor wederhoor voorgelegd aan de Fraudehelpdesk voor een feitencheck. Naar aanleiding daarvan is een kort gesprek gevoerd met de interim-directeur van de Fraudehelpdesk. Daarnaast heeft de Fraudehelpdesk in het document van het concepteindrapport opmerkingen geplaatst. Feitelijke onjuistheden zijn gecorrigeerd en enkele suggesties voor aanvullingen zijn in het rapport overgenomen.

Resultaten van het onderzoek

Beleidsreconstructie

De Fraudehelpdesk is ruim tien jaar geleden opgericht. Aanleiding voor het oprichten van een helpdesk was dat inzicht in aard en omvang van fraude ontbrak. Er was behoefte aan meer inzicht in soorten horizontale fraude en modus operandi. Daarnaast werd het noodzakelijk geacht meer fraudebewustzijn onder burgers en kleine ondernemers te creëren en slachtoffers te ondersteunen. In de loop der jaren is (horizontale) fraude steeds hoger op de politieke en beleidsmatige agenda's terecht gekomen en ziet het ministerie preventie als de meest effectieve inzet voor het voorkomen van fraude.

Het eerste doel van het oprichten van een helpdesk was het zo goed mogelijk ondersteunen van slachtoffers en het tweede doel was het weerbaarder maken van burgers en bedrijven tegen pogingen tot oplichting en fraude. Om deze doelen te bereiken moest de helpdesk – zoals vastgelegd in de subsidievoorwaarden van 2010 – drie (basis)diensten verlenen: (1) het registreren van aantallen en soorten meldingen, (2) het verstrekken van algemene informatie over bestaande vormen van fraude en (3) het doorverwijzen van slachtoffers naar de juiste organisaties. De wijze waarop de Fraudehelpdesk ruim tien jaar na de oprichting deze diensten in de praktijk verleent, lijkt overeen te komen met het oorspronkelijke idee zoals dat ook was vastgelegd in de subsidievoorwaarden die bij de oprichting waren opgesteld.

Op basis van wetenschappelijke literatuur zijn kritische kanttekeningen te plaatsen bij de veronderstelling dat het verstrekken van algemene informatie door middel van bijvoorbeeld campagnes effectief is. Ten aanzien van de veronderstelling dat een centraal meldpunt slachtoffers van fraude zou moeten ondersteunen is in de literatuur wel onderbouwing gevonden. Uit de beleidsreconstructie blijkt verder dat er destijds in een Kamerbrief een vijftal randvoorwaarden is geformuleerd door de minister.³ In het onderzoek is niet duidelijk geworden wat precies de achterliggende gedachte was van deze randvoorwaarden en het merendeel van deze randvoorwaarden werd ook niet door gesprekspartners herkend of als relevant gezien.

Een van de randvoorwaarden is dat er een zodanige infrastructuur aanwezig diende te zijn dat fraudemeldingen aan Politie en Openbaar Ministerie konden worden doorgegeven. De Fraudehelpdesk mag (tot op heden) door het ontbreken van de vergunning van de AP geen persoonsgegevens van strafrechtelijke aard ten behoeve van derden verwerken, waardoor het nu niet mogelijk is om aan de randvoorwaarde te voldoen. Enkele ketenpartners geven aan dat wanneer die gegevens wel mogen worden gedeeld, fraude beter bestreden kan worden. De vraag is of dit een taak is die past bij de doelen waarvoor de Fraudehelpdesk is opgericht.

³ *Kamerstukken II 2009/10, 29 911, nr. 41, p.2.*

De praktische inrichting en financiering van de Fraudehelpdesk

De Fraudehelpdesk ontving de afgelopen jaren subsidie van het ministerie van JenV en EZK. Het ministerie van EZK heeft de subsidieverlening in 2021 en 2022 afgebouwd, waardoor de Fraudehelpdesk vanaf 2023 alleen subsidie van het ministerie van JenV ontvangt. Het ministerie van JenV vindt het onwenselijk de enige subsidieverstrekker te zijn. De Fraudehelpdesk benadrukt de behoefte aan structurele financiering in een meerjarenplanning, met het oog op ontwikkelambities en aantrekkelijk werkgeverschap. Voor nieuwe projecten is de Fraudehelpdesk nu genoodzaakt tot het aanboren van nieuwe financieringsbronnen. Hier zet de Fraudehelpdesk de afgelopen jaren ook op in.

Hoewel de Fraudehelpdesk een private stichting is, is de Fraudehelpdesk voornamelijk afhankelijk van publieke middelen. Het verminderen van de afhankelijkheid van het ministerie van JenV als enige subsidieverstrekker, door het aanboren van andere financieringsbronnen maakt de organisatie minder kwetsbaar. Tegelijkertijd zal publieke financiering wel noodzakelijk zijn, omdat het gaat om publieke diensten waar marktpartijen waarschijnlijk niet in zullen voorzien.

Dat de organisatie van de Fraudehelpdesk kwetsbaar is wordt ook in meerdere gesprekken met ketenpartners aangegeven. Ketenpartners geven aan dat de kwetsbaarheid wordt veroorzaakt door het beperkte budget dat de Fraudehelpdesk ter beschikking staat. Ketenpartners zien wel dat de Fraudehelpdesk met een kleine groep werknemers veel werk verricht. Voldoende slagkracht in de toekomst is bij het voorkomen en bestrijden van fraude volgens meerdere ketenpartners van belang.

Uit de evaluatie blijkt dat de subsidievoorwaarden zoals die in 2010 zijn opgesteld niet meer van toepassing zijn. Wel wordt aan het merendeel van de destijds relevant geachte voorwaarden nog voldaan.

De bijdrage van de Fraudehelpdesk aan de preventie en bestrijding van horizontale fraude

De vraag welke bijdrage de Fraudehelpdesk heeft geleverd aan het bereiken van de doelstellingen is niet eenduidig en nauwkeurig te beantwoorden en het beoordelen van de effectiviteit van de diensten is in de praktijk ingewikkeld. De weerbaarheid van burgers en de ondersteuning van slachtoffers is nauwelijks meetbaar; beide worden beïnvloed door een groot aantal factoren. Bovendien ontbreekt een nulmeting, waardoor de maatregelen niet op effectiviteit kunnen worden beoordeeld. Het toetsen van de beleidstheorie is om deze redenen niet mogelijk. We hebben daarom gekeken naar de wijze waarop de Fraudehelpdesk invulling geeft aan het bereiken van de doelen en hoe de dienstverlening wordt beoordeeld door melders en ketenpartners.

Hoewel de vraag welke bijdrage de Fraudehelpdesk heeft geleverd aan het bereiken van de doelstellingen niet eenduidig en nauwkeurig te beantwoorden is, lijkt de Fraudehelpdesk wel een zekere meerwaarde te hebben. Bevindingen uit het vragenlijstonderzoek geven een indicatie van de mate waarin slachtoffers van fraude zich ondersteund voelen. De uitkomsten van het vragenlijstonderzoek ondersteunen gedeeltelijk de veronderstelling dat slachtoffers ondersteund worden, aangezien de helft van de respondenten tevreden is over de wijze waarop ze door de Fraudehelpdesk zijn geholpen en 61% van de respondenten het gevoel heeft naar de juiste organisatie te zijn doorverwezen. Toch blijkt uit het vragenlijstonderzoek ook dat lang niet alle respondenten tevreden zijn over de wijze waarop ze door de Fraudehelpdesk zijn

geholpen. Dit lijkt met name te komen door het feit dat een deel van de melders een andere verwachting had van de Fraudehelpdesk, namelijk dat er actie zou worden ondernomen tegen de fraudeur.

Er is geen directe informatiebron in dit onderzoek die inzicht geeft in de bijdrage van de Fraudehelpdesk aan het weerbaarder maken van burgers en bedrijven tegen (pogingen tot) oplichting. Afgaande op interviews met ketenpartners is het aannemelijk dat de Fraudehelpdesk bijdraagt aan het weerbaarder maken van burgers en bedrijven, zeker als het gaat om het geven van voorlichting. Ketenpartners zien met name op het gebied van preventie meerwaarde in de Fraudehelpdesk. Uit interviews met de Fraudehelpdesk en deskresearch blijkt dat de Fraudehelpdesk jaarlijks (in samenwerking met ketenpartners) campagnes opzet, waarschuwingsberichten over actuele fraudevormen plaatst en een maandmonitor met actuele informatie over trends en ontwikkelingen uitbrengt. Wel kunnen op basis van de literatuur enkele kritische kanttekeningen worden gemaakt bij de effectiviteit van het verstrekken van algemene informatie door bijvoorbeeld campagnes.

De positie van de Fraudehelpdesk in het landschap van meldpunten voor horizontale fraude

Uit de beleidsreconstructie blijkt dat het idee destijds was om één helpdesk op te richten waar burgers én bedrijven terechtkonden voor advies en antwoorden op vragen op het gebied van financieel-economische criminaliteit.⁴ Tegenwoordig zijn er tal van meld- en hulppunten voor horizontale fraude, waarvan de Fraudehelpdesk er één is. In dit onderzoek zijn in totaal 65 meld- en hulppunten geïnventariseerd.

De Fraudehelpdesk gebruikt meldingen over (potentiële) fraude om een bijdrage te leveren aan de voorkant van de fraudebestrijdingsketen (preventie en ondersteuning slachtoffers) en niet aan de achterkant van de keten (aanpakken en onderzoeken van fraudezaken). Hierin onderscheidt de Fraudehelpdesk zich van een groot aantal meldpunten dat onderdeel uitmaakt van grotere bedrijven, instellingen of publieke meldpunten die meldingen verzamelen als aanleiding voor onderzoek en opsporing of om maatregelen tegen fraudeurs te kunnen treffen. Daarnaast richt het merendeel van de meldpunten verbonden aan een groter bedrijf of instelling zich op specifieke vormen van fraude die niet altijd direct burgers of kleine ondernemers raken. Uit het onderzoek naar het landschap van fraudemeldpunten blijkt dat de Fraudehelpdesk geen diensten verleent die uniek zijn, maar de combinatie van diensten en de brede oriëntatie op alle vormen van fraude zijn in het landschap van fraudemeldpunten is wel uniek.

Het (verder) verbeteren van de doelbereiking van de Fraudehelpdesk

Van 'melddesk' naar 'helpdesk'

In de gesprekken met ketenpartners is aangegeven dat de naam 'Fraudehelpdesk' impliceert dat slachtoffers (inhoudelijk) worden geholpen. Dit is in beperkte mate het geval, waardoor de Fraudehelpdesk meer lijkt op een 'melddesk' dan op een 'helpdesk'. Uit het vragenlijstonderzoek blijkt dat 22% van de respondenten (zeer)ontevreden is over de wijze waarop ze door de Fraudehelpdesk zijn geholpen. Een van de belangrijkste oorzaken hiervan lijkt dat de melders een andere verwachting hadden van de dienstverlening door de Fraudehelpdesk; ze hadden verwacht dat er door de Fraudehelpdesk actie zou worden ondernomen. Mogelijkheden die tijdens de expertmeeting naar voren kwamen om slachtoffers meer te ondersteunen zijn

⁴ Kamerstukken II 2008/09 29 911, nr. 32, p.2.

het bieden van hulp bij het doen van aangifte, het invullen van formulieren of het verhalen van schade. Ook het warm doorverwijzen zou vanuit het perspectief van het slachtoffer meer waarde hebben. Slachtoffers hoeven dan niet meerdere keren hun verhaal te vertellen. Bovendien haken bij koud doorverwijzen veel melders af. Een deel van de informatie gaat op dit moment dus verloren. Maar warm doorverwijzen stuit op juridische bezwaren vanwege de persoonsgegevens die dan moeten worden doorgegeven.

De Fraudehelpdesk beschikt over waardevolle data, maar kan daar meer mee doen

De Fraudehelpdesk beschikt volgens de meerderheid van de ketenpartners over relevante en waardevolle informatie. De trends en ontwikkelingen die de Fraudehelpdesk signaleert worden over het algemeen ook herkend door ketenpartners. Wel geeft de informatie van de Fraudehelpdesk geen compleet beeld als het gaat om onder meer schadebedragen en aantallen slachtoffers. In de expertmeeting is aangegeven dat het waardevol zou zijn informatie van verschillende ketenpartners samen te brengen, zodat een meer compleet beeld ontstaat van de actuele stand van zaken rondom fraude. Daarbij hoeven niet direct persoonsgegevens van strafrechtelijke aard te worden gedeeld, omdat het kan gaan om gegevens op geabstraheerd niveau die niet tot personen herleidbaar is. Mogelijk ligt hier een rol voor de Fraudehelpdesk.

Versterken van de beleidsinhoudelijke relatie tussen het ministerie en de Fraudehelpdesk

Al jaren is preventie een van de belangrijkste pijlers van het fraudebeleid van het ministerie van JenV. In het kader van preventie verleent het ministerie subsidie aan de Fraudehelpdesk. Uit onder meer gesprekken met de Fraudehelpdesk volgt dat er de laatste jaren nauwelijks inhoudelijke afstemming is tussen het ministerie en de Fraudehelpdesk. Ook lijkt sturing vanuit het ministerie door middel van het stellen van subsidievoorwaarden de laatste jaren beperkt te zijn. Er zijn geen output/outcome-afspraken over de geleverde diensten. De doelbereiking van de Fraudehelpdesk kan verder worden verbeterd door in te zetten op structurele inhoudelijke afstemming met het ministerie over onder meer trends en ontwikkelingen, zodat deze informatie een bijdrage levert aan toekomstig beleid. Het ministerie heeft aangegeven dat het passend is om in de toekomst meer vraaggestuurd te gaan samenwerken vanuit een meerjarige beleidsvisie, maar eerst onderzoek te willen laten doen naar de bijdrage van de inrichting van de Fraudehelpdesk aan het behalen van de doelstellingen.⁵ De Fraudehelpdesk en het ministerie lijken het erover eens dat de beleidsinhoudelijke relatie voor verbetering vatbaar is.⁶

Continuïteit en stabiliteit in de financiering van de Fraudehelpdesk

De Fraudehelpdesk geeft aan dat de jaarlijkse subsidietoekenning veel financiële onzekerheid oplevert over de continuïteit van de organisatie en de Fraudehelpdesk beperkt in ontwikkelambities. Het is begrijpelijk dat de subsidiesystematiek een jaarlijkse cyclus kent, maar de inbedding in een meerjarenrelatie zou de Fraudehelpdesk meer stabiliteit geven en minder kwetsbaar maken.

Persoonsgegevens van strafrechtelijke aard

Voor het mogen verwerken van persoonsgegevens van strafrechtelijke aard ten behoeve van derden is een vergunning van de AP vereist. De aanvraag voor een vergunning door de Fraudehelpdesk voor het mogen verwerken van deze persoonsgegevens ten behoeve van de

⁵ Subsidietoekenning, 26 januari 2023.

⁶ Subsidietoekenning, 26 januari 2023.

helpdeskfunctie, heeft de AP afgewezen. De AP is – kortgezegd - van oordeel dat het niet noodzakelijk is dat de Fraudehelpdesk voor het adviseren van melders persoonsgegevens van strafrechtelijke aard kan verwerken.

De Fraudehelpdesk ervaart het niet mogen verwerken van persoonsgegevens van strafrechtelijke aard als een belemmering in het kunnen bieden van een optimale dienstverlening. Voor het behandelen van een melding is een goed beeld krijgen van de situatie noodzakelijk. Daarvoor is volgens de Fraudehelpdesk kennisneming van de onderliggende stukken van de melding (die persoonsgegevens van strafrechtelijke aard kunnen bevatten) nodig.⁷ Uit het vragenlijstonderzoek blijkt dat meer dan de helft van de respondenten (56%) tevreden is over het advies van de Fraudehelpdesk. In die zin lijkt, ondanks dat de Fraudehelpdesk op dit moment geen gegevens over de (mogelijke) fraudeur mag ontvangen, geen sprake te zijn van een grote ontevredenheid over de adviezen van de Fraudehelpdesk.

De meningen van ketenpartners ten aanzien van de meerwaarde van het delen van persoonsgegevens tussen organisaties zijn verdeeld. Een aantal ketenpartners is met de Fraudehelpdesk van mening dat door het delen van gegevens over fraudeurs, fraude beter kan worden bestreden. Enkele ketenpartners die deelnamen aan de expertmeeting zagen niet direct die noodzaak en wierpen de vraag op in hoeverre het bestrijden van fraude door de Fraudehelpdesk past bij de doelstellingen waarvoor de Fraudehelpdesk is opgericht.

Persoonsgegevens van strafrechtelijke aard zijn gevoelige gegevens. Het delen van deze gegevens met andere partijen kan een aanzienlijke inbreuk maken op de persoonlijke levenssfeer van betrokkenen. Uit de beleidsreconstructie volgt dat de Fraudehelpdesk is opgericht om met name aan de voorkant van de fraudebestrijdingsketenvoorkant een bijdrage te leveren. Met het delen van persoonsgegevens over fraudeurs aan andere organisaties zal de Fraudehelpdesk meer aan de achterkant (aanpakken van fraude) actief worden. Gelet op de doelstellingen die uit de beleidsreconstructie naar voren kwamen lijkt die inzet aan de achterkant dus niet voor de hand te liggen. Duidelijk is dat wanneer er een politieke en maatschappelijke wens bestaat voor het verwerken van persoonsgegevens van strafrechtelijke aard ten behoeve van derden door de Fraudehelpdesk, en de AP geen vergunning verleent, het nodig is hiervoor een expliciete wettelijke grondslag te creëren.

Ontwikkelrichtingen

Het ministerie wil deze evaluatie afwachten voor nadere besluitvorming voor de herijking van zowel de beleids- als de financieringsrelatie met de Fraudehelpdesk. Voor wat betreft de toekomst van de Fraudehelpdesk zijn verschillende ontwikkelrichtingen denkbaar. Op basis van dit onderzoek is het niet mogelijk eenduidige uitspraken te doen over de bijdrage die de Fraudehelpdesk, in het geval de Fraudehelpdesk op huidige wijze doorgaat, zal leveren aan het ondersteunen van slachtoffers en het weerbaarder maken van burgers en bedrijven tegen (pogingen) tot fraude. Wel lijkt de huidige dienstverlening van de Fraudehelpdesk gelet op de bevindingen van dit onderzoek een zekere meerwaarde te hebben op het gebied van preventie en het ondersteunen van slachtoffers.

Een andere mogelijkheid is dat de Fraudehelpdesk in de toekomst verdwijnt. In dat geval kan er op termijn een lacune op het gebied van fraudepreventie ontstaan. Zoals uit het onderzoek

⁷ Fraudehelpdesk, aanvulling beroepsschrift tegen het besluit met kenmerk z2021-14398, 22 mei 2022, p. 9.

naar het landschap van fraudemeldpunten blijkt is de Fraudehelpdesk de enige organisatie die is toegespitst op alle vormen van fraude. Bij het verdwijnen van de Fraudehelpdesk, verdwijnt een organisatie die een overkoepelend beeld heeft en trends en ontwikkelingen signaleert over alle vormen van fraude. Uit de gesprekken met ketenpartners komt naar voren dat ketenpartners deze informatie, onder meer met het oog op preventie, nuttig achten. Op basis van dit onderzoek is het niet mogelijk uitspraken te doen of andere organisaties (een deel van) de diensten van de Fraudehelpdesk (kunnen) overnemen wanneer de Fraudehelpdesk verdwijnt.

Een laatste ontwikkelrichting is dat de Fraudehelpdesk de huidige dienstverlening doorontwikkelt. Daarbij kan gedacht worden aan het (praktisch) ondersteunen van slachtoffers en het bij elkaar brengen van informatie van ketenpartners op het gebied van trends en ontwikkelingen. Het doorontwikkelen van de huidige dienstverlening kan de meerwaarde van de Fraudehelpdesk (verder) vergroten. Het doorontwikkelen van diensten vraagt naar verwachting wel om meer tijd en capaciteit en dus om meer middelen.

1 Inleiding

1.1 Aanleiding

In Nederland zijn er diverse informatie- en meldpunten waar burgers en bedrijven informatie kunnen inwinnen over (nieuwe) vormen van horizontale fraude, waarbij burgers en bedrijven worden benadeeld en waar fraude en oplichting kunnen worden gemeld.⁸ Een van die fraudemeldpunten – het meldpunt dat in dit onderzoek centraal staat en zich op alle vormen van fraude richt – is de Fraudehelpdesk. Stichting SafeCin heeft de Fraudehelpdesk opgericht, nadat het ministerie van Justitie en Veiligheid (hierna: JenV) eind 2010 daarvoor een subsidie beschikbaar stelde.

Het ministerie van JenV is op dit moment de enige subsidieverstrekker. Dit evaluatieonderzoek beoogt de besluitvorming over de verdere subsidiëring, de hoogte van de toe te kennen subsidie, de doelen van de subsidie en daarbij te stellen voorwaarden te ondersteunen.

1.2 Vraagstelling en onderzoeksthema's

De volgende onderzoeksvragen stonden in het onderzoek centraal:⁹

6. Welke positie bekleedt de Fraudehelpdesk in het veld van de Nederlandse fraude preventie en -bestrijding?
7. In hoeverre kunnen de doelen die de Fraudehelpdesk nastreeft in theorie via de geldende subsidievoorwaarden en het inrichtingsplan van de Fraudehelpdesk worden bereikt?
8. In welke mate volstaat de praktische invulling van het inrichtingsplan van de Fraudehelpdesk in het bereikbaar maken van deze doelen?
9. Welke bijdrage heeft de Fraudehelpdesk geleverd aan de preventie en bestrijding van horizontale fraude?

⁸ Met de nota Zicht op fraude expliciteerde het Openbaar Ministerie in 1997 het onderscheid tussen verticale en horizontale fraude. Bij verticale fraude is de overheid de benadeelde partij. Bij horizontale fraude wordt een burger of bedrijf benadeeld.

⁹ In bijlage 1 en in paragraaf 1.3 zijn de deelvragen van het onderzoek opgenomen.

10. Hoe zou de toekomstige doelbereiking van de Fraudehelpdesk (verder) kunnen worden verbeterd? Zijn er structurele of procesmatige aanpassingen nodig om de toekomstige bijdrage van de Fraudehelpdesk aan fraudepreventie en -bestrijding in Nederland te verbeteren?

Het onderzoek is uitgevoerd aan de hand van vier deelonderzoeken:

- I. Planevaluatie
- II. Procesevaluatie
- III. Het landschap van meldpunten
- IV. Synthese

Planevaluatie

In de planevaluatie stond de vraag centraal waarom een beleidsinterventie (het oprichten van een helpdesk) zou *kunnen* werken centraal. In dit deelonderzoek hebben we de beleidstheorie in beeld gebracht en op basis daarvan een doelenboom opgesteld. De door ons gereconstrueerde beleidstheorie is voorgelegd aan experts op het gebied van fraude(bestrijding). We vroegen hen of de maatregel geschikt was om de doelen te bereiken. Daarnaast is gekeken of er in de wetenschappelijke literatuur onderbouwing kan worden gevonden voor de veronderstelde werkzame mechanismen.

Procesevaluatie

De mogelijke effectiviteit van de Fraudehelpdesk wordt niet alleen bepaald door de kwaliteit van de beleidstheorie, maar ook door de uitvoering en de organisatie van de Fraudehelpdesk. Dat stond centraal in de procesevaluatie. Die richtte zich op de uitvoering van de Fraudehelpdesk in de praktijk. Daarnaast zijn knelpunten in de uitvoering in kaart gebracht. Omdat de uitvoering meerdere aspecten raakt richtte de procesevaluatie zich op vier onderdelen: de uitvoering, de bekendheid van de Fraudehelpdesk, de waardering van de Fraudehelpdesk, en de knelpunten. De onderzoeksactiviteiten voor de procesevaluatie zijn uitgevoerd in de eerste helft van 2023.

Het landschap van fraudemeldpunten

In de loop der jaren is er een veelheid aan fraudemeldpunten ontstaan. Sommige meldpunten richten zich op specifieke vormen van fraude, zoals hypotheekfraude, telecomfraude of voorschotfraude. Andere meldpunten, zoals de Fraudehelpdesk, richten zich op veel verschillende vormen van horizontale fraude. Horizontale fraude gaat over fraude die is gericht tegen burgers, financiële instellingen of bedrijven. In dit deelonderzoek zijn bestaande fraudemeldpunten voor horizontale fraude geïnventariseerd. We hebben gekeken met welke meldpunten er overlap in diensten bestaat en waarin de Fraudehelpdesk zich onderscheidt van de diensten van andere meldpunten. In het onderzoek wordt naar verschillende fraudevormen verwezen. In bijlage 9 is een overzicht met definities opgenomen.

Synthese

Het onderzoek is afgesloten met een synthesefase. Daarin zijn alle bevindingen uit de drie deelonderzoeken, samengevat en vertaald naar conclusies over de Fraudehelpdesk in het algemeen en worden de onderzoeksvragen beantwoord.

1.3 Onderzoeksaanpak

Startgesprek

Het onderzoek ging van start met een startgesprek met de directeur van de Fraudehelpdesk. In dit gesprek zijn de onderzoeksactiviteiten die we wilden uitvoeren en waarbij medewerking van de Fraudehelpdesk nodig was toegelicht. Onder meer zijn afspraken gemaakt over het uitzetten van een vragenlijst onder melders en het aanleveren van documenten.

Deskresearch

Bij aanvang van het onderzoek is informatie over de totstandkoming van de Fraudehelpdesk verzameld en bestudeerd. Daarbij ging het in de eerste plaats om parlementaire stukken, zoals Kamerstukken en (voortgangs)brieven van de minister aan de Tweede Kamer. Op basis van het bestuderen van deze stukken is de beleidstheorie in beeld gebracht en een doelenboom opgesteld. Daarnaast is gezocht naar relevante literatuur en documenten met informatie over de veronderstellingen waarop de beleidstheorie is gebaseerd.

Om de jaarlijkse ontwikkelingen sinds 2012 op het gebied van financiën en geleverde diensten in beeld te brengen, hebben we alle jaarverslagen vanaf 2012 van de Fraudehelpdesk bestudeerd. De jaarverslagen bevatten ook informatie over ontwikkelingen in de samenwerking met ketenpartners en de geleverde diensten. Ook zijn documenten bestudeerd die door de Fraudehelpdesk zijn aangeleverd. Het gaat daarbij onder andere om documenten over de subsidieverlening door het ministerie van JenV en het ministerie van Economische Zaken (hierna: EZK), onderzoeken die de Fraudehelpdesk heeft laten uitvoeren naar de naamsbekendheid, functieprofielen van medewerkers van de Fraudehelpdesk, het communicatieplan van 2023, het organogram en de statuten. Een overzicht van de voor dit rapport gebruikte documenten is opgenomen in bijlage 2.

Interviews

Om een beeld te krijgen van onder andere de (ontwikkeling van) diensten die de Fraudehelpdesk verleent en de knelpunten en uitdagingen, is in de beginfase van het onderzoek face-to-face met vijf medewerkers van de Fraudehelpdesk en digitaal met twee leden van de Raad van Toezicht gesproken. Daarnaast is ook een verdiepend gesprek gevoerd met de directeur van de Fraudehelpdesk.

Een onderdeel van het onderzoek was het in beeld brengen van de waardering van de dienstverlening door ketenpartners. Op basis van de ketenpartners die in jaarverslagen van de Fraudehelpdesk worden genoemd en is een lijst opgesteld met ketenpartners die we graag wilden interviewen. Het gaat daarbij om organisaties waar de Fraudehelpdesk mee samenwerkt en/of melders naar doorverwijst. De Fraudehelpdesk heeft ons contactgegevens van deze ketenpartners toegestuurd en heeft nog een enkele andere suggestie voor een ketenpartner gedaan. In totaal hebben we met zeventien gesprekspartners bij veertien verschillende ketenpartners gesproken. Onderwerpen die in deze gesprekken aan bod kwamen betroffen: de relatie en samenwerking met de Fraudehelpdesk, de waardering van de dienstverlening, en knelpunten en uitdagingen.

Ten slotte is gesproken met twee experts op het gebied van fraude. We hebben aan hen de doelenboom voorgelegd en de input van deze gesprekken is benut om te reflecteren op de

veronderstellingen die ten grondslag liggen aan de beleidstheorie. Een overzicht met functies van de gesprekspartners is opgenomen in bijlage 3.

Registratieonderzoek

Informatie uit de jaarverslagen is benut om het aantal doorverwijzingen, telefonische en digitale meldingen en kosten van de gemelde schade in beeld te brengen. Daarnaast is informatie aangeleverd door de Fraudehelpdesk over het aantal websitebezoekers. De informatie uit de jaarverslagen is met name terug te vinden in hoofdstuk 3 'Fraudehelpdesk: organisatie, financiën en activiteiten.' Dit hoofdstuk is voorgelegd aan tien ketenpartners met als doel om te verifiëren of de informatie en ontwikkelingen die in het hoofdstuk worden geschetst, werden herkend. Van vier ketenpartners is hierop een reactie ontvangen. De ketenpartners gaven aan dat het beeld overeenkwam met hun eigen waarneming.

Websiteonderzoek

Een websiteonderzoek is uitgevoerd om inzicht te krijgen in de vindbaarheid van de website van de Fraudehelpdesk. Hiervoor is gestart met het opstellen van een lijst met voor de hand liggende zoektermen, die vervolgens met synoniemen zijn aangevuld. Per zoekterm is gekeken op welke positie in Google de website van de Fraudehelpdesk verscheen. Een uitgebreide toelichting op de aanpak van het websiteonderzoek is opgenomen in hoofdstuk 4. Daarnaast is gekeken in hoeverre de website van de Fraudehelpdesk eenvoudig vindbaar is via websites van ketenpartners, door daarnaar op die websites te zoeken.

Vragenlijst en telefonische interviews melders

Om de waardering van de Fraudehelpdesk door melders te onderzoeken hebben we een digitale vragenlijst uitgezet onder bijna tweeduizend melders. De Fraudehelpdesk heeft drie weken nadat iemand een melding had gedaan, en aangegeven had mee te willen werken aan een vragenlijstonderzoek, een uitnodiging naar de melder gestuurd om deel te nemen aan het vragenlijstonderzoek. Dit heeft geleid tot in totaal 412 (deels en volledig) ingevulde vragenlijsten. Een responsverantwoording is opgenomen in hoofdstuk 5. De vragenlijst is opgenomen in bijlage 4.

Na afronding van het vragenlijstonderzoek is met een aantal respondenten contact opgenomen om een aantal aanvullende vragen te stellen. We spraken met tien respondenten die aangaven dat ze bereid waren om een aanvullende toelichting te geven. Bij de selectie van de respondenten is rekening gehouden met spreiding over het type melder (particulier/ondernemer) de wijze waarop een melding is gedaan (telefonisch en/of via het formulier op de website van de Fraudehelpdesk, of op andere wijze). Daarnaast is gekeken naar antwoorden waarop een nadere toelichting nuttig was. Hierdoor konden we doorvragen bij opvallende antwoorden.

Landschap fraudemeldpunten

Een van de deelonderzoeken was het in kaart brengen van het landschap van meldpunten voor horizontale fraude. Hiervoor is gebruik gemaakt van een eerdere inventarisatie van fraudemeldpunten uit 2015 van Homburg en Van den Tillaart.¹⁰ De inventarisatie uit dat onderzoek is geactualiseerd en aangevuld met nieuwe meldpunten. Voor het in kaart brengen van nieuwe meldpunten is gebruik gemaakt van de lijst met zoektermen die in het kader van het

¹⁰ Homburg en Van den Tillaart 2015.

websiteonderzoek is opgesteld. In hoofdstuk 6 is een uitgebreide toelichting op het onderzoek naar het landschap van fraudemeldpunten opgenomen.

Expertmeeting

Het onderzoek is afgesloten met een expertmeeting waarin we onze voorlopige bevindingen hebben voorgelegd aan ketenpartners en hebben besproken hoe de toekomstige doelbereiking van de Fraudehelpdesk (verder) kan worden verbeterd. Aan de expertmeeting nam een wetenschapper deel, het OM, de Politie, het ministerie van JenV (vanuit de integrale aanpak online fraude) de Ouderenbond, Seniorweb, en het Centraal Meldpunt Identiteitsfraude. In bijlage 3 is een overzicht van de deelnemers aan de expertmeeting gegeven.

Wederhoor

De laatste versie van het concepteindrapport (zonder de analyse) is voor wederhoor voorgelegd aan de Fraudehelpdesk voor een feitencheck. Naar aanleiding daarvan is een kort gesprek gevoerd met de interim-directeur van de Fraudehelpdesk. Daarnaast heeft de Fraudehelpdesk in het document van het concepteindrapport opmerkingen geplaatst. Feitelijke onjuistheden zijn gecorrigeerd en enkele suggesties voor aanvullingen zijn in het rapport overgenomen.

Onderstaande tabel beschrijft de methoden ingezet voor de beantwoording van de verschillende deelvragen.

Onderzoeksthema I: planevaluatie		Onderzoeksmethoden
1.	Wat is er beoogd met het oprichten van de Fraudehelpdesk? Welke doelen worden er met de Fraudehelpdesk nagestreefd?	Deskresearch Interviews Fraudehelpdesk en JenV/EZK
2.	Kunnen de beoogde doelen worden bereikt via het inrichtingsplan van de Fraudehelpdesk?	Deskresearch Interviews Fraudehelpdesk en JenV/EZK
Onderzoeksthema II: procesevaluatie		
3.	Welke ontwikkelingen waren er sinds de evaluatie in 2012 met betrekking tot de financiering van de Fraudehelpdesk en de geleverde diensten door de Fraudehelpdesk?	Deskresearch Interviews Fraudehelpdesk en JenV/EZK Registratieonderzoek
4.	Welke rol spelen de 23 formele subsidievoorwaarden die in de subsidieaankondiging uit 2010 zijn opgenomen in de huidige uitvoering van de diensten van de Fraudehelpdesk?	Deskresearch Interviews Fraudehelpdesk en JenV/EZK Websiteonderzoek
5.	In welke mate kunnen via de praktische inrichting van de Fraudehelpdesk de gestelde doelen ook worden bereikt?	Interviews Fraudehelpdesk en JenV/EZK Deskresearch
6.	In welke mate voorziet de Fraudehelpdesk in een behoefte van burgers en bedrijven?	Digitale vragenlijst melders Telefonische interviews melders Deskresearch
7.	Wat kan er worden gezegd over de bijdrage van de Fraudehelpdesk aan het functioneren van de fraudebestrijdingsketen?	Interviews ketenpartners Deskresearch Websiteonderzoek

8.	Hoe beoordelen burgers en bedrijven die contact hebben gehad met de Fraudehelpdesk de dienstverlening en de verstrekte informatie en/of het advies?	Digitale vragenlijst melders Telefonische interviews melders
9.	Hoe oordelen de ketenpartners van de Fraudehelpdesk over de dienstverlening van de helpdesk? Hoe kan de dienstverlening van de Fraudehelpdesk volgens de ketenpartners (verder) worden verbeterd?	Interviews ketenpartners
10.	Zijn er momenteel knelpunten die de bijdrage van de Fraudehelpdesk aan de preventie en bestrijding van fraude hinderen of in de weg staan? Welke zijn dat?	Interviews Fraudehelpdesk en ketenpartners
11.	Zijn er neveneffecten verbonden aan de dienstverlening door de Fraudehelpdesk? Welke zijn dat en hoe kunnen deze worden geduïd?	Interviews Fraudehelpdesk en ketenpartners
Onderzoeksthema III: Fraudehelpdesk in het landschap van meldpunten voor horizontale fraude		
12.	Welke loketten zijn er naast de Fraudehelpdesk in Nederland voor het melden van slachtofferschap en informatie over horizontale fraude en oplichting (onder burgers en bedrijven)? Wat is de specifieke rol van de meldpunten?	Deskresearch/onderzoek landschap fraudemeldpunten
Onderzoeksthema IV: Synthese		
13.	In hoeverre draagt de plaats van de Fraudehelpdesk in het Nederlandse fraudebestrijdingslandschap en de inrichting en uitvoering van de diensten van de Fraudehelpdesk bij aan de preventie en bestrijding van horizontale fraude?	Analyse Expertmeeting
14.	Op welke wijze zou de toekomstige bijdrage van de Fraudehelpdesk aan de preventie en bestrijding van fraude (verder) kunnen worden verbeterd?	Analyse Expertmeeting

1.4 Leeswijzer

In hoofdstuk 2 gaan we in op de beleidstheorie, de daaruit voortvloeiende doelenboom en een beoordeling van de beleidstheorie. Hoofdstuk 3 bevat een beschrijving van de organisatie van de Fraudehelpdesk, de ontwikkelingen in de financiering en dienstverlening en de subsidievoorwaarden. Hoofdstuk 4 behandelt de bekendheid van de Fraudehelpdesk aan de hand van onderzoek naar de vindbaarheid van de website en de naamsbekendheid van de Fraudehelpdesk. In hoofdstuk 5 worden de bevindingen over de waardering van de Fraudehelpdesk door ketenpartners en melders toegelicht. In hoofdstuk 6 worden de resultaten van het onderzoek naar het landschap van fraudemeldpunten gepresenteerd en ten slotte bevat hoofdstuk 7 een analyse en conclusie.

2 Beleidsreconstructie

2.1 Inleiding

In dit hoofdstuk komt de beleidstheorie voor het oprichten van een helpdesk op het gebied van fraude aan bod en worden deelvraag 1 en 2 beantwoord. Op basis van de wetsgeschiedenis en gesprekken met medewerkers van het ministerie van JenV en het ministerie van EZK is in beeld gebracht wat de aanleiding is geweest voor het oprichten van een helpdesk. De reconstructie van de beleidstheorie is opgenomen in paragraaf 2.2. In paragraaf 2.3 is de informatie uit Kamerstukken en interviews weergegeven in een doelenboom. Paragraaf 2.4 gaat in op de vraag of de maatregel geschikt was om de doelen te bereiken. Ten slotte wordt in paragraaf 2.5 gekeken in hoeverre de veronderstellingen over de wijze waarop de doelstellingen van de Fraudehelpdesk zouden moeten worden bereikt overeenkomen met de inrichting van de Fraudehelpdesk.

2.2 Totstandkoming van de Fraudehelpdesk

Het ministerie van JenV stelt eind 2010 voor een proefperiode van één jaar € 500.000 beschikbaar voor het oprichten van een helpdesk financieel-economische criminaliteit.¹¹ De subsidie wordt toegekend aan de Stichting Aanpak Financieel-Economische Criminaliteit in Nederland (SafeCin), die in februari 2011 de Fraudehelpdesk opent. In de jaren voorafgaand aan de oprichting van de Fraudehelpdesk is binnen het kabinet-Balkenende IV en de Tweede Kamer nagedacht en gediscussieerd over het doel, de uitgangspunten en de reikwijdte van een dergelijke helpdesk.

Motie De Wit en Azough

De aanleiding voor het oprichten van een helpdesk is mede terug te voeren op een aangenomen Tweede Kamermotie, ingediend op 15 november 2007 door Kamerleden De Wit (SP) en Azough (Groen Links). In de motie wordt de regering gevraagd onderzoek te verrichten naar de bestaande en mogelijke hulp aan slachtoffers van financieel-economische misdaad en daarvoor met concrete voorstellen te komen.¹² De Wit en Azough overwegen dat de regering het

¹¹ In 2010 heette het ministerie nog het ministerie van VenJ, maar ten behoeve van de leesbaarheid is overal JenV gebruikt.

¹² *Kamerstukken II 2007/08*, 31 200 VI, nr. 48; *Handelingen II 2007/08* nr. 28, p. 2191-2194.

voornemen heeft te komen met een voorstel voor een integrale aanpak van financieel-economische criminaliteit, maar zijn van mening dat er tot op dat moment onvoldoende aandacht is voor de schade van slachtoffers van financieel-economische misdaad.¹³

Kabinet-Balkenende IV - de aanpak van financieel-economische criminaliteit

Kabinet-Balkenende IV wil in de jaren na 2007 maatregelen treffen om de aanpak van financieel-economische criminaliteit te versterken. Volgens het kabinet is preventie het centrale uitgangspunt in de fraudeaanpak. De preventieve aanpak wil het kabinet versterken door in het kader van het Actieplan Veilig Ondernemen deel 3, de publiek-private samenwerkingen verder uit te bouwen. Daarbij wordt ook het Nationaal Platform Criminaliteitsbeheersing (NPC) benut. Verder worden maatregelen getroffen zoals de inrichting van een hulpdienst of meldpunt voor slachtoffers van oplichting.¹⁴

In de jaren na de motie vinden verschillende Algemene Overleggen plaats en wordt de Kamer meermaals geïnformeerd over de voortgang van het oprichten van een helpdesk. Het oprichten van een helpdesk voor mensen die vragen hebben over financieel-economische criminaliteit, die daarvan geen slachtoffer willen worden en voor slachtoffers, zal onderdeel worden van het Actieplan Veilig Ondernemen deel 3 van het NPC.¹⁵

Nationaal Platform Criminaliteitsbeheersing

Het NPC is een samenwerkingsverband tussen de overheid en het bedrijfsleven dat zich richt op de aanpak van verschillende vormen van criminaliteit waarmee het bedrijfsleven te maken heeft. Dit doet het NPC door criminaliteitsvraagstukken te agenderen die het bedrijfsleven raken en door samen te werken (o.a. door het opzetten van projecten uitvoeren van onderzoek en kennisdeling) aan mogelijke oplossingen.

Volgens de minister is het wenselijk dat de overheid consumenten helpt weerbaar te worden als het gaat om de beslissing al of niet in zee te gaan met financieel-economische aanbiedingen en hen helpt zich bewust te worden van de eigen mogelijkheden om te voorkomen slachtoffer te worden.¹⁶ Onderzoek onder burgers heeft namelijk uitgewezen dat er behoefte is aan een helpdesk waar mensen informatie kunnen krijgen over oplichting.¹⁷ Het idee is om één helpdesk op te richten waar burgers én bedrijven terecht kunnen voor advies en antwoorden op vragen op het gebied van financieel-economische criminaliteit.¹⁸ De minister merkt op dat de helpdesk geen advies geeft over individuele aanbiedingen. Wel kan informatie worden gegeven over datgene waar mensen op moeten letten bij het ingaan op een bepaalde aanbieding en wat mogelijke risico's zijn.¹⁹ Verder zal bij meer complexe vragen door de helpdesk worden samengewerkt met bestaande organisaties die op dit gebied deskundig zijn. De helpdesk kan ook wijzen op de mogelijkheid om private organisaties in te schakelen, bijvoorbeeld in het geval van producten van individuele aanbieders.²⁰

¹³ Kamerstukken II 2007/08, 31 200 VI, nr. 48.

¹⁴ Kamerstukken II, 2007/08, 28 684, nr. 119, p. 18.

¹⁵ Kamerstukken II 2008/09, 29 911, nr. 22, p. 43.

¹⁶ Kamerstukken II 2008/09, 29 911, nr. 32.

¹⁷ Oudejans en Vis 2008.

¹⁸ Kamerstukken II 2008/09 29 911, nr. 32, p. 2.

¹⁹ Kamerstukken II 2008/09 29 911, nr. 32, p. 2.

²⁰ Kamerstukken II 2008/09 29 911, nr. 32, p. 2.

Oprichting digitaal loket voor bedrijven

Begin 2010 informeert de minister van JenV de Tweede Kamer over de besluitvorming in het NPC over de helpdesk financieel-economische criminaliteit.²¹ Waar eerder het idee was om een helpdesk voor burgers én bedrijven op te zetten, is nu besloten alleen een digitaal loket voor bedrijven op te zetten.

Met de betrokken ministeries en in overleg met private partijen is vastgesteld dat de Consumentenautoriteit (ACM) de centrale ingang dient te zijn voor *burgers* met vragen op het gebied van oneerlijke handelspraktijken en algemene vragen over fraude en oplichting. De Autoriteit Financiële Markten (AFM) is voor consumenten het aanspreekpunt op het gebied van financiële producten en diensten. Ten aanzien van *bedrijven* is in het NPC besloten tot het starten van een digitaal loket van de overheid waar bedrijven terecht kunnen met vragen op het gebied van fraude en oplichting.²² De minister geeft aan dat het digitale loket algemene informatie over fraude en oplichting zal verschaffen en zal doorverwijzen naar de juiste netwerkpartners, zodat bedrijven op weg worden geholpen en zelf een oordeel kunnen vormen over mogelijke risico's op het gebied van fraude en oplichting.²³

Aan de vormgeving van het digitale loket liggen twee uitgangspunten ten grondslag. Ten eerste is er de wens om geen nieuwe voorziening te treffen die taken uitvoert op die terreinen waar reeds bestaande overheidsorganisaties actief zijn. Ten tweede kan het digitale loket geen advies verstrekken over individuele aanbieders of aanbiedingen.²⁴

Oprichting van een helpdesk voor consumenten

Op 18 mei 2010 wordt de Kamer opnieuw geïnformeerd over het oprichten van een helpdesk financieel-economische criminaliteit.²⁵ Naar aanleiding van de wens van de Kamer is de minister voornemens om een helpdesk op te richten die een centraal meldpunt zal zijn voor *consumenten* met vragen op het gebied van fraude en oplichting.²⁶ Het idee van het oprichten van een digitaal loket voor bedrijven lijkt dus van de baan. Wel merkt de minister op dat ook kleine ondernemers bij de nieuwe helpdesk terecht kunnen.²⁷

De helpdesk zal een frontoffice worden waar consumenten en kleine ondernemers terecht kunnen met vragen over fraude en oplichting.²⁸ 'De meerwaarde van de helpdesk is dat er één laagdrempelige ingang komt waar de consument terecht kan met vragen.' De helpdesk zal algemene kennis en informatie verstrekken over bestaande vormen van fraude en oplichting, met als doel burgers weerbaarder te maken tegen pogingen tot oplichting.²⁹ Het idee is dat door het verschaffen van informatie over de werkwijzen van fraudeurs, een consument fraude of oplichting sneller kan herkennen. Daarnaast krijgt de helpdesk een doorverwijzende functie als het gaat om meldingen en vragen van consumenten die bijvoorbeeld op het werkterrein van de AFM (fraude/oneerlijke handelspraktijken gerelateerd aan financiële producten en

²¹ Kamerstukken II 2009/10, 29 911, nr. 37.

²² Kamerstukken II 2009/10, 29 911, nr. 37, p. 1.

²³ Kamerstukken II 2009/10, 29 911, nr. 37, p. 2.

²⁴ Kamerstukken II 2009/10, 29 911, nr. 37, p. 2.

²⁵ Kamerstukken II 2009/10, 29 911, nr. 41.

²⁶ Tijdens een Algemeen Overleg op 10 februari 2010 hadden enkele Kamerleden hun bedenkingen geuit over het onderscheid dat werd gemaakt tussen burgers en bedrijven (zie Kamerstukken II 2009/10, 29 911, nr. 39).

²⁷ Kamerstukken II 2009/10, 29 911, nr. 41, p.1 en 2.

²⁸ Kamerstukken II 2009/10, 29 911, nr. 41, p.2.

²⁹ Met 'algemene informatie' wordt bedoeld dat informatie wordt gegeven over bijvoorbeeld veel voorkomende fraudevormen of handelwijzen van fraudeurs en geen informatie over individuele aanbiedingen.

diensten) en de ACM (oneerlijke handelspraktijken in het algemeen) liggen. Het meldpunt zal zelf geen meldingen verwerken, maar doorverwijzen naar de daarvoor bestaande instanties, zoals bijvoorbeeld Politie, AFM of de ACM. Daarnaast zal de helpdesk een registratie bijhouden van de aantallen en soorten meldingen.’³⁰

De minister stelt de volgende specifieke randvoorwaarden waar de helpdesk aan dient te voldoen:³¹

- ‘er dient een zodanige infrastructuur te zijn dat fraudemeldingen aan Politie en Openbaar Ministerie kunnen worden doorgegeven;
- binnen het versterkingsprogramma FINEC wordt gekeken hoe het aangifteproces bij Politie en Openbaar Ministerie kan worden verbeterd. Deze ontwikkeling zal ook bij de opzet van het nieuw te vormen meldpunt meegenomen dienen te worden;
- er kan alleen openbare informatie verstrekt worden en geen specifiek advies over financiële producten of oneerlijke handelspraktijken worden gegeven door de helpdesk. Er zal dus geen individuele risico aanduiding worden gegeven door de helpdesk;
- er zullen geen partijen bij de helpdesk betrokken zijn die onder toezicht staan van de AFM of de Consumentenautoriteit;
- er zal in kaart worden gebracht wie de ketenpartners zijn en met deze ketenpartners zullen afspraken worden gemaakt over de afbakening van de front office en de back office. Er wordt vastgelegd waar iedere ketenpartner voor verantwoordelijk is en wanneer er wordt doorverwezen naar de ketenpartner. Dit zal resulteren in samenwerkingsprotocollen.’

Naar aanleiding van het voornemen om een helpdesk op te richten, worden bij twee partijen offertes opgevraagd. De subsidie wordt uiteindelijk toegekend aan SafeCin voor een proefperiode van één jaar. Safecin opent begin 2011 de Fraudehelpdesk.³²

In het gesprek met medewerkers van het ministerie van JenV is aangegeven dat ten tijde van het oprichten van de helpdesk fraude nog niet zo hoog op de politieke agenda stond en er minder aandacht en urgentie was voor het onderwerp dan in de huidige tijd. Er was weinig zicht op fraudevormen en er werd gezocht naar hoe hier meer zicht op kon worden verkregen. Banken en andere organisaties waren nog niet zo alert op fraude als tegenwoordig. Bovendien was fraude waarvan ondernemers slachtoffer werden, mede door internationalisering, een fenomeen dat van karakter veranderde. Burgers en bedrijven werden daarbij, met name door de opkomst van ICT, kwetsbaarder om slachtoffer te worden van fraude. Preventieve maatregelen in de vorm van voorlichting en bewustwording over frauderisico’s werden destijds als noodzakelijk gezien.³³ Daarnaast gaven medewerkers van het ministerie aan dat het merendeel van de randvoorwaarden die door de minister zijn gesteld in een Kamerbrief over georganiseerde criminaliteit,³⁴ niet worden herkend. Eén van de randvoorwaarden is dat er geen specifiek advies over financiële producten of oneerlijke handelspraktijken wordt gegeven door de helpdesk. Hierover wordt opgemerkt dat al snel na het oprichten van de Fraudehelpdesk bleek dat deze randvoorwaarde achterhaald was, omdat het anders erg lastig was om burgers en bedrijven goed te kunnen ondersteunen. Een andere opvallende randvoorwaarde is dat er

³⁰ Kamerstukken II 2009/10, 29 911, nr. 41, p.2.

³¹ Kamerstukken II 2009/10, 29 911, nr. 41, p.2.

³² Frierson e.a. 2012.

³³ Tromp e.a. 2010, p. 3.

³⁴ Kamerstukken II 2009/10, 29 911, nr. 41, p.2.

een zodanige infrastructuur dient te zijn dat fraudemeldingen aan de Politie en het Openbaar Ministerie kunnen worden doorgegeven. Ten aanzien van deze randvoorwaarde kan worden opgemerkt dat het delen van fraudemeldingen die persoonsgegevens van strafrechtelijke aard bevatten, niet zomaar met ketenpartners kunnen worden gedeeld. Hiervoor is een vergunning van de Autoriteit Persoonsgegevens (AP) vereist.

2.3 Veronderstelde doel-middelrelaties en werkzame mechanismen

De reconstructie van de veronderstelde doel-middelrelaties is gemaakt op basis van Kamerstukken. Een aantal veronderstelde doel-middelrelaties en werkzame mechanismen zijn expliciet terug te vinden in de Kamerstukken, andere zijn afgeleid uit impliciete beschrijvingen. De doelenboom is voorgelegd aan medewerkers van het ministerie van JenV. In het gesprek werd aangegeven dat zij zich konden vinden in de geïdentificeerde middelen, doelen en mechanismen. Hoe tot de doelen, mechanismen en middelen is gekomen, is hieronder toegelicht waarbij wordt verwezen naar relevante Kamerstukken waar de doelen, mechanismen en middelen uit zijn afgeleid.

Het eerste doel dat wordt nagestreefd is:

Doel: Burgers en kleine bedrijven weerbaarder maken tegen een poging tot oplichting.

De middelen die worden ingezet om het doel te bereiken zijn:

Middel: Verstrekken van algemene kennis en informatie over bestaande vormen van fraude en oplichting.

Middel: Registreren van aantallen en soorten meldingen.

Het veronderstelde werkzame mechanisme is:

Mechanisme: Door het verstrekken van algemene kennis over fraude, en door het registreren van meldingen kan beter worden gewaarschuwd voor werkwijzen van fraudeurs of vormen van fraude en worden burgers weerbaarder tegen poging tot oplichting. In de doelenboom in figuur 2.1 is dit mechanisme opgenomen als 'verbeteren preventie'.

Het eerste doel 'burgers en kleine bedrijven weerbaarder maken tegen poging tot oplichting' en het mechanisme 'kennis over en herkennen van fraude verbeteren bij burgers' worden min of meer expliciet genoemd door de regering en hebben we daarom overgenomen. Het begrip weerbaarheid wordt in de Kamerstukken niet gedefinieerd. Ook het middel 'verstrekken van algemene kennis en informatie' wordt door de regering benoemd. Het registreren van aantallen en soorten meldingen wordt wel genoemd als taak van de helpdesk, maar niet direct gekoppeld aan het mechanisme om burgers in staat te stellen fraude beter te herkennen.³⁵ Dit mechanisme ligt wel impliciet ten grondslag aan het middel. Door het registreren van meldingen, krijgt de Fraudehelpdesk zicht op voorkomende modus operandi en fraudevormen, en kan er worden gewaarschuwd voor werkwijzen van fraudeurs, wat burgers en kleine bedrijven in staat stelt fraude beter te herkennen.

³⁵ Kamerstukken II 2009/10, 29 911, nr. 41, p.1 en 2.

Het tweede doel dat wordt nagestreefd is:

Doel: Slachtoffers van fraude zo goed mogelijk ondersteunen.

De middelen die worden ingezet om dit doel te bereiken zijn:

Middel: Doorverwijzen van meldingen naar organisaties als de Politie, AFM, de ACM of Slachtofferhulp Nederland.

Middel: Verstrekken van algemene kennis en informatie over bestaande vormen van fraude en oplichting.

Het veronderstelde werkzame mechanisme is:

Mechanisme: Door het doorverwijzen en verstrekken van algemene informatie bij meldingen, vormt de helpdesk één laagdrempelig centraal meldpunt waardoor slachtoffers ondersteund worden.³⁶ In de doelenboom in figuur 2.1 is dit mechanisme opgenomen als 'creëren van één centraal meldpunt'.

Het tweede doel wordt niet expliciet genoemd, maar komt wel een aantal keren terug in de bestudeerde Kamerstukken. Zo is de aanleiding voor het oprichten van een helpdesk mede terug te voeren op een Kamermotie waarin wordt gesteld dat er op dat moment onvoldoende aandacht is voor de schade van slachtoffers van financieel-economische misdaad.³⁷ Ook in 2009 geeft de minister aan dat de bevindingen uit het rapport Slachtofferschap van Fraude, waaruit blijkt dat één op de vijf mensen die te maken hebben gehad met oplichting een hulplijn of helpdesk heeft gemist, worden betrokken bij de verdere uitwerking voor de voorstellen van een helpdesk.³⁸ De middelen die worden ingezet om slachtoffers te ondersteunen zijn het doorverwijzen van meldingen naar andere organisaties en het verstrekken van algemene kennis en informatie over fraude. Deze middelen worden in de Kamerstukken niet expliciet gelinkt aan het doel om slachtoffers te ondersteunen, maar volgen wel impliciet uit de beleidsreconstructie. Ook het werkzame mechanisme wordt niet expliciet gekoppeld aan de doelen of middelen, maar wordt wel benoemd: 'De meerwaarde van de helpdesk is dat er één laagdrempelige ingang komt waar de consument terecht kan met vragen.'³⁹

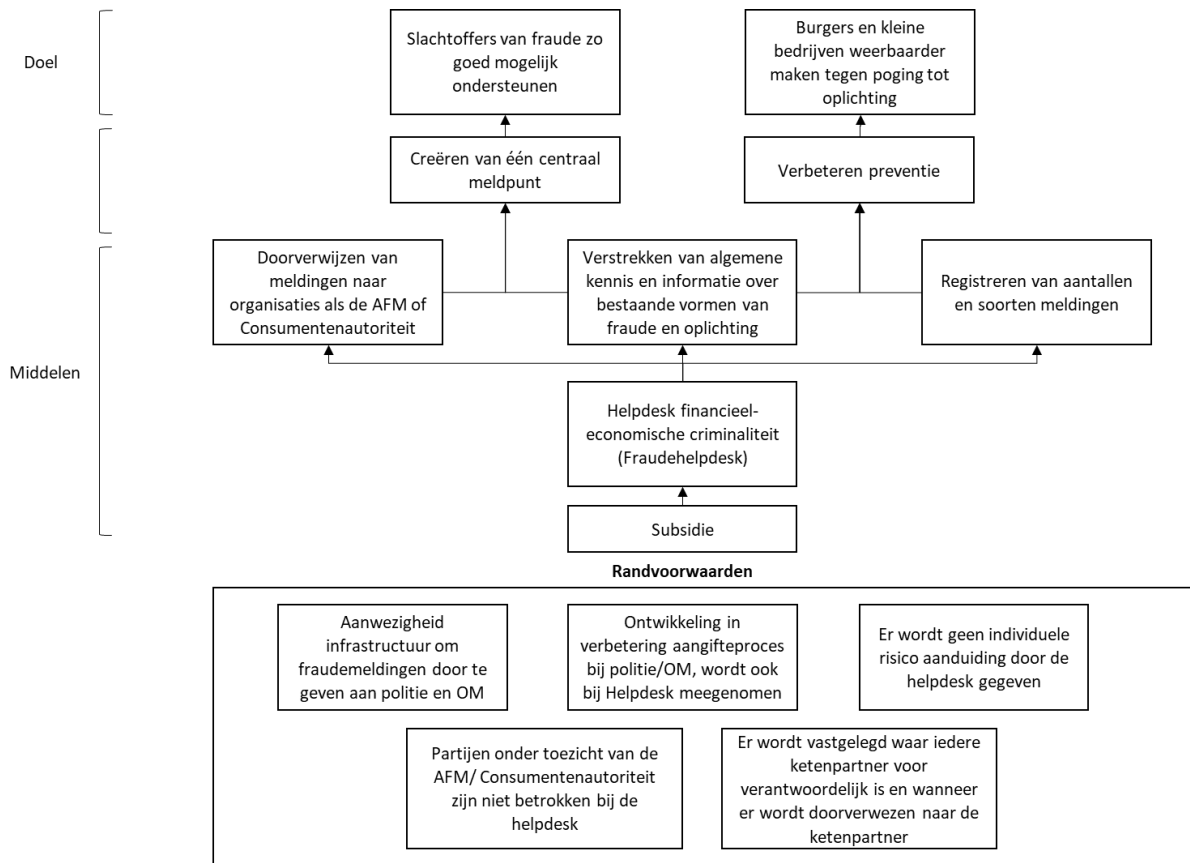
³⁶ Met het verstrekken van algemene informatie wordt in dit rapport bedoeld dat informatie wordt gegeven over bepaalde categorieën van fraude of handelswijzen van fraudeurs. Het gaat bij algemene informatie niet over specifieke zaken.

³⁷ *Kamerstukken II 2007/08*, 31 200 VI, nr. 48 en *Handelingen II 2007/08* nr. 28, p. 2191-2194.

³⁸ *Kamerstukken II 2009/10*, 29 911, nr. 35, p. 1-3.

³⁹ *Kamerstukken II 2009/10*, 29 911, nr. 35, p. 1-3.

FIGUUR 2.1: DOELENBOOM



2.4 Evaluatie van de veronderstelde mechanismen

2.4.1 Literatuuronderzoek veronderstelde mechanismen

In de voorgaande paragraaf zijn de doel-middelrelaties en de onderliggende mechanismen beschreven. De beleidstheorie ziet er op papier aannemelijk en consistent uit, maar empirische onderbouwing op basis van bijvoorbeeld ervaringen met andere meldpunten in een andere context ontbreekt. In deze paragraaf wordt met behulp van een literatuuronderzoek nagegaan of de veronderstelde werkzame mechanismen kunnen worden onderbouwd met bevindingen uit de literatuur.

Verbeteren preventie

De veronderstelling die aan de beleidstheorie ten grondslag ligt is dat het delen van kennis en informatie over bestaande vormen van fraude en oplichting burgers en kleine bedrijven weerbaarder maakt tegen fraude. Deze kennis en informatie wordt onder andere opgedaan door het registreren van aantallen en soorten meldingen, zodat bekend is welke fraudevormen op welk moment het meest voorkomen. Het delen van kennis en informatie kan onder andere worden gedaan door middel van campagnes.

In de literatuur bestaat discussie over de effectiviteit van het delen van kennis en informatie ter bestrijding van fraude en oplichting. Zo vinden Bada e.a. in hun literatuuronderzoek naar

campagnes voor cybersecurity zowel succesvolle als onsuccesvolle overheidscampagnes. De onderzoekers hebben onderzocht waarom overheidscampagnes falen en aan de hand van welke voorwaarden deze campagnes succesvol kunnen zijn. Volgens hen worden campagnes ingezet met het doel het gedrag van burgers te veranderen en daarmee online gedrag veiliger te maken.⁴⁰ Zij concluderen dat kennis en bekendheid van fraudetypes noodzakelijk zijn om fraude te voorkomen, maar dat deze kennis alleen onvoldoende is om gedragsverandering bij burgers te bewerkstelligen. Factoren die kunnen bijdragen aan het versterken van kennis over veiligheid is dat de informatie: gericht, bruikbaar en uitvoerbaar is voor burgers en feedback moet geven op het gedrag van burgers.⁴¹

Ook in andere literatuur komt naar voren dat het effect van een interventie afhankelijk is van verschillende factoren.⁴² Zo blijkt uit de meta-analyse van Bullée en Junger dat een interventie het aantal slachtoffers van online fraude kan verminderen, maar dat het effect van de interventie sterk afhankelijk is van de soort interventie.⁴³ Allereerst blijkt een interventie die op een specifiek onderdeel gericht is, zoals waar een burger op kan letten in een URL, effectiever is dan een algemeen gerichte interventie die zich op meerdere onderwerpen tegelijkertijd richt.⁴⁴ Daarnaast blijkt een interactieve en redelijk intensieve interventie (bijvoorbeeld door middel van spel of een les) effectiever te zijn. Voor een optimale interventie kan gedacht worden aan een training waarin deelnemers in een spelvorm een specifieke vorm van misleiding of oplichting leren herkennen.⁴⁵ Voor een interventie is ook de timing van de gedragsinterventie cruciaal. Interventies (zoals overheidscampagnes) zijn in de beleving van deelnemers aan het onderzoek niet effectief, omdat die vaak worden ontvangen op momenten dat dit irrelevant is (bijvoorbeeld via de radio tijdens het rijden in een auto). Advies over veilig cybergedrag is leerzamer en wordt sneller overgenomen, wanneer deze gegeven wordt op het moment dat de onveilige gedraging (bijna) plaatsvindt.⁴⁶

Van der Kleij e.a. dragen aan dat een toename in kennis over cybercrime wellicht een negatief gevolg heeft voor het online gedrag van burgers. Zo blijkt uit hun onderzoek dat burgers hun online gedrag vaak veiliger inschatten dan deze daadwerkelijk is.⁴⁷ Ook blijkt dat de respondenten niet op verschillende domeinen hetzelfde gedrag vertonen. Zo kiezen zij soms wel voor een sterk wachtwoord, maar downloaden zij alsnog onbekende software. Van der Kleij e.a. geven hiervoor als mogelijke verklaring dat door een toename in kennis men vermoedt zich in een veilige omgeving te bevinden, waardoor meer risico's in andere domeinen worden genomen.⁴⁸ Volgens Van der Kleij e.a. overschatten overheden dan ook vaak de waarde van kennisdeling. Vaak worden bewustmakingscampagnes gelanceerd vanuit de veronderstelling dat kennis over online cybersecurity ontbreekt, terwijl in feite andere factoren (zoals een slecht ontworpen securitydesign) de oorzaak zijn van onveilig gedrag.⁴⁹

⁴⁰ Bada e.a. 2015, p. 119.

⁴¹ Bada e.a. 2015, p.127.

⁴² Bullée en Junger, *Information and Computer Security 2020*; Van 't Hoff-de Goede e.a. 2019, p. 123; Jansen e.a. 2019, p. 59.

⁴³ Bullée en Junger, *Information and Computer Security 2020*.

⁴⁴ Bullée en Junger, *Information and Computer Security 2020*; Jansen e.a. 2019, p. 59.

⁴⁵ Bullée en Junger, *Information and Computer Security 2020*.

⁴⁶ Van 't Hoff-de Goede e.a. 2019, p. 123.

⁴⁷ Van der Kleij e.a. 2020, p.119.

⁴⁸ Van der Kleij e.a. 2020, p.124.

⁴⁹ Van der Kleij, e.a. 2020 p. 124.

De effectiviteit van het overdragen van kennis en van campagnes op het voorkomen van slachtofferschap van online fraude wordt dus verschillend beoordeeld in de literatuur en is afhankelijk van verschillende factoren. Uit verschillende onderzoeken blijkt dat het slechts delen van kennis over fraude en oplichting niet of slechts beperkt effectief is in het veranderen van het online gedrag van mensen. De effectiviteit wordt vergroot door een interventie op het juiste moment plaats te laten vinden, interactief te maken en burgers te voorzien van feedback. Het delen van kennis over online fraude is in deze studies wel een voorwaarde voor het slagen van de interventies. Ook uit gesprekken met experts op het gebied van fraude komt naar voren dat het verstrekken van algemene kennis en informatie van belang is, maar dat het verstrekken van algemene informatie alleen waarschijnlijk onvoldoende is om burgers weerbaarder te maken tegen fraude en oplichting.

Een centraal meldpunt

Het tweede doel is dat slachtoffers van fraude zo goed mogelijk ondersteund worden. De veronderstelling was dat door één laagdrempelig centraal meldpunt te creëren dat informatie kan verstrekken over fraude, en slachtoffers kan doorverwijzen naar de juiste partij, burgers beter worden ondersteund. Uit onderzoek blijkt dat de gevolgen die slachtoffers ervaren van zowel online als offline fraude gelijk zijn. Slachtoffers ervaren voornamelijk financiële gevolgen, zijn indirect veel tijd kwijt aan het herstellen van de fraude en ervaren in sommige gevallen psychische gevolgen.⁵⁰ Wel blijkt dat de impact van de gevolgen van online fraude, bijvoorbeeld financiële schade, groter zijn dan die van offline fraude.⁵¹

Slachtoffers van online delicten hebben met name behoefte aan het stoppen van slachtofferschap, straf en vergelding en willen anderen helpen.⁵² De belangrijkste emotionele behoeften zijn behoeftes aan eerste opvang, erkenning, zorg en steun.⁵³ De Politie wordt door slachtoffers aangewezen als verantwoordelijke actor voor onderkenning van hun behoeften. De Politie is echter niet altijd de geschikte partij die in staat is aan de behoeften van slachtoffers tegemoet te komen.⁵⁴ Uit Australisch onderzoek van Cross blijkt dat slachtoffers die moeite hebben om de juiste instantie te vinden zich vaak boos, gefrustreerd en teleurgesteld voelen.⁵⁵ Ze geven aan het gevoel te hebben van het kastje naar de muur te worden gestuurd en daarbij iedere keer opnieuw hun verhaal moeten doen.⁵⁶ Het gevoel 'van het kastje naar de muur te worden gestuurd' kan leiden tot een toename van stress bij slachtoffers.⁵⁷ Voor veel slachtoffers is het dan ook wenselijk dat zij een melding kunnen doen en hierop duidelijke informatie krijgen over wat er kan worden gedaan in hun situatie en wat zij mogen verwachten in het proces.⁵⁸

Ook zijn er slachtoffers die geen fraude melden. Een aantal van deze slachtoffers geeft aan niet te weten waar het met de melding naartoe moet. Anderen denken dat ze daarmee het probleem niet oplossen, schamen zich te diep of bedenken het niet om een melding te doen.⁵⁹

⁵⁰ Leukfeldt e.a. 2018, p. 114.

⁵¹ Leukfeldt e.a. 2018, p. 114-115.

⁵² Leukfeldt e.a. 2018, p. 88.

⁵³ Leukfeldt e.a. 2018, p. 111.

⁵⁴ Leukfeldt e.a. 2018, p. 94, 120-121.

⁵⁵ Cross 2018, p. 5; Cross e.a. 2016, p. 43.

⁵⁶ Cross 2018, p. 5; Cross e.a. 2016, p. 46.

⁵⁷ Cross, 2016, p. 19.

⁵⁸ Cross e.a. 2016 p. 56; Leukfeldt e.a. 2018, p. 100.

⁵⁹ Cross e.a. 2016, p. 59.

Als antwoord op wat hen had geholpen wel te melden geven slachtoffers aan dat informatie over hoe en waar ze kunnen melden behulpzaam zou zijn.⁶⁰

Slachtoffers van fraude weten dus vaak niet bij welke organisatie zij hun melding kwijt kunnen en wat zij vervolgens mogen verwachten. Uit onderzoek van Button e.a. naar de behoeften en ervaringen van slachtoffers blijkt dan ook dat slachtoffers voornamelijk behoefte hebben aan een 'single point of contact' waar zij hun melding over fraude konden doen en waar hen wordt verteld wat zij in het proces kunnen verwachten.⁶¹ Een laagdrempelig centraal meldpunt voor slachtoffers van fraude lijkt daarmee aan te sluiten op de wens van slachtoffers van fraude.

2.5 Conclusie

In dit hoofdstuk is de beleidstheorie van het opzetten van een helpdesk in kaart gebracht en is gekeken of de veronderstellingen die aan deze beleidstheorie ten grondslag liggen, door de literatuur worden ondersteund.

De aanleiding voor het oprichten van een helpdesk is mede terug te voeren op een Kamermotie waarin werd gesteld dat er onvoldoende aandacht was voor de schade van slachtoffers van financieel-economische misdaad. Daarnaast wees onderzoek onder burgers uit dat er behoefte was aan een helpdesk waar mensen informatie konden krijgen over oplichting.⁶² Een helpdesk zou burgers en kleine bedrijven weerbaarder moeten maken tegen fraude en zou daarnaast slachtoffers van fraude moeten ondersteunen. De helpdesk zou dat moeten doen door zich bezig te houden met het registreren van aantallen en soorten meldingen, slachtoffers naar de juiste instantie door te verwijzen en algemene kennis en informatie te verstrekken over fraude.

Op basis van de literatuur kan een aantal kritische kanttekeningen worden gemaakt bij de onderbouwing van de theorie dat door het verstrekken van algemene kennis en informatie burgers weerbaarder kunnen worden gemaakt tegen fraude. Bada e.a. concluderen in hun onderzoek naar bewustzijns campagnes over cyber security dat kennis en bekendheid van fraudetypes noodzakelijk zijn om slachtofferschap tegen te gaan, maar dat alleen kennis onvoldoende is om gedragsverandering bij burgers te bewerkstelligen.⁶³ Naast campagnes kunnen ook andere interventies worden ingezet voor het verstrekken van algemene kennis en informatie. Uit de conclusies van een meta-analyse van studies naar de effectiviteit van interventies op het gebied van digitale fraude en misleiding blijkt dat er zeker interventies zijn die helpen om de effecten van menselijke misleiding te beperken. De auteurs van deze studie geven wel aan dat de ideale interventie interactief is, bestaat uit contact met de gebruiker, een specifieke focus heeft, een of twee onderwerpen behandelt en relatief intensief is. In het onderzoek van Van 't Hoff-de Goede e.a. geven experts aan dat de timing van gedragsinterventies cruciaal is.⁶⁴ Randvoorwaarden over de vorm waarin algemene informatie zou moeten worden verstrekt door de helpdesk, lijken niet te zijn gesteld.

⁶⁰ Cross e.a. 2016, p. 59.

⁶¹ Button e.a. 2009, p. 68, 78.

⁶² Oudejans en Vis, 2008.

⁶³ Bada e.a. 2015, p.127.

⁶⁴ Van 't Hoff-de Goede e.a. 2019, p. 123.

Ten aanzien van het mechanisme dat een centraal meldpunt slachtoffers van fraude zou moeten ondersteunen is in de literatuur wel onderbouwing gevonden. Het onderzoek van Button e.a. ondersteunt de gedachte dat slachtoffers van fraude behoefte hebben aan een centraal meldpunt, waarbij zij informatie krijgen over wat hun mogelijkheden zijn en hoe hun melding wordt opgepakt.⁶⁵ Belangrijk is dat slachtoffers door het meldpunt in hun behoeften worden ondersteund. Deze behoeften zien met name op erkenning en steun, eenduidige informatie over hoe hun melding wordt opgepakt en wat zij in de rest van de procedure kunnen verwachten. Daarbij is het voor hen relevant dat zij niet vaak hun verhaal aan verschillende instanties hoeven te doen.⁶⁶

⁶⁵ Button e.a. 2009, p. 68, 78.

⁶⁶ Cross e.a. 2016, p. 56; Leukfeldt e.a. 2018, p. 100.

3 Organisatie, financiën en activiteiten

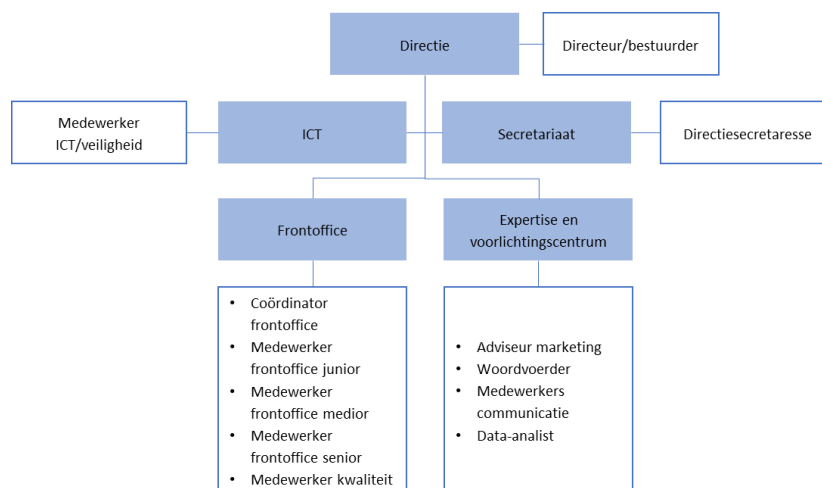
3.1 Inleiding

Dit hoofdstuk gaat in op de ontwikkeling in de financiering van de Fraudehelpdesk en de geleverde diensten (deelvraag 3 en 6). Daarnaast wordt ook aandacht besteed aan de subsidievoorwaarden (deelvraag 4) en het signaleren van fraudevormen door de Fraudehelpdesk (deelvraag 7a). In paragraaf 3.2 wordt eerst een korte schets van de inrichting van de organisatie gegeven. Paragraaf 3.3 gaat in op de ontwikkelingen in de financiering van de Fraudehelpdesk. In paragraaf 3.4 worden de diensten en activiteiten besproken. Paragraaf 3.5 spreekt overige ontwikkelingen rondom de dienstverlening. In paragraaf 3.6 is ten slotte een conclusie opgenomen (deelvraag 5).

3.2 Inrichting organisatie

In figuur 3.1 is het organogram van de Fraudehelpdesk weergegeven.

FIGUUR 3.1: ORGANOGRAM FRAUDEHELPDESK



Directie en staf

De dagelijkse leiding en aansturing van de organisatie ligt bij de directeur van de Fraudehelpdesk. Sinds de oprichting van de Fraudehelpdesk heeft de organisatie drie directeuren gehad. Halverwege 2019 is de tweede directeur van de Fraudehelpdesk aangetreden, en halverwege 2023 (ten tijde van dit onderzoek) is een interim-directeur aangetreden. De directeur is eindverantwoordelijk voor de Fraudehelpdesk en legt vanuit die rol verantwoording af aan de Raad van Toezicht. Daarnaast onderhoudt de directeur contacten met ketenpartners. De organisatie wordt ondersteund door een medewerker ICT/veiligheid en een directiesecretaresse.

Frontoffice

De medewerkers van de frontoffice houden zich bezig met alle meldingen die telefonisch en via de digitale formulieren op de website binnenkomen. De frontoffice is verantwoordelijk voor het telefonisch en digitaal te woord staan van melders van fraude, het vaststellen van modus operandi en gevolgschade. Daarnaast zijn de medewerkers verantwoordelijk voor het adviseren van melders en het doorverwijzen van slachtoffers naar de juiste partijen of instanties die ze verder kunnen helpen. Ten slotte registreren, categoriseren en bewaken de medewerkers de fraudegevallen in de systemen. De frontoffice wordt aangestuurd door een coördinator. Om de kwaliteit van de frontoffice te bewaken is er een kwaliteitsmedewerker.

De frontoffice houdt zich ook bezig met de dienst 'valse e-mailcheck'. Via een speciaal e-mailadres van de Fraudehelpdesk kunnen melders een vermoedelijke valse e-mail doorsturen. Het systeem beoordeelt of de e-mail vals is of niet, waarna een melder een automatisch bericht ontvangt over de mail en wat de melder moet doen als bijvoorbeeld een link in de mail is aangeklikt. Bij minimaal vijf keer dezelfde valse e-mail, wordt er een geanonimiseerde versie van de e-mail op de website van de Fraudehelpdesk geplaatst.

Expertise- en voorlichtingscentrum

De medewerkers van het expertise- en voorlichtingscentrum houden zich voornamelijk bezig met de communicatie en marketing van de Fraudehelpdesk en met voorlichting. Er wordt jaarlijks een communicatieplan opgesteld, waarin de plannen en activiteiten op het gebied van communicatie zijn opgenomen. Daarnaast houden de medewerkers zich bezig met het bedenken, opzetten en uitvoeren van campagnes die al dan niet in samenwerking met ketenpartners kunnen worden opgezet. Met name in de afgelopen jaren wordt volgens de gesprekspartners meer ingezet op het gezamenlijk met ketenpartners voeren van campagnes. Ook houdt de afdeling zich bezig met de vindbaarheid van de website en plaatst men waarschuwingsberichten op de website.

Organisatieontwikkeling

Het aantal FTE is in de afgelopen jaren toegenomen van 9 fte in 2012 tot 15 fte in 2022. Uit de interviews komt naar voren dat de organisatie in de afgelopen jaren verder geprofessionaliseerd is. Zo is er in 2021 door een extern bureau in opdracht van de Fraudehelpdesk een ontwikkelagenda opgesteld voor de verdere professionalisering in de komende jaren. De ontwikkelagenda is opgesteld om helderheid te bieden over de fasering en planning die nodig zijn om een volgende stap te maken in het positioneren en functioneren van de organisatie.⁶⁷ Daarnaast is in de afgelopen jaren een organogram en een functiehuis opgesteld.

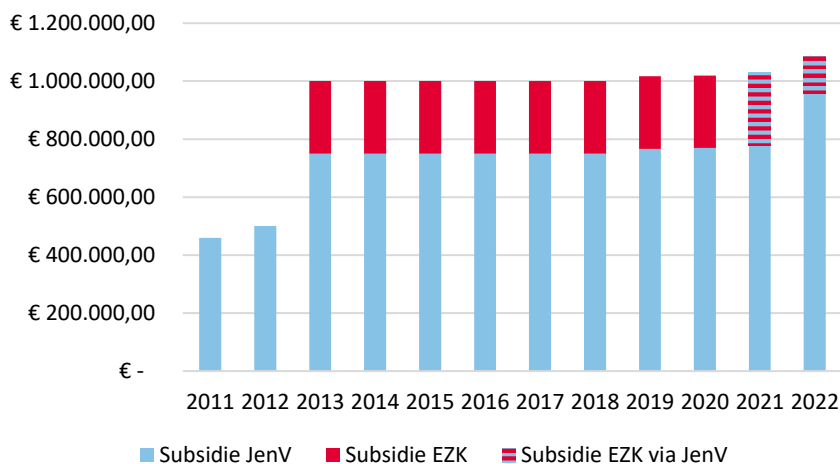
⁶⁷ Ontwikkelagenda AEF, p.4.

3.3 Financiën

De Fraudehelpdesk wordt sinds de oprichting in 2011 (grotendeels) gefinancierd door het ministerie van JenV. Voor het eerste jaar 2011 ontving de Fraudehelpdesk € 460.066 en voor 2012 € 500.000.⁶⁸ Vanaf 2013 heeft het ministerie de subsidie verhoogd tot € 750.000 per jaar en wordt de Fraudehelpdesk ook door het ministerie van EZK gesubsidieerd. Aanleiding voor de subsidiëring van het ministerie van EZK was een aangenomen Tweede Kamermotie waarin de regering werd verzocht de begroting van de Fraudehelpdesk voor het openstaande deel (€ 250.000) te dekken.⁶⁹ In november 2019, geeft het ministerie van EZK aan hun subsidiedeel te willen afbouwen. Gedurende twee jaar zou het ministerie van EZK een begrotingsoverheveling doen aan het ministerie van JenV. In 2021 betaalde het ministerie van EZK nog het volledige subsidiebedrag van € 250.000 en voor 2022 betrof dit € 125.000.⁷⁰

In figuur 3.2 is de ontwikkeling van de inkomsten van de Fraudehelpdesk in de periode 2011 tot 2022 weergegeven.

FIGUUR 3.2: ONTWIKKELINGEN INKOMSTEN FRAUDEHELPDESK⁷¹



In 2016 is er binnen de Fraudehelpdesk een reorganisatie ingezet, die er toe heeft geleid dat de begroting vanaf 2017 uitsluitend wordt gedekt door de subsidie van het Rijk.⁷² Tot 2017 zorgden ook de inkomsten uit de private sector voor een deel van de financiering. Er wordt vanaf 2017 onderscheid gemaakt tussen de gesubsidieerde publieke taken van de Fraudehelpdesk en de private activiteiten van SafeCin. Uit het jaarverslag 2016 blijkt dat voor deze ingezette beleidslijn overleg met de departementen heeft plaatsgevonden.⁷³ Particuliere baten die de Fraudehelpdesk ophaalt uit het bedrijfsleven en onder meer afkomstig zijn uit deelnemersbijdragen voor ondersteuning bij acquisitiefraude zijn niet meegenomen in de grafiek, omdat dit onderzoek zich richt op de publieke middelen en activiteiten.

⁶⁸ Financieel verslag 2012.

⁶⁹ Kamerstukken 33 400-XIII, nr. 45.

⁷⁰ Brief van de minister van Justitie en Veiligheid van 24 november 2020, 83083700.

⁷¹ Deze cijfers zijn afkomstig uit de jaarverslagen van de Fraudehelpdesk. Subsidies of andere bijdragen voor speciale projecten zijn hierin niet meegenomen. De overige inkomsten bestaan, afhankelijk van het jaar, uit: deelnemersbijdragen, branchelidmaatschappen, juridische ondersteuning en overige bijdragen, sponsoring en managementfee van Stichting Mores, subsidie van het NPC en subsidie van het CCV.

⁷² Jaarverslag 2016, p. 8.

⁷³ Jaarverslag 2016, p. 8.

In 2018 heeft de Fraudehelpdesk de minister van JenV gevraagd de jaarlijkse subsidie te verhogen en een meerjarige financiering te verstrekken. Reden hiervoor was ten eerste om ruimte voor groei van de salariëring van de medewerkers in loondienst te creëren en ten tweede om het budget voor preventie en voorlichting te verhogen. De minister stemde in met verhoging van de subsidie in 2019 in verband met de loonbijstelling. Toename van de meerjarige financiering was binnen de huidige financiële kaders niet mogelijk volgens de minister.⁷⁴

Uit de jaarverslagen van de Fraudehelpdesk komt naar voren dat het bestuur van mening is dat de continuïteit van de organisatie onder druk staat, omdat de verstrekking van de subsidie door de ministeries ieder jaar weer onzeker is.⁷⁵ Een meerjarig budget zou volgens de Fraudehelpdesk meer structuur aanbrengen om de organisatie en activiteiten nog beter vorm te geven en toekomstbestendig uit te voeren.⁷⁶ Tegelijkertijd probeert de Fraudehelpdesk de private activiteiten uit te bouwen, met als doel financieel onafhankelijker te worden.⁷⁷

Uit het jaarverslag van 2022 komt naar voren dat 2022 financieel gezien een lastig en onzeker jaar was voor de Fraudehelpdesk. Aanvankelijk werd de subsidie voor 2022 verlaagd en moesten bezuinigingsmaatregelen worden getroffen. Deze maatregelen hielden in dat werd ingezet op de basisdienstverlening en dat de Fraudehelpdesk niet in staat was eigenstandige voorlichtingscampagnes te ontwikkelen. In 2022 is alsnog het volledige subsidiebedrag van € 1.084.168 toegekend.⁷⁸ Voor 2023 is vooralsnog eenzelfde bedrag toegekend als voor 2022. Het ministerie acht het van belang dat de Fraudehelpdesk de meldpuntfunctie als basisvoorziening, ook in 2023, zo goed mogelijk in stand houdt.⁷⁹

De Fraudehelpdesk geeft aan ambities te hebben om het experticeentrum op het gebied van fraude (verder) te ontwikkelen, zich te richten op toename van het aantal meldingen, en wil de analyse van data een vaste plek geven. Met de huidige financiële middelen en beperkte capaciteit is het lastig om al deze onderwerpen op te pakken. Hiervoor zullen professionals moeten worden aangetrokken die gespecialiseerd zijn op bepaalde terreinen van fraude.⁸⁰

3.3.1 Subsidievoorwaarden

In 2010 stelde het ministerie van JenV 23 subsidievoorwaarden voor het oprichten van een helpdesk. De subsidievoorwaarden zijn opgenomen in bijlage 8. Uit de evaluatie van de Fraudehelpdesk die in 2012 is uitgevoerd kwam naar voren dat SafeCin aan het merendeel van de formele subsidievoorwaarden voldeed. Ook constateerden de onderzoekers dat er voldoende aanwijzingen waren dat de Fraudehelpdesk de subsidie van € 500.000 doelmatig had besteed. Daarnaast zou de Fraudehelpdesk zich tot een centraal punt voor burgers en bedrijven met vragen over fraude ontwikkelen. Wel was volgens de onderzoekers onduidelijk wat het effect van de Fraudehelpdesk was op het voorkomen van fraude tegen burgers en bedrijven. Enerzijds was een positieve aanwijzing dat het merendeel van de burgers en bedrijven tevreden was over de inhoudelijke afhandeling van vragen door de Fraudehelpdesk. Ook geeft het

⁷⁴ Brief van de minister van Justitie en Veiligheid van 16 november 2018.

⁷⁵ Zie bijvoorbeeld jaarverslag 2018, p. 13 en jaarverslag 2019, p. 16.

⁷⁶ Jaarverslag 2020, p. 17.

⁷⁷ Jaarverslag 2019, p. 16 en 17.

⁷⁸ Wijziging subsidiebesluit 2022, brief van 28 november 2022.

⁷⁹ Subsidietoekenning 2023, 26 januari 2023.

⁸⁰ Jaarverslag 2020, p. 17.

merendeel van de burgers aan te zijn doorverwezen naar de juiste organisatie. Anderzijds konden volgens de onderzoekers meldingen die naar de Politie werden doorverwezen vaak niet worden opgepakt, doordat de politieorganisatie is ingericht op het verwerken van aangiften.

Uit de subsidiebeschikkingen blijkt dat de 23 subsidievoorwaarden die het ministerie van JenV in 2010 heeft gesteld sinds 2021 niet meer van toepassing zijn. Gesprekspartners bevestigen dat de afgelopen jaren niet meer wordt getoetst aan de subsidievoorwaarden zoals die in 2010 zijn opgesteld. Gesprekspartners geven aan dat het wijzigen van de subsidievoorwaarden te maken heeft met het aanpassen van de subsidieregelgevingssystematiek binnen het ministerie van JenV. Doel daarvan was het bevorderen van de eenheid in het subsidierecht. Dit uniforme kader voor subsidies van het ministerie van JenV is sinds 1 juli 2022 met de Kaderwet overige JenV-subsidies in werking getreden. De subsidievoorwaarden zijn teruggebracht tot een aantal meer algemene voorwaarden, zoals dat iedere twee maanden afstemming moet plaatsvinden met de subsidievertrekker over de activiteiten en ontwikkelingen met het oog op de volgende subsidieaanvraag en dat tijdig melding moet worden gemaakt van eventuele wijzigingen in de activiteiten of de begroting.

Het ministerie van JenV verstrekt subsidie. In ruil daarvoor verwacht het ministerie dat de Fraudehelpdesk slachtoffers ondersteunt en inzet op preventie. Preventie is namelijk een van de belangrijkste pijlers van het Nederlandse fraudebeleid. Uit de gesprekken komt verder naar voren dat er beleidsinhoudelijk weinig afstemming bestaat met het ministerie van JenV. Zo zijn er bijvoorbeeld geen voorwaarden gesteld aan het rapporteren over fraudegevallen en schadebedragen aan het ministerie en wordt er in beperkte mate doorgesproken over trends en ontwikkelingen. Het ministerie van JenV geeft aan dat het passend is om in de toekomst meer vraaggestuurd te gaan samenwerken vanuit een meerjarige beleidsvisie. In de subsidiebeschikking van 2023 is aangegeven dat er behoefte is aan de ontwikkeling van een meerjarige beleidsvisie voor de aanpak van online fraude, waarvan de positie en taken van de Fraudehelpdesk als ook de integrale aanpak van online fraude deel van uitmaken.⁸¹

Programma Integrale aanpak online fraude

Uit een onderzoek van de Universiteit van Twente uit 2022 blijkt dat het aantal slachtoffers van online fraude stijgt.⁸² Naast financiële schade voor burgers als in het bedrijfsleven, kan online fraude ook emotionele of psychische schade veroorzaken. Het is volgens de minister van JenV van groot belang om met brede preventie en gerichte repressie een kentering aan te brengen in deze ontwikkeling. Uit gesprekken die het ministerie met stakeholders heeft gevoerd, kwam naar voren dat er behoefte blijkt aan intensievere samenwerking in de bestrijding van online fraude vanuit een gezamenlijke visie. Hiertoe is het programma integrale aanpak van online fraude ontwikkeld.⁸³ De integrale aanpak is een samenwerking waarin betrokken partners daartoe acties met elkaar afspreken om in hun eigen aanpak effectiever te zijn.⁸⁴ De zes thema's uit het actieplan zijn: zicht op fraude, gegevensdeling, (technische) barrières en interventies, opvolging Politie en Openbaar Ministerie, weerbaarheid/preventie en hulp aan slachtoffers. Naast een integrale aanpak online fraude is er vanuit het ministerie in 2018 ook een integrale aanpak cybercrime geïntroduceerd.

⁸¹ Subsidietoekenning, 26 januari 2023.

⁸² Junger e.a. 2022.

⁸³ Brief over de Integrale aanpak online fraude van 8 juli 2022.

⁸⁴ Actieplan integrale aanpak online fraude, p. 3.

Hoewel de subsidievoorwaarden die in 2010 zijn gesteld niet meer van toepassing zijn, is in het kader van dit onderzoek nagegaan in hoeverre aan de voorwaarden wordt voldaan. De subsidievoorwaarden richten zich met name op de werking en inrichting van de Fraudehelpdesk. Zo dient de helpdesk als frontoffice informatie over bestaande vormen van fraude en oplichting te verstrekken, maar ook slachtoffers en melders van fraude en oplichting te helpen en door te verwijzen naar de juiste instantie. Uit bijlage 8 blijkt dat de Fraudehelpdesk aan twee voorwaarden niet volledig voldoet. Zo is een van de voorwaarden dat continuïteit en capaciteit gegarandeerd zijn op werkdagen tussen 9.00 en 17.00 uur. Hoewel er wel 24/7 digitale meldingen kunnen worden gedaan, is de helpdesk op woensdagochtend (in verband met interne overleggen) gesloten en sluit de helpdesk iedere middag om 15.00 uur. Een andere voorwaarde is dat er een reactietijd dient te zijn op schriftelijke vragen van twee dagen. Uit het vragenlijstonderzoek (zie paragraaf 5.3.3) blijkt dat 43 procent van de respondenten binnen twee dagen een reactie heeft gehad, maar 44 procent binnen een week of langer dan een week.

Andere subsidievoorwaarden hebben betrekking op de ervaring en expertise van medewerkers van de Fraudehelpdesk, financiën en rapportage en de omvang en contacten van netwerkpartners. Aan deze voorwaarden wordt, zoals ook reeds in de evaluatie van 2012 werd geconstateerd, (nog) voldaan.⁸⁵

3.4 Activiteiten

In deze paragraaf wordt stilgestaan bij de ontwikkeling van de geleverde diensten van de Fraudehelpdesk sinds 2012. De basisdiensten van de Fraudehelpdesk bestaan uit het registreren van fraudemeldingen, het doorverwijzen van melders naar de instanties die hem of haar verder kunnen helpen, en het verstrekken van algemene informatie.

3.4.1 Registratie van fraudemeldingen

De Fraudehelpdesk registreert meldingen die binnenkomen. Op basis van deze meldingen worden sinds de beginperiode van de Fraudehelpdesk rapportages opgesteld voor het ministerie van JenV, het ministerie van EZK, het OM en de Politie. Tot medio 2022 werden deze periodieke rapportages maandelijks opgesteld. In 2022 is de Fraudehelpdesk in afstemming met het ministerie van JenV overgestapt op kwartaalrapportages. Ook de inhoud van de rapportages is sindsdien aangepast. Voorheen was dit voornamelijk een getalsmatige rapportage van gemelde fraudevormen, maar sinds 2022 is dit uitgebreid met (vroegtijdige) duiding van gesignaleerde ontwikkelingen op een meer gedetailleerd niveau.⁸⁶ Medio 2022 is de Fraudehelpdesk gestart met het opstellen van een maandelijkse nieuwsbrief, de zogenoemde Maandmonitor, die aan een bredere doelgroep wordt toegestuurd. Maandelijks ontvangen, het ministerie van JenV, ketenpartners en andere geïnteresseerden een nieuwsbrief waarin

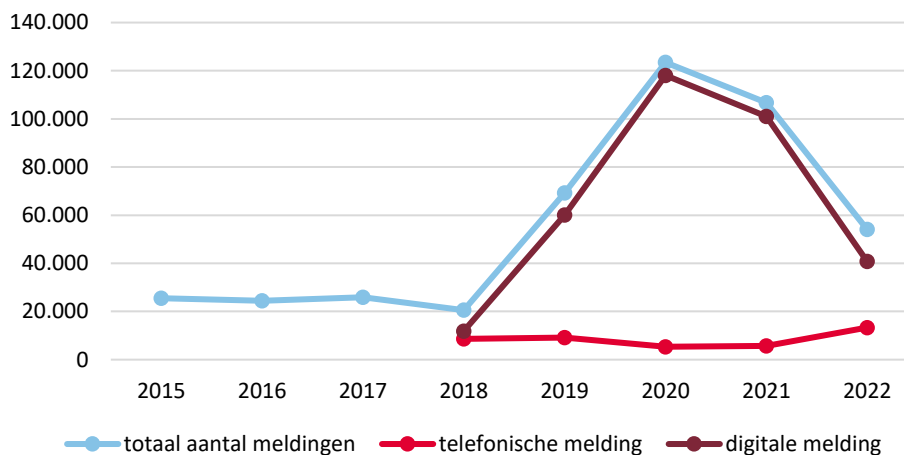
⁸⁵ Uit bijlage 8 blijkt dat we niet voor alle voorwaarden konden nagaan of daaraan is voldaan (zoals dat het voorstel een plan diende te bevatten om de netwerkpartners in beeld te brengen), omdat we daarover geen informatie hebben ontvangen. Uit de evaluatie uit 2012 blijkt dat hier wel aan is voldaan. Ook zijn enkele voorwaarden niet meer relevant. Het gaat om de voorwaarde dat er iedere twee maanden een netwerkoeverleg dient te zijn (hiervan was eerder aangegeven dat daar vanaf werd gezien) en dat verantwoording wordt afgelegd over de gestelde subsidievoorwaarden. Aangezien de voorwaarden niet meer van toepassing zijn is ook deze voorwaarde niet relevant.

⁸⁶ Jaarverslag 2022, p. 6.

de opvallendste trends vanuit de frauderegistraties en andere relevante onderwerpen zijn beschreven.

In figuur 3.3 is het jaarlijks aantal fraudemeldingen dat bij de Fraudehelpdesk wordt gedaan weergegeven. Fraudemeldingen komen via drie wegen bij de Fraudehelpdesk binnen: het call-center, het digitale meldformulier of de valse-e-mail-check (doorgestuurde verdachte e-mails). Sinds 2018 wordt het totaal aantal meldingen bij de Fraudehelpdesk uitgesplitst per kanaal: telefonische melding of digitale melding.

FIGUUR 3.3: TOTAAL AANTAL MELDINGEN⁸⁷



De toename van het aantal digitale meldingen in 2019 ten opzichte van 2018 kan volgens de Fraudehelpdesk worden verklaard door een nieuwe website die veel gebruiksvriendelijker is. De nieuwe website zou gemakkelijker zijn in het gebruik als deze wordt geraadpleegd via een tablet of mobiele telefoon.⁸⁸ Ook in 2020 steeg het totaal aantal meldingen fors ten opzichte van 2019. De oorzaak hiervoor is volgens de Fraudehelpdesk de introductie van de verkorte melding: de mogelijkheid om snel en zonder uitgebreide informatie de ontvangst van verdachte berichten te kunnen melden. Hierdoor konden ook berichten die per sms of WhatsApp waren ontvangen, worden gemeld.⁸⁹ Aanleiding voor het introduceren van het verkorte meldformulier was het afwijzen van de eerste vergunningaanvraag om persoonsgegevens van strafrechtelijke aard te mogen verwerken door de AP, waardoor de valse-e-mail-check moest worden gestopt. De AP oordeelde dat de Fraudehelpdesk de noodzaak voor het verwerken van persoonsgegevens van strafrechtelijke aard onvoldoende had aangetoond.^{90/91} Daarnaast kan volgens de Fraudehelpdesk hebben meegespeeld dat mensen vanwege thuiswerken en blijven

⁸⁷ Cijfers zijn gebaseerd op registraties uit de jaarverslagen. De aantallen zijn exclusief het gebruik van de dienst valse-e-mailcheck. Voor 1 januari 2015 werden niet alle meldingen en telefoontjes van het call center vastgelegd als fraude gerelateerde zaken. Met ingang van 1 januari 2015 is hier wel mee gestart. In de jaarverslagen van 2011 tot en met 2014 wordt niet tot nauwelijks ingegaan op het aantal doorverwijzingen. Omdat sinds 1 januari 2015 alles wordt geregistreerd en dit een betrouwbare weergave vormt van de meldingen en doorverwijzingen, zijn vanaf 2015 de registraties opgenomen.

⁸⁸ Jaarverslag 2019, p. 10.

⁸⁹ Jaarverslag 2020, p. 10.

⁹⁰ AP, Besluit inzake de vergunningaanvraag voor de verwerking van gegevens van strafrechtelijke aard ten behoeve van derden van de verwerking van 'Fraudehelpdesk' van Safecin, 19 juni 2019.

⁹¹ Na de afwijzing van de eerste vergunningaanvraag bij de AP heeft de Fraudehelpdesk voor de verschillende diensten een data protection impact assessment (DPIA) opgesteld. Na onder meer het opstellen van een DPIA voor de dienst van de valse e-mail-check concludeerde de Fraudehelpdesk dat het aanvragen van een vergunning voor deze dienst niet noodzakelijk was en is de dienst hervat (zie het jaarverslag van 2019).

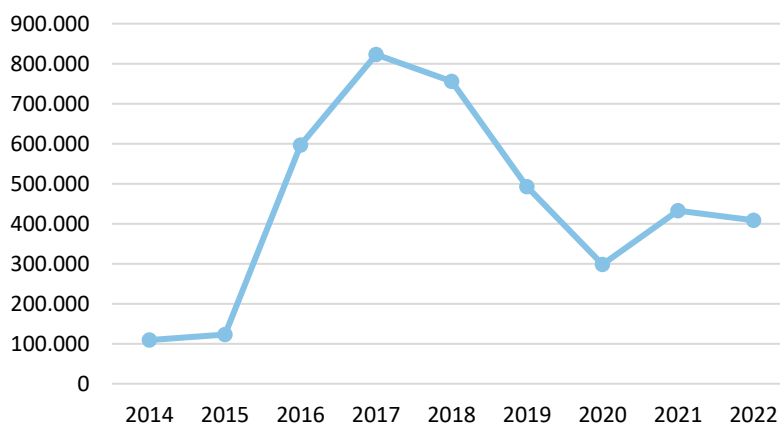
vaker achter de computer zaten en wellicht ook sneller de moeite namen om een melding te doen bij de Fraudehelpdesk.⁹² In paragraaf 5.3.2 wordt verder ingegaan op welke invloed de coronacrisis kan hebben gehad op het aantal meldingen.

Uit figuur 3.3 blijkt verder dat het aantal digitale meldingen de laatste twee jaar daalde ten opzichte van 2020. Volgens de Fraudehelpdesk is de afname met name veroorzaakt door de aanpassing van het verkorte meldformulier, waardoor relatief veel informatie van melders wordt gevraagd in verhouding tot hetgeen hen is overkomen.⁹³ Hierdoor worden minder meldingen gedaan via het verkorte formulier (in 2021 waren dit 54.866 verkorte meldingen en in 2022 14.730).⁹⁴ Het aantal meldingen via het uitgebreide formulier nam volgens de Fraudehelpdesk in 2021 wel toe ten opzichte van een jaar eerder, maar nam in 2022 af ten opzichte van 2021.⁹⁵

Het aantal telefonische meldingen nam in 2020 (5.363) ten opzichte van 2019 (9.118) af. De reden hiervoor is waarschijnlijk dat het callcenter door de lockdowns in 2020 drie keer werd gesloten.⁹⁶ Ook in 2021 was het callcenter vanwege de coronamaatregelen in 2021 deels gesloten. Het aantal telefonische meldingen nam in 2021 (5.644) iets toe ten opzichte van 2020. In 2022 is er meer dan een verdubbeling van het aantal telefonische meldingen ten opzichte van 2021 te zien.

In figuur 3.4 is weergegeven hoe vaak per jaar gebruik is gemaakt van de dienst valse-e-mailcheck.

FIGUUR 3.4: GEBRUIK VALSE-E-MAILCHECK⁹⁷



⁹² Jaarverslag 2020, p. 9.

⁹³ Via de website kan een particulier via één formulier een melding doen. Het formulier kent, afhankelijk van het type fraude dat de melder aanklikt, een lange en korte versie. De korte versie van het formulier, wordt het verkorte formulier genoemd. De lange versie, die ook de gelegenheid biedt aan de melder om gebruik te maken van open invulvelden, wordt het uitgebreide formulier genoemd.

⁹⁴ Jaarverslag 2022, p. 4.

⁹⁵ Dit is door de Fraudehelpdesk aangegeven in de wederhoorfase.

⁹⁶ In 2019 werd het callcenter in ieder geval vijf weken gesloten zo blijkt uit het jaarverslag. Daarnaast is het callcenter tijdelijk met aangepaste openingstijden en minimale bezetting open geweest. Het aantal weken dat het callcenter in 2021 gesloten was blijkt niet precies uit het jaarverslag van 2021. Wel wordt aangegeven dat het kantoor, meer dan in 2020, periodes helemaal dicht is geweest.

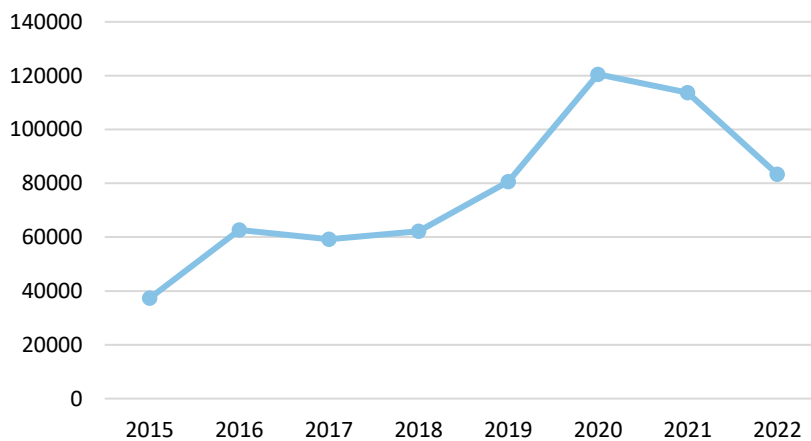
⁹⁷ Cijfers zijn gebaseerd op registraties uit de jaarverslagen.

Waar de meldingen via het digitaal meldformulier en telefonisch in de periode 2015 tot 2018 nagenoeg constant bleven, nam het gebruik van de dienst valse-e-mailcheck in 2016 en 2017 jaar fors toe. In de jaarverslagen van de Fraudehelpdesk wordt hiervoor geen verklaring gegeven. Medio 2019 is de Fraudehelpdesk gestopt met de dienst valse-e-mail-check in verband met het afwijzen van de vergunning van de AP (zie voor een verdere toelichting paragraaf 3.5.1).⁹⁸ Dit verklaart volgens de Fraudehelpdesk de terugval in het gebruik van de dienst.⁹⁹ In maart 2020 heeft de Fraudehelpdesk, na het opstellen van een data protection impact assessment (DPIA), de dienst valse-e-mailcheck weer hervat. Sinds dat moment worden verdachte e-mails ook gepubliceerd op de website.¹⁰⁰ In 2021 steeg het gebruik van de valse-e-mailcheck ten opzichte van 2020. Ook hiervoor ligt de oorzaak naar verwachting in het feit dat de dienst in de eerste twee maanden van 2020 niet gebruikt kon worden en in dezelfde periode in 2021 wel meldingen zijn binnengekomen.

Registratie van meldingen door de Fraudehelpdesk in relatie tot aangifte van horizontale fraude

In figuur 3.5 is het aantal aangiften van horizontale fraude bij de Politie weergegeven in de periode 2015 tot en met 2022.

FIGUUR 3.5: TOTAAL AANTAL AANGIFTEN HORIZONTALE FRAUDE¹⁰¹



Wat opvalt is dat, net als het aantal meldingen bij de Fraudehelpdesk (figuur 3.3), in 2019 en 2020 een relatief grote toename van het aantal aangiften waarneembaar is. Ook daalde, net als de meldingen bij de Fraudehelpdesk, het aantal aangiften van horizontale fraude in 2021 en 2022.

Slachtoffers van fraude die melden bij de Fraudehelpdesk

In de slachtofferstudie die Junger e.a. in 2022 uitvoerden blijkt dat 7 van 393 (1,4 procent) slachtoffers na een eerste betaling of verlies van geld als gevolg van een frauduleus incident melding hebben gedaan bij de Fraudehelpdesk.¹⁰² Uit een ander onderzoek van Conradie en Doms naar de beleving van digitale veiligheid blijkt dat van de 898 respondenten die aangaven in een privé-situatie met cybercrime te maken hebben gehad, de meeste mensen die melding

⁹⁸ Zie paragraaf 3.5.

⁹⁹ Jaarverslag 2019, p. 10.

¹⁰⁰ Jaarverslag 2020, p. 10.

¹⁰¹ Data.politie.nl.

¹⁰² Junger e.a. 2020, paragraaf 3.4.6 van de bijlage bij het rapport.

deden, dit deden bij de Fraudehelpdesk (16 procent).¹⁰³ De meest genoemde reden om geen melding of aangifte te doen was dat mensen dachten dat dat geen zin had (29%).

Nieuwe fraudevormen

In algemene zin ziet de Fraudehelpdesk dat de wijze waarop fraudeurs te werk gaan door de jaren heen steeds geraffineerder is geworden. Dit komt onder meer door het gebruik van nieuwe technieken, datalekken en social engineering. Nieuwe fraudevormen die de Fraudehelpdesk sinds de vorige evaluatie in 2012 onder meer heeft gesignaleerd zijn: hulpvraagfraude, helpdeskfraude, nep-telefoontjes van de bank, nep-betaalverzoeken, 1-centfraude, acquisitiefraude, datingfraude, beleggingsfraude en vacaturefraude.¹⁰⁴

De invloed van de coronacrisis op fraude

De Fraudehelpdesk zag tijdens de coronacrisis in 2020 een toename van met name meldingen op het gebied van hulpvraagfraude en aan- en verkoopfraude. Mensen werden tijdens de coronacrisis volgens de Fraudehelpdesk actief op platforms en kanalen waar ze dat voorheen niet waren en er werd (gedwongen) meer online gewinkeld, met alle gevolgen van dien.¹⁰⁵ Dat er tijdens de coronacrisis een toename was in aan- en verkoopfraude lijkt aan te sluiten bij de bevindingen van onderzoek dat is gedaan naar de invloed van de coronacrisis op het aantal slachtoffers van cybercriminaliteit.¹⁰⁶

Aan de andere kant laat het onderzoek zien dat cybercriminaliteit in het algemeen niet significant is toegenomen tijdens de coronacrisis.¹⁰⁷ De onderzoekers geven aan dat deze bevinding niet overeenkomt met andere studies op basis van officiële registraties (bijv. registraties van aangiften) over cybercriminaliteit; die vonden juist een toename van slachtofferschap gedurende de pandemie. Deze discrepantie tussen gevonden trends in cybercriminaliteit in officiële registraties en in zelf-rapportages suggereert volgens de onderzoekers dat er niet zo zeer een toename is geweest van cybercriminaliteit, maar dat er een toename heeft plaatsgevonden in het melden en registreren van cybercriminaliteit.¹⁰⁸ Hoewel de resultaten van het onderzoek geen invloed laten zien in de omvang van cybercriminaliteit tijdens de coronacrisis, lijkt de modus operandi van criminelen volgens de onderzoekers wel te zijn veranderd. Met name slachtoffers van fraude gaven aan dat daders bij het plegen van fraude misbruik hadden gemaakt van de pandemie.¹⁰⁹

Ontwikkeling online- aan en verkoopfraude

Een toename in online aan- en verkoopfraude lijkt een ontwikkeling die zich al langere tijd voordoet. In 2020 hebben Beerthuizen e.a. onderzoek gedaan naar de aard en omvang van slachtofferschap van diverse vormen van fraude. Het onderzoek laat op basis van een aantal longitudinale bronnen zien dat er een groei te zien is in slachtoffers van online aan- en verkoopfraude. De Veiligheidsmonitor van het CBS laat een toename zien van bijna 2,9 procent in 2012 tot 4,6 procent in 2019 en het LISS-panel laat een toename zien van 2,6 procent in

¹⁰³ Conradie en Doms 2022, p.39.

¹⁰⁴ Deze informatie is in de wederhoorfase verkregen van de Fraudehelpdesk. We hebben niet de beschikking gekregen over alle rapportages die zijn opgesteld vóór de invoering van de maandmonitoren, om na te gaan of daarin bepaalde nieuwe fraudevormen worden genoemd. In bijlage 9 is een toelichting te vinden op de genoemde fraudevormen.

¹⁰⁵ Jaarverslag 2020, p. 9.

¹⁰⁶ Van de Weijer en Leukfeldt 2023, p. 25.

¹⁰⁷ De onderzoekers hebben in 2021 en 2019 een vragenlijst uitgezet onder mkb'ers en burgers.

¹⁰⁸ Van de Weijer en Leukfeldt 2023, p. 25-26.

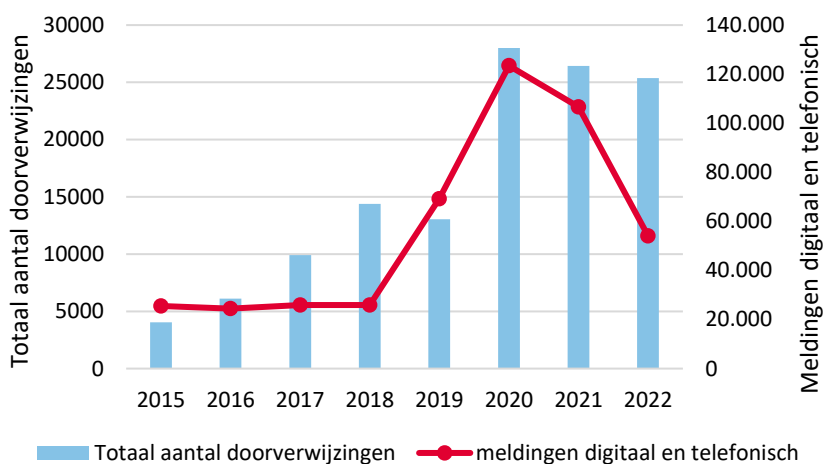
¹⁰⁹ Van de Weijer en Leukfeldt, 2023, p. 26.

2012 tot 4,4 procent in 2018.¹¹⁰ Deze toename is volgens de onderzoekers niet verwonderlijk gezien een toename in online winkelen, wat meer gelegenheid creëert voor dit soort fraude.

3.4.2 Doorverwijzen meldingen

Een van de publieke kerntaken van de Fraudehelpdesk is het doorverwijzen van meldingen naar de instantie die de melder verder kan helpen. Melders die de Fraudehelpdesk benaderen worden geadviseerd en op basis van de specifieke situatie van de melder doorverwezen. In grafiek 3.6 is in de blauwe staven het totaal aantal doorverwijzingen per jaar weergegeven. De rode lijn geeft het totaal aantal meldingen (exclusief valse-e-mailcheck) weer.¹¹¹

FIGUUR 3.6: TOTAAL AANTAL DOORVERWIJZINGEN PER JAAR DOOR DE FRAUDEHELPDESK



De grafiek laat zien dat het aantal doorverwijzingen in de periode 2015 - 2018 relatief gezien toenam. In 2019 nam het aantal doorverwijzingen ten opzichte van 2018 met ongeveer duizend af, terwijl door de komst van de nieuwe website het aantal meldingen toenam. In 2020 is het aantal doorverwijzingen ten opzichte van 2019 meer dan verdubbeld. De Fraudehelpdesk geeft aan dat dit komt doordat er steeds meer complexe meldingen binnenkwamen, waardoor de melder naar meerdere partijen moet worden doorverwezen. Daarnaast wordt sinds 2020 ook iedereen die kans maakt om geld terug te vragen doorgestuurd naar partijen die slachtoffers hierbij kunnen helpen.

In 2021 en 2022 is het aantal doorverwijzingen – net als het aantal meldingen – ten opzichte van een jaar eerder iets gedaald.¹¹² Melders kunnen naar meerdere organisaties worden doorverwezen, daarom ligt het aantal doorverwijzingen in de laatste jaren hoger dan het totaal aantal meldingen.

Uit tabel 3.7 blijkt dat de meeste slachtoffers worden doorverwezen naar de Politie, het Landelijk Meldpunt Internetoplichting (LMIO), ConsuWijzer (ACM), het centraal Meldpunt Identiteitsfraude (CMI) en de laatste jaren ook naar Stichting Slachtofferhulp Nederland (SHN).

¹¹⁰ Beerthuizen e.a. 2020, p. 37 en 40.

¹¹¹ De valse-e-mailcheck meldingen zijn niet meegenomen.

¹¹² Voor 1 januari 2015 werden niet alle meldingen en telefoontjes van het call center vastgelegd als fraude gerelateerde zaken. Met ingang van 1 januari 2015 is hier wel mee gestart. In de jaarverslagen van 2011 tot en met 2014 wordt niet tot nauwelijks ingegaan op het aantal doorverwijzingen. Omdat sinds 1 januari 2015 alles wordt geregistreerd en dit een betrouwbare weergave vormt van de meldingen en doorverwijzingen, zijn vanaf 2015 de registraties opgenomen.

TABEL 3.7: DOORVERWIJZINGEN¹¹³

	2014	2015	2016	2017	2018	2019	2020	2021	2022
ACM (ConsuWijzer)	609	1629	2153	2487	3282	3148	3900	2468	3731
ACM ondernemers	0	0	0	0	244	228	192	62	0
AFM	0	17	23	130	171	112	472	533	658
BFT	0	3	0	7	12	7	5	0	6
CMI	0	263	307	351	680	592	1416	1719	1742
DUO	0	0	0	0	0	1	0	0	0
ECC	92	109	280	350	379	349	575	180	416
Fiscus	0	10	7	61	35	65	476	472	640
IGZ	0	3	0	7	4	2	15	4	6
Juridisch adviseur	0	90	292	1879	2410	1944	2247	1597	4052
Het juridisch Loket	0	176	0	0	0	0	0	0	0
Kansspelautoriteit	0	9	5	5	8	5	12	4	18
LMIO	520	1233	1352	1428	1218	1214	3919	5055	4679
Politie	0	662	1689	3072	5552	5076	12066	12355	7635
SHN	0	0	0	136	319	287	2692	1995	1777
KIFID	0	7	0	0	0	0	0	0	0
Ombudsman	0	8	0	0	0	0	0	0	0
Totaal	1.221	4.219	6.108	9.913	14.314	13.030	27.987	26.444	25.360

Sinds 2020 is het aantal doorverwijzingen naar Slachtofferhulp Nederland (SHN) relatief toegenomen. Deze ontwikkeling komt overeen met wat in de gesprekken naar voren is gekomen, namelijk dat er ongeveer sinds 2019 een betere samenwerking met Slachtofferhulp Nederland is.

In 2021 werden ongeveer duizend extra melders doorverwezen naar het LMIO. Dit had volgens de Fraudehelpdesk te maken met een forse toename in het aantal meldingen over frauduleuze online aan- en verkopen, namelijk een stijging van ruim 25% ten opzichte van 2020. Datzelfde is terug te vinden bij beleggingsfraude, daar zag de Fraudehelpdesk het schadebedrag stijgen naar 19 miljoen euro. Dit was een toename van 45% ten opzichte van 2020 en zorgde voor een stijging van het aantal doorverwijzingen naar de Autoriteit Financiële Markten.¹¹⁴

In 2022 zijn er ten opzichte van de voorgaande jaren relatief veel melders doorverwezen naar juridische raadgevers. De oorzaak hiervoor is volgens de Fraudehelpdesk dat de frontoffice-medewerker de slachtoffers van telefonische en online fraude wijst op een civiele procedure tegen de persoon door wie het slachtoffer is opgelicht. Op die manier kan het slachtoffer proberen geld terug te krijgen.¹¹⁵

¹¹³ De cijfers zijn afkomstig uit de jaarverslagen van de Fraudehelpdesk. Deze aantallen zijn voorgelegd aan een aantal ketenpartners ter verificatie. In een van de reacties die de onderzoekers hebben ontvangen, werd aangegeven dat niet achterhaald kan worden door welke partner is doorverwezen, omdat het gaat om 'koude' doorverwijzingen.

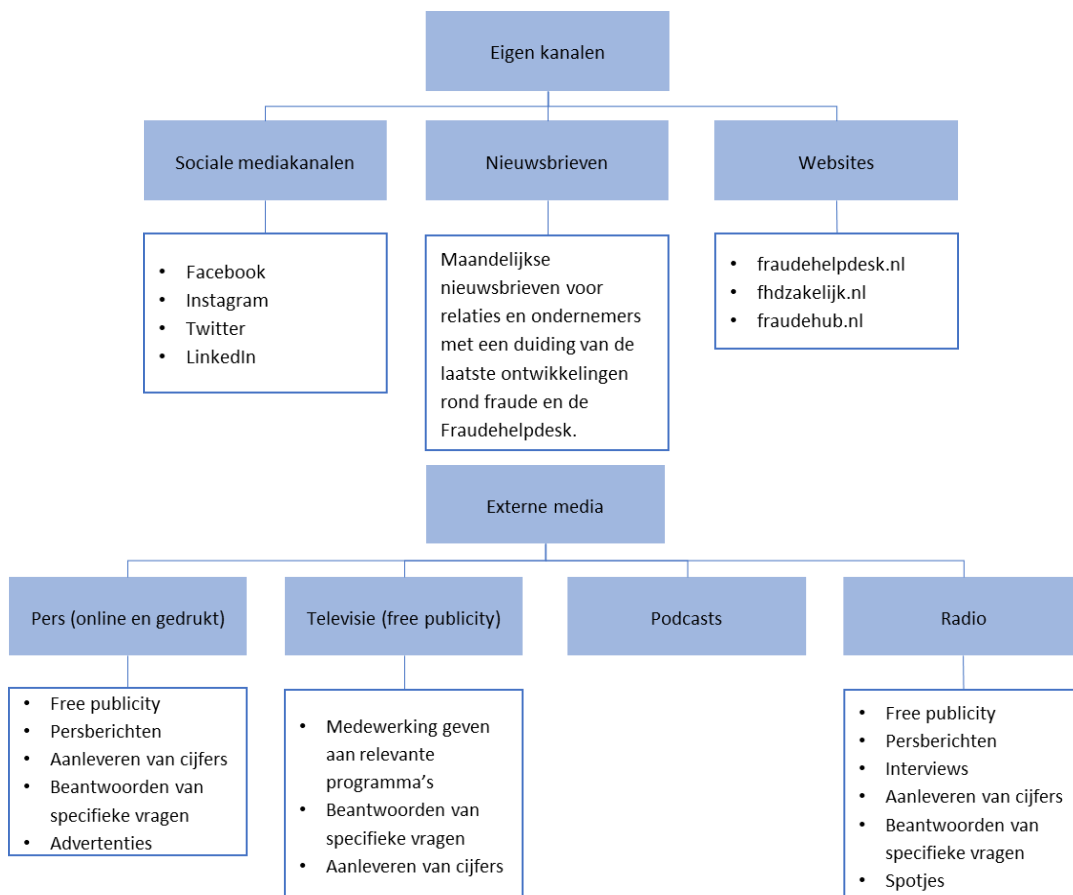
¹¹⁴ Jaarverslag 2021, p. 11.

¹¹⁵ Jaarverslag 2022, p.6.

3.4.3 Preventie

De Fraudehelpdesk is mede opgericht om burgers en kleine bedrijven weerbaarder te maken tegen pogingen tot oplichting. De Fraudehelpdesk doet dit onder andere door het beantwoorden van vragen van mensen die mogelijk te maken hebben met fraude, het opzetten en uitvoeren van campagnes, door het waarschuwen over actuele fraudevormen en het opzetten van projecten zoals de FraudeInfodesk, de FraudeHub en Fraudehelpdesk zakelijk. Het opzetten van deze projecten valt niet onder de basisdienstverlening die de Fraudehelpdesk aanbiedt, daarom worden voor deze projecten specifieke projectsubsidies aangevraagd bij ministeries en/of decentrale overheden. Om burgers en kleine bedrijven te bereiken is het noodzakelijk om communicatiekanalen zo goed mogelijk te benutten. In figuur 3.8 is een overzicht gegeven van de communicatiekanalen die de Fraudehelpdesk inzet. Deze middelen zet de Fraudehelpdesk in voor zowel de gesubsidieerde basisdienstverlening als overige projecten en initiatieven.¹¹⁶

FIGUUR 3.8: OVERZICHT COMMUNICATIEKANALEN



¹¹⁶ Dit overzicht is overgenomen uit het communicatieplan van de Fraudehelpdesk voor 2023.

De eigen kanalen die de Fraudehelpdesk inzet zijn sociale mediakanalen, de nieuwsbrief en websites. In 2022 heeft de Fraudehelpdesk het internetdomein fhdzakelijk.nl gekocht. Deze website is in 2023 online gegaan. De website van de Fraudehub is alleen toegankelijk voor specifieke ketenpartners. Ten behoeve van de zichtbaarheid van de Fraudehelpdesk op sociale media is in 2021 een medewerker sociale media gestart bij de Fraudehelpdesk.¹¹⁷

De externe media die de Fraudehelpdesk inzet zijn: pers, televisie, podcasts en radio. In gesprekken is aangegeven dat door het beperkte budget vooral wordt ingezet op free publicity. In bijlage 5 is aangegeven welke communicatiekanalen en projecten de Fraudehelpdesk vanaf 2012 heeft ingezet om burgers in te lichten over bepaalde fraudevormen.

Door de Fraudehelpdesk wordt in gesprekken aangegeven dat de laatste jaren steeds meer samenwerking wordt gezocht met ketenpartners als het gaat om het opzetten en uitvoeren van campagnes. In het jaarverslag van 2020 wordt aangegeven dat in dat jaar de samenwerking met ketenpartners centraal stond. De Fraudehelpdesk heeft de inhoud van verschillende campagnes afgestemd met relevante partnerorganisaties, zodat zij de burger eenzelfde handelingsperspectief bieden en zo veel mogelijk dezelfde terminologie hanteren. Verder waren de campagnes zo gepland dat ze waar mogelijk aansluiten op tijdgebonden evenementen en door partners geïnitieerde campagnes.¹¹⁸

3.5 Overige ontwikkelingen rondom de dienstverlening

3.5.1 Verwerken van persoonsgegevens van strafrechtelijke aard

Uit enkele gesprekken met onder meer ketenpartners blijkt dat in de beginperiode van de Fraudehelpdesk er een intensieve samenwerking was tussen het ministerie van JenV, de Fraudehelpdesk en andere ketenpartners in de fraudebestrijdingsketen. Ten tijde van de oprichting van de Fraudehelpdesk was fraude een opkomend fenomeen en er was weinig bekendheid met het onderwerp. De Fraudehelpdesk verwerkte destijds nog persoonsgegevens van daders en deelde die met ketenpartners. Zo wordt in het jaarverslag van 2014 aangegeven dat met de Belastingdienst landelijk afspraken zijn gemaakt over informatieverstrekking door de Fraudehelpdesk. Daarnaast werd samengewerkt met het Expertisecentrum Identiteitsfraude en Documenten van de Koninklijke Marechaussee op Schiphol in het kader van controle op identiteitsdocumenten en werden indien nodig zaken aan de FIOD doorgespeeld. Ook werden zaken doorgespeeld aan de banken, de Politie en Post NL.¹¹⁹ Tot en met het jaarverslag van 2016 wordt aangegeven dat de focus van de Fraudehelpdesk onder andere ligt – voor zover dat in haar vermogen ligt en past in de aan haar opgedragen taak – in het actief helpen inrichten en opwerpen van barrières tegen fraudeurs, waar mogelijk samen te werken met organisaties als banken, verzekeraars, geldtransactiekantoren, telecom en hostingbedrijven, accountants en administratiekantoren, softwareleveranciers en datingsites.¹²⁰

Het verwerken van persoonsgegevens van strafrechtelijke aard ten behoeve van derden is op grond van de Algemene Verordening Gegevensbescherming (AVG) in principe niet toegestaan.

¹¹⁷ Jaarverslag 2021, p. 14.

¹¹⁸ Jaarverslag 2020, p. 12.

¹¹⁹ Jaarverslag 2014 p. 7.

¹²⁰ Jaarverslag 2016, p. 9.

Om deze gegevens ten behoeve van derden te mogen verwerken is een vergunning vereist van de AP.

Het verwerken van persoonsgegevens van strafrechtelijke aard ten behoeve van derden

De AVG maakt onderscheid tussen ‘gewone’ persoonsgegevens, bijzondere persoonsgegevens en persoonsgegevens van strafrechtelijke aard. Persoonsgegevens van strafrechtelijke aard zijn gegevens over strafrechtelijke veroordelingen en strafbare feiten of daarmee verband houdende veiligheidsmaatregelen en persoonsgegevens over een door de rechter opgelegd verbod naar aanleiding van onrechtmatig of hinderlijk gedrag. Het verwerken van persoonsgegevens van strafrechtelijke aard ten behoeve van derden is in principe verboden.

De uitzondering op het verwerken van persoonsgegevens van strafrechtelijke aard ten behoeve van derden is opgenomen in artikel 33, vierde lid, aanhef en onder c van de UAVG. Op grond van dat lid moet een vergunning bij de AP worden aangevraagd. De AP kan een vergunning verlenen, indien de verwerking noodzakelijk is met het oog op een zwaarwegend belang van derden en bij de uitvoering is voorzien in zodanige waarborgen dat de persoonlijke levenssfeer van de betrokkene niet onevenredig wordt geschaad.

De Fraudehelpdesk heeft om persoonsgegevens van strafrechtelijke aard te mogen verwerken in 2019 een eerste vergunning aangevraagd bij de AP maar deze aanvraag werd afgewezen.¹²¹ De aanvraag had betrekking op meerdere diensten die door de Fraudehelpdesk werden aangeboden, zoals het openbaar publiceren over frauduleuze activiteiten, het informeren en doorverwijzen van melders en de valse e-mailcheck. De AP oordeelde dat de Fraudehelpdesk de noodzaak en proportionaliteit voor het verwerken van persoonsgegevens van strafrechtelijke aard onvoldoende had onderbouwd. Volgens de AP had de Fraudehelpdesk per verwerking de noodzakelijkheid moeten onderbouwen.

Na de afwijzing van de eerste vergunningaanvraag in 2019 heeft de Fraudehelpdesk voor verschillende diensten een DPIA opgesteld. Voor specifiek de helpdeskfunctie is vervolgens in 2020 een tweede vergunningaanvraag ingediend bij de AP. Deze aanvraag is op 12 juli 2021 afgewezen.¹²² De reden voor de afwijzing is kortgezegd dat er volgens de AP geen noodzaak is om persoonsgegevens van strafrechtelijke aard te verwerken om de doelen van de Fraudehelpdesk te bereiken. De AP is er niet van overtuigd dat persoonsgegevens van en over de (vermoedelijke) dader nodig zijn om de melder te informeren, adviseren en door te verwijzen naar de juiste organisatie. De AP is van oordeel dat de Fraudehelpdesk melders ook kan adviseren door alleen gebruik te maken van informatie over de modus operandi. Met informatie over de wijze waarop de (vermeende) fraude heeft plaatsgevonden, moet de Fraudehelpdesk de melder zodanig kunnen adviseren en informeren dat de melder weet of hij slachtoffer is geworden van fraude, welk type fraude het betreft, of hoe hij daar met behulp van informatie van de Fraudehelpdesk achter kan komen. ‘Het verwerken van persoonsgegevens van strafrechtelijke aard om mogelijke stelselmatigheid te kunnen aantonen – ten behoeve van toekomstige melders – of iemand overtuigen van slachtofferschap’ is daarvoor naar het oordeel van de AP niet noodzakelijk.¹²³

¹²¹ AP, Beslissing van 19 juni 2019, z2018-12010.

¹²² Er loopt ten tijde van dit onderzoek een hoger beroepszaak bij de rechtbank Gelderland tegen de afwijzing van de vergunning.

¹²³ AP, Beslissing op bezwaar, 3 februari 2022, p. 9.

Door het niet meer mogen verwerken van persoonsgegevens van strafrechtelijke aard, is de samenwerking op het gebied van het actief helpen inrichten en opwerpen van barrières tegen fraudeurs weggefallen. Uit de gesprekken met de Fraudehelpdesk en ketenpartners blijkt dat er een veel minder intensieve samenwerking is met bijvoorbeeld het ministerie van JenV, de Politie en het OM als het gaat om het bestrijden van fraude ten opzichte van de beginperiode van de Fraudehelpdesk.

Uit de gesprekken met de Fraudehelpdesk komt naar voren dat de organisatie van mening is dat om een optimale dienstverlening te kunnen bieden, het mogen verwerken van persoonsgegevens van strafrechtelijke aard essentieel is. Het afwijzen van de aanvraag om een vergunning heeft veel impact gehad op de dienstverlening. Het mogen verwerken van persoonsgegevens van strafrechtelijke aard is volgens de Fraudehelpdesk noodzakelijk om vast te stellen of de melder te maken heeft met een legitiem bericht en om de melder te kunnen voorzien van een goed advies. Veel melders kunnen een vals bericht zelf niet herkennen en telefonisch of schriftelijk moeilijk beschrijven volgens de Fraudehelpdesk.¹²⁴ Daarnaast blijkt volgens de Fraudehelpdesk dat de gehanteerde werkwijze afwijkt van de (versimpelde en incomplete) beschrijving van de melder zelf. Een melder ziet relevante informatie vaak over het hoofd, wat leidt tot een verkeerde kwalificatie en daarop (onjuist) gebaseerd advies. Wanneer de Fraudehelpdesk persoonsgegevens van strafrechtelijke aard wel mag verwerken, kan een melder onderliggende stukken met de Fraudehelpdesk delen. Daarnaast zou, wanneer de persoonsgegevens van strafrechtelijke aard mogen worden gedeeld met andere organisaties, de Fraudehelpdesk bijvoorbeeld bankrekeningnummers kunnen doorgeven aan banken die vervolgens die rekeningnummers zouden kunnen blokkeren.¹²⁵ Ook kan voor melders worden nagegaan of een ondernemer staat ingeschreven bij de Kamer van Koophandel (KvK) en daarmee een advies worden gegeven in het geval een melder een e-mail van een ondernemer bijvoorbeeld niet helemaal vertrouwt.

3.6 Conclusie

In dit hoofdstuk is onderzocht op welke manier de organisatie van de Fraudehelpdesk is ingericht en welke ontwikkelingen er sinds 2012 zijn geweest op het gebied van de financiering en geleverde diensten. De Fraudehelpdesk heeft de afgelopen jaren ingezet op een verdere professionalisering van de organisatie, zo zijn er functieprofielen en een organogram opgesteld die helderheid moeten bieden over de inhoud van functies en verdeling van taken en verantwoordelijkheden.

Met betrekking tot de financiering van de Fraudehelpdesk is gebleken dat de subsidiebatensinds 2012 afkomstig waren van het ministerie van JenV en het ministerie van EZK, waarbij EZK de subsidie in 2021 en 2022 heeft afgebouwd. Uit gesprekken en jaarverslagen blijkt dat de Fraudehelpdesk behoefte heeft aan meer en structurele subsidie. Door het ontbreken van een meerjarige subsidierelatie is er volgens de Fraudehelpdesk veel onzekerheid en zijn er geen middelen om te innoveren en investeren. De Fraudehelpdesk probeert daarom nu ook in te zetten op het ophalen van middelen bij brancheorganisaties en gemeenten. Daarnaast is

¹²⁴ AP, Beslissing op bezwaar, 3 februari 2022, p. 8.

¹²⁵ De vergunning die de Fraudehelpdesk in 2020 heeft aangevraagd voor het mogen verwerken van persoonsgegevens van strafrechtelijke aard had alleen betrekking op de helpdeskfunctie.

gebleken dat de relatie tussen de Fraudehelpdesk en het ministerie van JenV op dit moment vooral financieel van aard is en dat er beleidsinhoudelijk in geringe mate afstemming is. Het ministerie van JenV geeft aan dat het passend is om in de toekomst meer vraaggestuurd te gaan samenwerken vanuit een meerjarige beleidsvisie, maar voor nadere besluitvorming voor de herijking van zowel de beleids- als de financieringsrelatie met de Fraudehelpdesk dienen eerst de uitkomsten van dit onderzoek te worden afgewacht.¹²⁶

De subsidievoorwaarden die in 2010 zijn opgesteld voor de Fraudehelpdesk zijn sinds 2021, door aanpassen van de subsidieregelgevingssystematiek binnen het ministerie van JenV, niet meer van toepassing. Wel lijkt de Fraudehelpdesk grotendeels nog aan de destijds gestelde voorwaarden te voldoen. Aan twee aspecten lijkt niet volledig te worden voldaan. Zo is de telefonische helpdesk niet iedere dag van 9.00 - 17.00 uur bereikbaar en blijkt uit het vragenlijstonderzoek dat niet alle vragen/meldingen binnen twee dagen worden beantwoord (ruim 40 procent wordt wel binnen twee dagen beantwoord, zie paragraaf 3.3).

De diensten die de Fraudehelpdesk verleent, bestaan uit het doorverwijzen van melders, het registreren van aantallen en soorten meldingen en het verstrekken van kennis en informatie over (nieuwe) vormen van fraude. Uit de registraties blijkt dat het aantal meldingen bij de Fraudehelpdesk tussen 2015 en 2018 vrij stabiel was, in 2019 en 2020 het aantal meldingen fors toenam, en in 2021 en 2022 er een afname te zien is in het aantal geregistreerde meldingen (met name via het verkorte meldformulier). De ontwikkeling van het aantal meldingen komt vanaf 2019 gedeeltelijk overeen met het aantal aangiften bij de Politie van horizontale fraude. In de periode tussen 2015 en 2018 was er bij de Politie een lichte toename van het aantal aangiften van horizontale fraude, terwijl deze stijging niet uit de registraties van de Fraudehelpdesk valt af te leiden. Het feit dat het aantal meldingen in de periode 2019 tot en met 2022 hoger lag dan in de jaren daarvoor, kan te maken hebben met de coronacrisis. Uit onderzoek van Van de Weijer en Leukfeldt blijkt dat er een discrepantie lijkt te bestaan tussen gevonden trends in cybercriminaliteit in officiële registraties en in zelf-rapportages. Dit suggereert volgens de onderzoekers dat er niet zo zeer een toename is geweest van cybercriminaliteit, maar dat er een toename heeft plaatsgevonden in het melden en registreren van cybercriminaliteit.¹²⁷ De Fraudehelpdesk signaleert dat fraudeurs, door de komst van nieuwe technieken, in de afgelopen jaren steeds geraffineerder te werk gaan. Nieuwe fraudevormen die de Fraudehelpdesk sinds de vorige evaluatie heeft gesignaleerd zijn onder meer: hulpvraagfraude, helpdeskfraude en datingfraude.¹²⁸

Uit de jaarverslagen blijkt dat jaarlijks via campagnes wordt ingezet op het verstrekken van informatie en (nieuwe) vormen van fraude. Daarnaast plaatst de Fraudehelpdesk waarschuwingsberichten op de website en worden maandmonitoren met trends en ontwikkelingen verstuurd. De Fraudehelpdesk wil daarnaast graag een expertisecentrum worden op het gebied van horizontale fraude en andere initiatieven ontwikkelen zoals het opzetten van een Fraudehub, het opzetten van een Fraudehelpdesk zakelijk voor ondernemers en het deelnemen aan verschillende

¹²⁶ Subsidiebeschikking, 26 januari 2023.

¹²⁷ Van de Weijer en Leukfeldt 2023, p. 25-26.

¹²⁸ Deze informatie is in de wederhoorfase verkregen van de Fraudehelpdesk.

Voor het mogen verwerken van persoonsgegevens van strafrechtelijke aard ten behoeve van derden is een vergunning van de AP vereist. De Fraudehelpdesk heeft in 2020 een vergunning aangevraagd voor het mogen verwerken van deze persoonsgegevens van strafrechtelijke aard ten behoeve van de helpdeskfunctie. De vergunningaanvraag is afgewezen, omdat de AP van oordeel is dat persoonsgegevens van de (mogelijke) dader niet nodig zijn om de melder te overtuigen van zijn slachtofferschap, om stelselmatigheid van fraude vast te stellen en/of om te bepalen of een melding van frauduleuze aard is. Volgens de AP zou informatie over de wijze waarop de fraude heeft plaatsgevonden ook voldoende moeten zijn om slachtoffers bij te staan en te informeren. De Fraudehelpdesk ervaart het niet mogen verwerken van persoonsgegevens van strafrechtelijke aard aan de andere kant als een belemmering voor optimale dienstverlening. De Fraudehelpdesk geeft aan dat de melders beter zouden kunnen worden geholpen als ook persoonsgegevens van strafrechtelijke aard zouden mogen worden verwerkt. Voor het behandelen van een melding is het noodzakelijk een goed beeld te krijgen van de situatie. Daarvoor zijn volgens de Fraudehelpdesk onderliggende stukken van de melding nodig. Op die manier kan de Fraudehelpdesk vaststellen of de melder te maken heeft met een legitiem bericht en om de melder op de juiste wijze te adviseren.¹²⁹

¹²⁹ Fraudehelpdesk, aanvulling beroepsschrift tegen het besluit met kenmerk z2021-14398, p. 9.

4 Bekendheid Fraudehelpdesk

4.1 Inleiding

In dit hoofdstuk staat de bekendheid van de Fraudehelpdesk centraal (deelvraag 6). In paragraaf 4.2 lichten we toe hoe we de bekendheid van de Fraudehelpdesk hebben onderzocht. In paragraaf 4.3 wordt aandacht besteed aan de naamsbekendheid van de Fraudehelpdesk. Paragraaf 4.4 gaat in op de vindbaarheid van de website en paragraaf 4.5 op het aantal bezoekers van de website. Paragraaf 4.6 bevat een conclusie.

4.2 Websiteonderzoek

We zijn voor dit deelonderzoek gestart met het opstellen van een lijst met zoektermen waarvan mag worden verwacht dat daarbij de website van de Fraudehelpdesk naar voren komt. Deze lijst is vervolgens aangevuld door middel van een SEO-tool (Search Engine Optimization) met synoniemen.¹³⁰ Ook is gekeken naar zoektermen waarop niet of nauwelijks zoekvolume zat. Deze zoektermen zijn uit de lijst met zoektermen verwijderd.¹³¹ Dit heeft geleid tot een lijst met in totaal 153 zoektermen, verdeeld over verschillende type fraude zoals voorschot-fraude, fraude met online handel en algemene zoektermen zoals 'ik ben opgelicht' en 'fraude melden'. Het onderzoek is uitgevoerd in april 2023.

4.3 Naamsbekendheid Fraudehelpdesk

4.3.1 Onderzoek naar de naamsbekendheid door de Fraudehelpdesk

De Fraudehelpdesk laat eens in de twee jaar onderzoek naar de naamsbekendheid onder Nederlanders uitvoeren.¹³² Bij alle naamsbekendheidsonderzoeken die in de afgelopen jaren zijn uitgevoerd is gebruik gemaakt van een panel. De onderzoeken zijn uitgevoerd in een periode van twee tot vier weken. Deelnemers van het panel komen uit heel Nederland, met spreiding over opleidingsniveau, sekse, leeftijd, inkomen, huishoudinkomen en/of huishoudsituatie. Bij

¹³⁰ De SEO-tool die hiervoor is ingezet is Ahrefs.

¹³¹ Als minder dan tien keer per maand op een zoekterm wordt gezocht is de zoekterm niet meegenomen in het onderzoek.

¹³² Wij hebben van de Fraudehelpdesk onderzoeken naar de naamsbekendheid uit 2014 (Infact Marktonderzoek), 2016 (Panel inzicht), 2018 (Markteffect), 2020 (Markteffect) en 2022 (Markteffect) ontvangen.

de onderzoeken die door Markteffect in 2018, 2020 en 2022 zijn uitgevoerd wordt in de onderzoeksverantwoording toegelicht dat de resultaten in de rapporten zijn gewogen naar een representatieve verdeling van leeftijd, geslacht en regio in Nederland. De steekproef bij alle onderzoeken onder burgers bestond uit minimaal duizend respondenten.¹³³

TABEL 4.1: STEEKPROEFSAMENSTELLING NAAMSBEKENDHEIDSONDERZOEKEN¹³⁴

<i>Onderzoek onder burgers</i>						<i>Onderzoek onder ondernemers</i>
<i>Jaar</i>	2014	2016	2018	2020	2022	2020
<i>N=</i>	1.000	1.000	1.000	1.111	1.015	440
<i>Geslacht</i>						
Man	48%	50%	49%	49%	49%	63%
Vrouw	52%	50%	51%	51%	51%	37%
<i>Leeftijd¹³⁵</i>						
Jonger dan 34 jaar	-	-	26%	27%	27%	12%
35 tot 50 jaar	-	-	27%	23%	23%	36%
50 jaar of ouder	-	-	47%	50%	50%	52%
<i>Regio¹³⁶</i>						
West-Nederland	-	41%	45%	47%	46%	47%
Zuid-Nederland	-	25%	24%	22%	24%	23%
Oost-Nederland	-	22%	21%	21%	20%	18%
Noord-Nederland	-	12%	10%	10%	10%	11%

Uit de rapportages van de naamsbekendheidsonderzoeken en navraag bij Markteffect blijkt niet hoe groot het panel is waar de vragenlijst bij is uitgezet, hoe (vaak) respondenten zijn benaderd om de vragenlijst in te vullen en hoe hoog het responspercentage is. Door het ontbreken van deze informatie en het feit dat deze onderzoeken in opdracht van de Fraudehulpdesk zijn uitgevoerd is de betrouwbaarheid van deze onderzoeken niet te toetsen. Aan de andere kant lijkt de toename van de naamsbekendheid wel in lijn te zijn met andere bevindingen van dit onderzoek, zoals de bevinding dat de website van de Fraudehulpdesk over het algemeen goed vindbaar is (paragraaf 4.4) en de groei van het aantal websitebezoekers in de loop der jaren (paragraaf 4.5). Ook het in de loop van de tijd gestegen aantal meldingen lijkt te wijzen op toegenomen bekendheid van de Fraudehulpdesk (figuur 3.3).¹³⁷

Daarnaast is in 2020 onderzoek gedaan naar de naamsbekendheid onder ondernemers. Aan het naamsbekendheidsonderzoek onder ondernemers namen 128 zzp'ers en 312 ondernemers uit het mkb deel.

¹³³ In bijlage 10 is de uitgebreide steekproefverantwoording zoals die in de onderzoeken van de bureaus is opgenomen overgenomen.

¹³⁴ Deze informatie is afkomstig uit de naamsbekendheidsonderzoeken die in opdracht van de Fraudehulpdesk zijn uitgevoerd; door afronding kan het voorkomen dat een percentage tot net onder of boven de honderd procent optelt zo wordt in de onderzoeksverantwoording van de onderzoeken aangegeven.

¹³⁵ In 2014 en 2016 werden andere leeftijdscategorieën aangehouden die in bijlage 10 zijn toegelicht.

¹³⁶ In 2014 werd een andere categorisering voor de regio aangehouden namelijk per provincie. In bijlage 10 is de respons per provincie opgenomen.

¹³⁷ Het totaal aantal meldingen nam in 2021 en 2022 wel weer af ten opzichte van 2020, maar ligt nog altijd hoger dan het totaal aantal meldingen in de periode tussen 2015 en 2018.

In de onderzoeken wordt onderscheid gemaakt tussen drie vormen van naamsbekendheid: top-of-mind naamsbekendheid, spontane naamsbekendheid en geholpen naamsbekendheid.

Top-of-mind naamsbekendheid

De top-of-mind naamsbekendheid geeft weer aan welke meldpunten respondenten het eerste moeten denken als gevraagd wordt naar fraudemeldpunten.¹³⁸ De ontwikkeling van de top-of-mind naamsbekendheid is weergegeven in tabel 4.2. De top-of-mind naamsbekendheid blijkt in de periode tussen 2014 en 2022 te zijn toegenomen met 10%. De top-of-mind naamsbekendheid onder ondernemers in 2020 bedroeg de helft ten opzichte van particulieren.

TABEL 4.2: TOP-OF-MIND NAAMSBEKENDHEID

	2014	2016	2018	2020	2022
Particulieren	2%	2%	9%	8%	12%
Ondernemers				4%	

Spontane naamsbekendheid

Bij spontane naamsbekendheid wordt aan respondenten gevraagd welke fraudemeldpunten zij allemaal (van naam) kennen.¹³⁹ Het verschil met top-of-mind naamsbekendheid is dat het hierbij niet gaat om welk meldpunt als eerste wordt genoemd. De ontwikkeling van de spontane naamsbekendheid is weergegeven in tabel 4.3. Uit de tabel blijkt dat ook de spontane naamsbekendheid in de periode tussen 2014 en 2022 is toegenomen met ruim 10%. Anders dan bij de top-of-mind naamsbekendheid, lag de spontane naamsbekendheid onder ondernemers hoger dan bij particulieren in 2020.

TABEL 4.3: SPONTANE NAAMSBEKENDHEID

	2014	2016	2018	2020	2022
Particulieren	1% ¹⁴⁰	3%	12%	10%	13%
Ondernemers				11%	

Geholpen naamsbekendheid

Geholpen naamsbekendheid heeft betrekking op de vraag of respondenten de Fraudehulpdesk herkennen.¹⁴¹ De ontwikkeling van de geholpen naamsbekendheid is weergegeven in tabel 4.4. Uit de tabel blijkt dat de geholpen naamsbekendheid in de periode tussen 2014 en 2022 is toegenomen met ruim 30%. Waar de top-of-mind en spontane naamsbekendheid onder ondernemers in 2020 lager of nagenoeg gelijk was dan bij particulieren, lag de geholpen naamsbekendheid onder ondernemers in 2020 9% hoger dan bij particulieren.

¹³⁸ De vraag die hiervoor aan respondenten bij het naamsbekendheidsonderzoek in 2020 en 2022 is voorgelegd luidt: 'welke organisaties die zich bezighouden met fraude kent u, ook al kent u het alleen van naam?'. Het antwoord dat als eerste werd gegeven, is gecategoriseerd als top-of-mind naamsbekendheid.

¹³⁹ De vraag die hiervoor aan respondenten bij het naamsbekendheidsonderzoek in 2020 en 2022 is voorgelegd is hetzelfde als bij de top-of-mind naamsbekendheid. Alle antwoorden die de respondent heeft gegeven, is gecategoriseerd als spontane naamsbekendheid.

¹⁴⁰ Het is de onderzoekers op basis van het naamsbekendheidsonderzoek uit 2014 niet duidelijk geworden waarom de spontane naamsbekendheid (1%) iets lager is dan de top-of-mind naamsbekendheid (2%).

¹⁴¹ De vraag die hiervoor aan respondenten bij het naamsbekendheidsonderzoek in 2020 en 2022 is voorgelegd luidt: 'welke van de onderstaande fraudemeldpunten kent u, ook al kent u het alleen van naam?'. Respondenten konden daarbij kiezen uit zeven antwoorden (Politie, Meld Misdaad Anoniem, Fraudehulpdesk, CMI, LMIO, anders of geen van deze).

TABEL 4.4: GEHOLPEN NAAMSBEKENDHEID

	2014	2016	2018	2020	2022
Particulieren	15%	15%	34%	43%	48%
Ondernemers				52%	

4.4 Vindbaarheid van de website

Om *het* meldpunt te zijn dat (potentiële) slachtoffers van fraude benaderen met vragen of meldingen is het van belang dat de Fraudehelpdesk een website heeft die eenvoudig vindbaar is op internet. We hebben daarom onderzoek gedaan naar de vindbaarheid van de Fraudehelpdesk in Google op voor de hand liggende zoektermen.

Per zoekterm is gekeken op welke positie de website van de Fraudehelpdesk als resultaat op Google verschijnt. Om de vindbaarheid van de website te beoordelen zijn de resultaten ingedeeld in drie categorieën:

Goed zichtbaar: positie 1 tot en met 10 (zichtbaar in de eerste resultatenpagina van Google)

Zichtbaar: positie 11 tot en met 100 (zichtbaar in Google maar niet op de eerste resultatenpagina in Google)

Slecht zichtbaar positie 101 e.v. (niet binnen de eerste tien resultatenpagina's in Google)¹⁴²

In tabel 4.5 is de zichtbaarheid van de Fraudehelpdesk in Google per categorie fraude weergegeven. De kolom 'categorie' geeft het overkoepelende thema weer van de zoektermen waarop is gezocht. In totaal zijn de zoektermen verdeeld over elf categorieën.¹⁴³ Een overzicht van alle zoektermen die zijn meegenomen in het onderzoek is opgenomen in bijlage 6. In de kolom 'aantal zoektermen' is het aantal zoektermen dat is onderzocht binnen een bepaalde categorie weergegeven. Er zijn bijvoorbeeld 66 zoektermen in relatie tot fraude met betaalmiddelen meegenomen. Kolom 'gemiddeld zoekvolume p/m' laat zien hoe vaak per maand in totaal op de zoektermen is gezocht. De 'gemiddelde positie' in de laatste kolom geeft weer op welke positie de website van de Fraudehelpdesk in de zoekresultaten van Google verschijnt. Hierbij is meegewogen dat zoektermen met meer zoekvolume zwaarder meewegen dan zoektermen met een laag zoekvolume. Indien de website van de Fraudehelpdesk niet in de eerste tien resultatenpagina's in Google verschijnt is dit weergegeven met het cijfer 0.

¹⁴² Het was met het gebruik van de SEO-tool alleen mogelijk om na te gaan of de website van de Fraudehelpdesk op een van de eerste tien pagina's voorkomt. Bij de categorie 'slecht zichtbaar' kan het dus zijn dat de Fraudehelpdesk op pagina 12 verschijnt of helemaal niet vindbaar is.

¹⁴³ Bij de categorisering is aansluiting gezocht bij de categorieën uit het Nationaal Dreigingsbeeld 2017. De categorie identiteitsfraude is hieraan toegevoegd.

TABEL 4.5: VINDBAARHEID GOOGLE

	Categorie	Aantal zoektermen	Gemiddeld zoekvolume p/m	Gemiddelde positie
1	Fraude met betaalmiddelen	66	42.480	15
2	Fraude met online handel	21	7.690	15
3	Algemeen	12	3.660	3
4	Beleggingsfraude	5	3.100	0
5	Telecomfraude	5	1.040	11
6	Acquisitiefraude	30	1.040	3
7	Identiteitsfraude	2	210	21
8	Hypotheekfraude	2	190	2
9	Faillissementsfraude	2	180	12
10	Verzekeringsfraude	2	100	50
11	Voorschotfraude	6	80	8

Uit deze tabel valt niet op te maken in hoeverre de website van de Fraudehelpdesk vindbaar is bij zoektermen binnen de elf categorieën. Een compleet overzicht met zoektermen en op welke positie de website van de Fraudehelpdesk in Google verschijnt is opgenomen in bijlage 6.

Van de 153 zoektermen die zijn onderzocht verschijnt de website van de Fraudehelpdesk bij 90 zoektermen (bijna 60%) op de eerste resultatenpagina, bij 31 zoektermen (ongeveer 20%) op de eerste tien pagina's en bij 32 zoektermen (ongeveer 20%) niet op één van de eerste tien pagina's.¹⁴⁴ Als het gaat om een zoekterm over een bepaald type fraude in combinatie met een term als 'melden' verschijnt de website van de Fraudehelpdesk in de meeste gevallen (42 van de 47 zoektermen) op de eerste resultatenpagina in Google. Alleen bij de zoektermen 'ransomware melden', 'telenet hacking melden', 'tikkie fraude melden', 'verzekeringsfraude melden' en 'identiteitsfraude melden' verschijnt de Fraudehelpdesk niet op de eerste resultatenpagina in Google.

Daarnaast blijkt uit bijlage 6 dat van de elf zoektermen met het hoogste gemiddelde zoekvolume per maand, de website van de Fraudehelpdesk twee keer op de eerste positie in Google verschijnt, drie keer binnen de eerste tien pagina's en zes keer niet binnen de eerste tien pagina's.¹⁴⁵ In onderstaande tabel zijn deze zoektermen weergegeven. In de tabel valt af te lezen dat voor de termen 'fraude melden' en 'phising mail' de website van de Fraudehelpdesk als eerste resultaat in Google verschijnt.

¹⁴⁴ De termen 'datingfraude' en 'datingfraude melden' zijn niet meegenomen in het websiteonderzoek, maar handmatig opgezocht. De website van de Fraudehelpdesk verschijnt bij die termen ook op de eerste pagina in Google.

¹⁴⁵ Zit zijn elf zoektermen met gemiddeld zoekvolume van 1.000 of hoger per maand.

TABEL 4.6: ZICHTBAARHEID VAN FRAUDEHELPDESK BIJ ZOEKTERMEN MET HET HOOGSTE ZOEKVOLUME

Zoekterm	Gemiddeld zoekvolume p/m	Positie Google	Zichtbaarheid
spoofing betekenis	1000	19	Zichtbaar op positie 11 tot en met 100
cybercrime	1000	101	Niet zichtbaar binnen positie 1 tot en met 100
fraude melden	1300	1	Zichtbaar op positie 1 tot en met 10
skimmen	1900	101	Niet zichtbaar binnen positie 1 tot en met 100
ponzifraude	2400	101	Niet zichtbaar binnen positie 1 tot en met 100
phishing mail	3600	1	Zichtbaar op positie 1 tot en met 10
malware	3600	101	Niet zichtbaar binnen positie 1 tot en met 100
ransomware	3600	101	Niet zichtbaar binnen positie 1 tot en met 100
spoofing	5400	16	Zichtbaar op positie 11 tot en met 100
phishing	8100	15	Zichtbaar op positie 11 tot en met 100
hacking	14800	101	Niet zichtbaar binnen positie 1 tot en met 100

Daarnaast blijkt uit bijlage 6 dat zoektermen in relatie tot acquisitiefraude goed vindbaar zijn. Van de dertig zoektermen in relatie tot acquisitiefraude verschijnt de website van de Fraudehulpdesk op 29 van de dertig zoektermen op de eerste resultatenpagina in Google. Alleen de zoekterm 'factuurfraude' verschijnt niet op de eerste pagina, maar wel binnen de eerste tien pagina's in Google.

Zoals gezegd blijkt uit bijlage 6 dat voor 32 zoektermen de website van de Fraudehulpdesk niet zichtbaar is binnen de eerste tien pagina's van Google. De Fraudehulpdesk blijkt niet goed zichtbaar te zijn bij zoektermen in de categorie 'beleggingsfraude'. Er is binnen die categorie gekeken naar de volgende zoektermen: 'boilerroomfraude', 'wat is boilerroomfraude', 'ponzifraude', 'piramidespel opgelicht', 'piramidefraude'. Bij geen van de onderzochte zoektermen blijkt de Fraudehulpdesk zichtbaar binnen de eerste tien resultatenpagina's van Google. Daarnaast blijkt de Fraudehulpdesk niet goed zichtbaar te zijn voor zoektermen over ransomware, skimmen, cybercrime, malware, spoofing, hacking en smishing.¹⁴⁶ Hierbij wordt opgemerkt dat de website van de Fraudehulpdesk dan wel weer vindbaar is voor deze zoektermen in combinatie met 'melden'.¹⁴⁷

4.4.1 Vindbaarheid van de website van de Fraudehulpdesk op websites van ketenpartners

Ketenpartners van de Fraudehulpdesk verwijzen in de meeste gevallen op hun website naar de website van de Fraudehulpdesk. In tabel 4.7 is aangegeven hoeveel muisklikken nodig zijn om vanaf de eerste pagina van een website op een pagina te komen met een verwijzing naar de website van de Fraudehulpdesk. Op geen van de websites van ketenpartners wordt op de eerste pagina verwezen naar website van de Fraudehulpdesk. Op twee websites is geen verwijzing gevonden naar de website van de Fraudehulpdesk en op twee websites werd wel in nieuwsberichten naar de Fraudehulpdesk verwezen, maar niet op een vaste pagina op de website zelf.

¹⁴⁶ Zie bijlage 9 voor een overzicht van definities van fraudevormen.

¹⁴⁷ De Fraudehulpdesk is wel goed vindbaar voor de volgende termen: cybercrime melden, malware melden, malware mail melden, spoof melden, spoofing melden, spoofing telefoonnummer melden, hack melden, hackers melden, hacking melden en smishing melden.

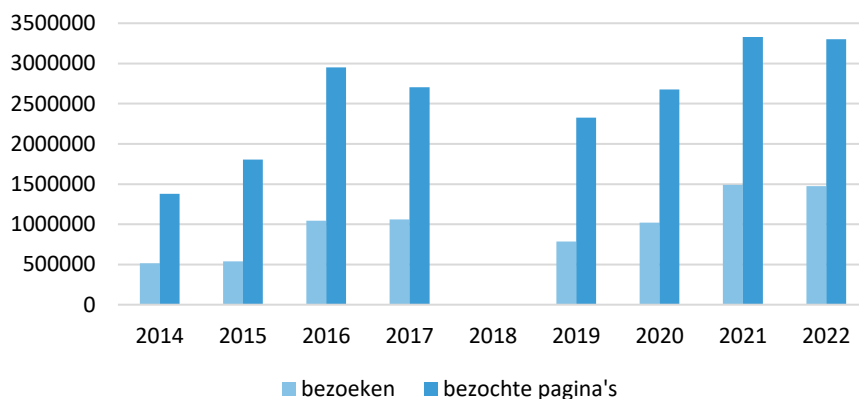
TABEL 4.7: VINDBAARHEID WEBSITE VIA WEBSITES VAN KETENPARTNERS¹⁴⁸

Ketenpartner	Aantal klikken
Autoriteit Consument en Markt	4 keer klikken
Autoriteit Financiële Markten	3 keer klikken
Centrum voor Criminaliteitspreventie en Veiligheid	3 keer klikken
De Algemene Bond voor Ouderen	3 keer klikken
Europees Consumenten Centrum	3 keer klikken
ESET Nederland (internetbeveiligingsorganisatie)	-
Nederlandse Vereniging van Banken	-
Openbaar Ministerie	2 klikken
Politie	3 klikken
Slachtofferhulp Nederland	4 klikken
The Hague security Delta	via nieuwsberichten
VNO-NCW en MKB Nederland	via nieuwberichten

In de evaluatie van de Fraudehelpdesk in 2012 is ook gekeken of ketenpartners met een link op hun website doorverwijzen naar de website van de Fraudehelpdesk. De onderzoekers constateerden toen dat op minder dan de helft (8 van de 19) van de websites van ketenpartners werd doorverwezen naar de Fraudehelpdesk.

4.5 Bezoekers website

Het aantal websitebezoekers en het aantal bezochte pagina's is in figuur 4.8 weergegeven

FIGUUR 4.8: WEBSITEBEZOEKERS¹⁴⁹

¹⁴⁸ De vindbaarheid van de website van de Fraudehelpdesk via websites van ketenpartners is uitgevoerd op 11 mei 2023.

¹⁴⁹ Cijfers zijn aangeleverd door de Fraudehelpdesk. Van 2011 tot en met 2013 hebben we geen registraties over het aantal websitebezoekers van de Fraudehelpdesk ontvangen. Ook in de jaarverslagen van 2011 tot en met 2013 zijn geen registraties over het aantal websitebezoekers opgenomen. Ook van 2018 hebben we geen registraties ontvangen van de Fraudehelpdesk. Uit het jaarverslag blijkt dat in 2018 het aantal bezoekers, met ruim een miljoen, vrijwel gelijk was aan 2017. De registraties die wij van de Fraudehelpdesk hebben ontvangen over 2022 wijken iets af van de registraties die in het jaarverslag van 2022 zijn opgenomen. Volgens het jaarverslag 2022 hebben er 1.441.893 unieke personen de website geraadpleegd die zorgen voor 3.253.590 pagina-bezoeken.

Uit het figuur valt af te lezen dat het aantal websitebezoekers en bezochte pagina's in 2016 bijna verdubbelde ten opzichte van 2015. Een van de redenen voor deze toename zou volgens de Fraudehelpdesk kunnen zijn dat in 2016 voor het eerst twaalf maanden met een voltijds-webredacteur werd gewerkt. Daarnaast zou de bekendheid van de Fraudehelpdesk verder gegroeid zijn. Deze ontwikkelingen zorgden er volgens de Fraudehelpdesk voor dat bezoekers steeds meer via Facebook en andere sociale media op de website terechtkomen.¹⁵⁰ In maart 2019 is een nieuwe website gelanceerd en waren er minder bezoekers op de website dan in 2018, zo blijkt uit het jaarverslag. Het aantal meldingen daarentegen was wel hoger dan in 2018 (zie paragraaf 3.4.2). In 2020 groeide het aantal website bezoekers met ongeveer 30% ten opzichte van 2019. Een reden hiervoor kan zijn dat de doorontwikkeling van een gebruiksvriendelijke website met bruikbare handelingsperspectieven en toegankelijke meldformulieren in 2020 verder is voortgezet.¹⁵¹ Deze groei zette ook in 2021 door met ongeveer 25% ten opzichte van 2020. Het aantal bezoekers en bezochte pagina's was in 2022 nagenoeg gelijk aan het aantal bezoekers uit 2021.

4.6 Conclusie

In dit hoofdstuk stond de bekendheid van de Fraudehelpdesk centraal. Om de bekendheid te onderzoeken is gekeken naar de naamsbekendheid en de zichtbaarheid van de website van de Fraudehelpdesk. De Fraudehelpdesk laat eens in de twee jaar door een extern bureau onderzoek uitvoeren naar de naamsbekendheid van de Fraudehelpdesk. Deze onderzoeken zijn naast elkaar gelegd om inzicht te krijgen in de ontwikkeling van de naamsbekendheid door de jaren heen. Onderscheid kan daarbij worden gemaakt tussen top-of-mind naamsbekendheid, spontane naamsbekendheid en geholpen naamsbekendheid. Er is enige twijfel over de betrouwbaarheid van de onderzoeken omdat deze in opdracht van de Fraudehelpdesk zijn uitgevoerd en niet volledige duidelijkheid is verkregen over de wijze waarop de onderzoeken zijn uitgevoerd. Dat neemt niet weg dat voor particulieren een stijgende trend te zien is in zowel de top-of-mind naamsbekendheid als de spontane en de geholpen naamsbekendheid van de Fraudehelpdesk. Onderzoek naar de naamsbekendheid onder ondernemers is alleen in 2020 uitgevoerd, waardoor geen uitspraken kunnen worden gedaan over de ontwikkeling van de naamsbekendheid onder ondernemers. Wel kan een vergelijking worden gemaakt met de naamsbekendheid onder particulieren. Daaruit blijkt dat de top-of-mind naamsbekendheid vier procent lager ligt ten opzichte van particulieren, de spontane naamsbekendheid onder ondernemers nagenoeg gelijk is aan dat van particulieren en de geholpen naamsbekendheid bijna tien procent hoger is dan die van particulieren.

Met betrekking tot de zichtbaarheid van de website van de Fraudehelpdesk kan worden gezegd dat deze over het algemeen goed zichtbaar is. Om de zichtbaarheid te beoordelen is onderscheid gemaakt tussen zoektermen waarop de website goed zichtbaar is (positie 1 tot en met 10 in Google), zoektermen waar de Fraudehelpdesk iets minder goed zichtbaar is, maar wel te vinden (positie 11 tot en met 100 Google), en zoektermen waarop de website slecht zichtbaar is (positie 101 en verder in Google). Op 60% van de onderzochte zoektermen is de website goed zichtbaar. De website is met name goed zichtbaar op zoektermen over een bepaalde vorm van fraude in combinatie met het woord 'melden'. Het is goed voorstelbaar dat

¹⁵⁰ Jaarverslag 2016, p. 11.

¹⁵¹ Jaarverslag 2020, p.14.

burgers of ondernemers juist ook op die termen zoeken als zij met fraude te maken hebben gehad. Bij de zoektermen die in dit onderzoek zijn meegenomen en waar per maand het vaakst op wordt gezocht, is de website voor het merendeel niet zichtbaar op positie 1 tot en met 10. Het gaat in die gevallen om meer algemene zoektermen over online vormen van fraude zoals hacking, malware en spoofing. Dat de Fraudehelpdesk op deze zoektermen minder goed zichtbaar is, is niet verwonderlijk. Bij zoektermen met een hoog zoekvolume is de concurrentie om op een hoge positie te komen immers hoger en is het daardoor moeilijker om hoog in de zoekresultaten te verschijnen. Daarnaast kunnen mensen die op algemene termen zoals 'hacking' en 'phishing' zoeken ook andere bedoelingen hebben en is het de vraag of de website dan ook zichtbaar moet zijn.

We hebben ook gekeken in hoeverre de website van de Fraudehelpdesk vindbaar is via de websites van ketenpartners. Hieruit blijkt dat op geen van de websites van ketenpartners op de eerste pagina wordt verwezen naar website van de Fraudehelpdesk. Bij het merendeel van de andere websites van ketenpartners is wel een link opgenomen op een pagina naar de website van de Fraudehelpdesk, maar zijn hiervoor ongeveer 3 muislikken nodig.

Ten slotte is ook gekeken naar de ontwikkeling van het aantal websitebezoekers. Hieruit blijkt dat het aantal websitebezoekers in 2022 ongeveer drie keer zo groot was als het aantal websitebezoekers in 2014. Wel lijkt het aantal bezoekers en bezochte pagina's de laatste jaren te zijn gestabiliseerd dan wel licht te zijn verminderd.

5 Waardering van de Fraudehelpdesk

5.1 Inleiding

De mate waarin de Fraudehelpdesk wordt gewaardeerd door melders en ketenpartners staat in dit hoofdstuk centraal (deelvraag 7b, 8 - 11). Paragraaf 5.2 bevat een toelichting op de respons en verantwoording van het vragenlijstonderzoek. In paragraaf 5.3 worden de resultaten van het vragenlijstonderzoek onder melders gepresenteerd. Paragraaf 5.4 bevat een verslag van de gesprekken die zijn gevoerd met ketenpartners over hun waardering van de Fraudehelpdesk. In paragraaf 5.5 is een conclusie van dit hoofdstuk opgenomen.

5.2 Respons en verantwoording vragenlijstonderzoek

Om de waardering van de dienstverlening van de Fraudehelpdesk onder melders in kaart te brengen, is onder deze doelgroep een digitale vragenlijst uitgezet. Dit is gedaan onder alle melders die tussen 3 mei en 21 mei 2023 en tussen 28 juni en 18 juli 2023 melding hebben gedaan en bij de melding aangaven mee te willen werken aan een vragenlijstonderzoek. Deze melders ontvingen van de Fraudehelpdesk drie weken nadat zij een melding hadden gedaan een e-mail met een uitnodiging om deel te nemen aan ons vragenlijstonderzoek. In deze e-mail was een link naar de vragenlijst opgenomen. De vragenlijst is gebouwd in het programma LimeSurvey. De Fraudehelpdesk had geen toegang tot de respons, maar verstuurd alleen een uitnodiging naar deelnemers om de vragenlijst in te vullen. De respons op de vragenlijst is in tabel 5.1 weergegeven. Van de melders die alleen de vragenlijst hebben geopend of alleen de introductievragen hebben ingevuld, is de respons niet meegenomen. Niet elke respondent heeft alle vragen ingevuld, waardoor de respons per vraag kan verschillen. In totaal zijn in de periode tussen 3 mei en 21 mei en 28 juni en 18 juli 2023 5.280 meldingen ontvangen. Bij deze populatie en 361 volledig ingevulde vragenlijsten, kunnen we uitgaan van een foutenmarge van 5%.

TABEL 5.1: RESPONS VRAGENLIJST

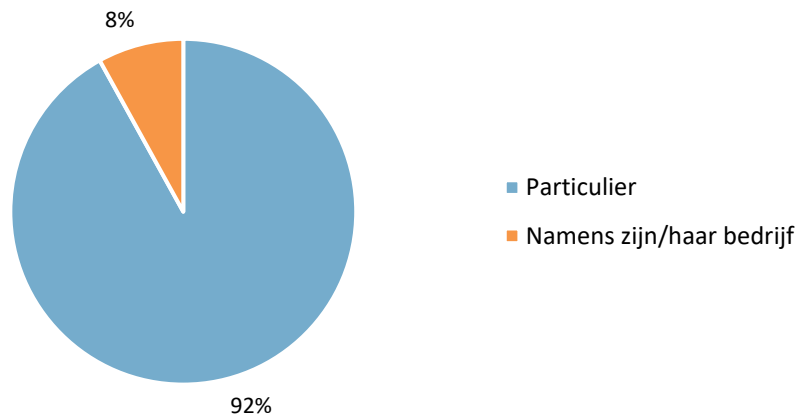
	Absolute aantallen	Percentage
Uitgezette vragenlijsten	1.842	100%
Non-respons	1.381	75%
Vragenlijst alleen geopend of alleen de introductievragen ingevuld	49	3%
Deels of volledig ingevulde vragenlijsten	412	22%
Volledig ingevuld	361	20%
Deels ingevuld	51	2%

5.3 Waardering door melders

5.3.1 Achtergrond respondenten

Respondenten is gevraagd of zij als particulier of namens hun bedrijf een melding hebben gedaan bij de Fraudehelpdesk. Het overgrote merendeel van de respondenten deed een melding als particulier.

FIGUUR 5.2: ACHTERGROND RESPONDENTEN (N=361)



5.3.2 De melding

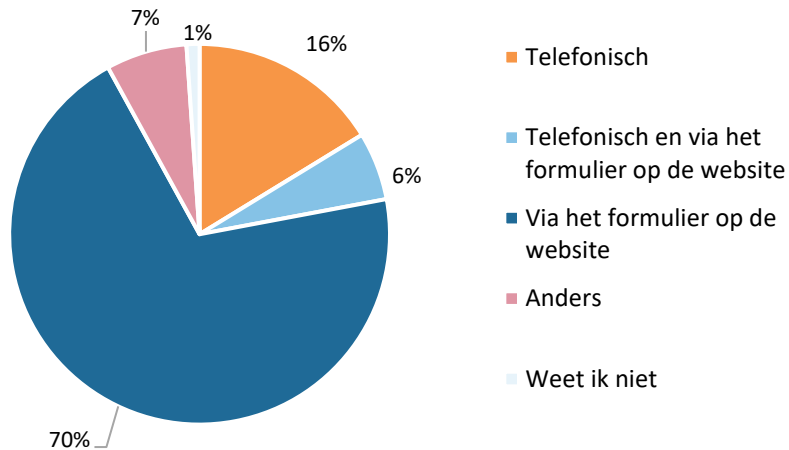
Vervolgens is de respondenten gevraagd op welke wijze zij een melding hebben gedaan. Uit figuur 5.3 blijkt dat bijna driekwart van de respondenten (alleen) een melding heeft gedaan via het formulier op de website van de Fraudehelpdesk.¹⁵² Het aantal respondenten dat telefonisch melding heeft gedaan is relatief gezien kleiner dan het aandeel melders dat telefonisch melding heeft gedaan in 2022 (zie figuur 3.3). Een reden hiervoor kan zijn dat mensen die digitaal een melding doen eerder geneigd zijn een digitale vragenlijst in te vullen, dan respondenten die telefonisch een melding doen.¹⁵³

¹⁵² Uit antwoorden van een aantal respondenten blijkt dat als zij hebben aangegeven op 'andere' wijze meldingen te hebben gedaan, zij dit via een e-mail hebben gedaan.

¹⁵³ In de coronaperiode was de telefonische helpdesk meerdere malen tijdelijk gesloten, waardoor de verhouding tussen het aantal telefonische en digitale meldingen in die jaren waarschijnlijk anders lag.

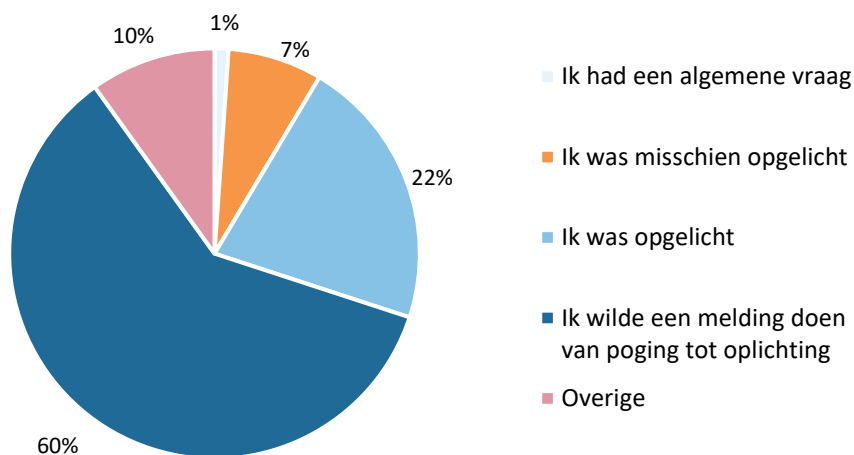
Wanneer respondenten aangeven te zijn opgelicht (figuur 5.4) lijken zij relatief gezien vaker telefonisch een melding te doen. Van het aantal respondenten dat was opgelicht deed meer dan een kwart van de respondenten (27%) hiervan alleen telefonisch melding, terwijl van het totaal aantal respondenten 7% alleen telefonisch een melding deed.

FIGUUR 5.3: WIJZE VAN MELDEN (N=363)



Daarnaast is gevraagd naar de reden waarom contact is gezocht met de Fraudehelpdesk. Uit figuur 5.4 blijkt dat de meeste respondenten (60%) een melding wilden doen van een poging tot oplichting. Ruim een kwart van de respondenten was (misschien) opgelicht.

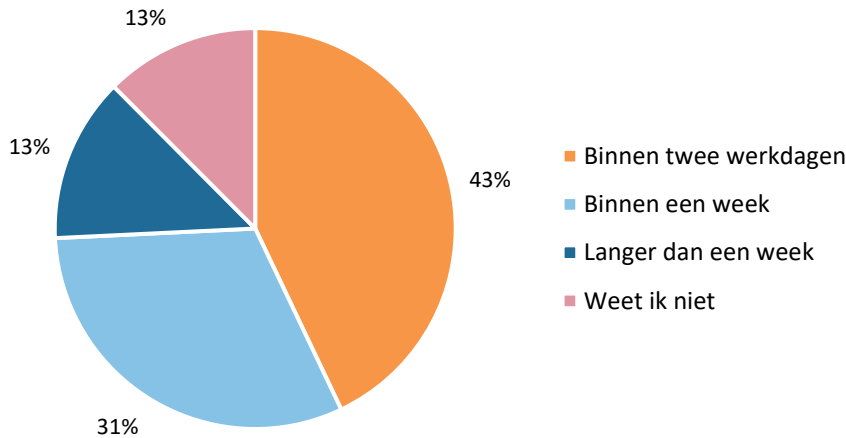
FIGUUR 5.4: REDEN VAN DE MELDING (N=363)



5.3.3 Reactietermijn

Respondenten is gevraagd binnen welke termijn hun melding werd beantwoord. Minder dan de helft (43%) van de respondenten ontving binnen twee werkdagen reactie op hun melding. Bijna een derde (31%) van de respondenten ontving binnen een week reactie van de Fraudehelpdesk.

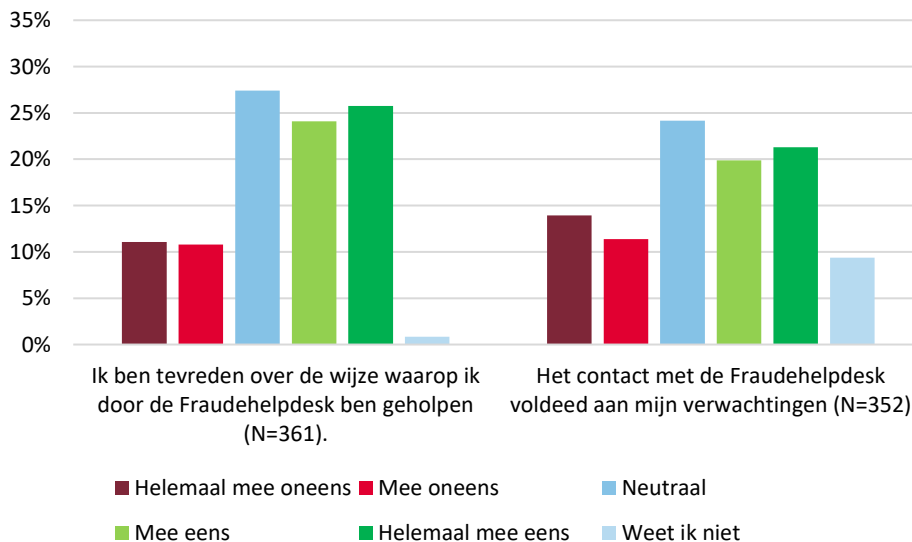
FIGUUR 5.5: REACTIETERMIJN (N=361)



5.3.4 Tevredenheid dienstverlening

Vervolgens zijn melders een aantal stellingen voorgelegd met betrekking tot de tevredenheid over de dienstverlening van de Fraudehelpdesk.

FIGUUR 5.6: STELLINGEN OVER DE TEVREDENHEID VAN DE DIENSTVERLENING



Uit figuur 5.6 blijkt dat de 22% van de respondenten (zeer) ontevreden is over de wijze waarop ze door de Fraudehelpdesk zijn geholpen. De helft van de respondenten is juist (zeer) tevreden over de wijze waarop ze door de Fraudehelpdesk zijn geholpen. Er lijkt geen verband te zijn tussen de reden van melding en de algemene tevredenheid over de wijze waarop een respondent door de Fraudehelpdesk is geholpen. Zo zijn van de 78 respondenten die aangaven te zijn opgelicht, 38 van de respondenten (zeer) tevreden over de wijze waarop zij zijn geholpen. Later in dit hoofdstuk wordt een stelling toegelicht over of respondenten die zijn doorverwezen naar een andere organisatie, het gevoel hebben dat zij naar de juiste organisatie zijn doorverwezen. Van de 21 respondenten die aangeven niet het gevoel te hebben naar de juiste

organisatie te zijn doorverwezen, is meer dan de helft (14 respondenten) (zeer) ontevreden over de wijze waarop zij door de Fraudehelpdesk zijn geholpen.

Uit de toelichting van respondenten op waarom zij ontevreden waren, blijkt dat de melders een andere verwachting hadden van de dienstverlening door de Fraudehelpdesk en dat dit voor een groot deel te maken heeft met het feit dat zij geen telefoonnummers van oplichters mochten doorgeven en/of er door de Fraudehelpdesk geen actie werd ondernomen. Het niet ondernemen van actie naar aanleiding van een melding kan ook reden zijn voor slachtoffers om helemaal geen melding te doen. In het onderzoek van Akkermans e.a. is slachtoffers gevraagd naar de reden waarom zij geen melding of aangifte bij de Politie hebben gedaan. De meest genoemde reden om geen melding of aangifte bij de Politie te doen waren dat het 'toch niets helpt' of dat 'er niet aan gedacht was/het niet zo belangrijk was'.¹⁵⁴ Een uitzondering hierop was dat bij fraude in het betalingsverkeer vaak werd aangegeven dat de financiële schade al was vergoed of dat het al was opgelost.

Bij minder dan de helft van de respondenten (41%) voldeed het contact met de Fraudehelpdesk aan de verwachtingen, en bij een kwart (25%) voldeed het contact niet aan de verwachtingen.

5.3.5 Waardering dienstverlening van de medewerkers

Respondenten is een drietal stellingen voorgelegd over de medewerkers van de Fraudehelpdesk. Bij de stellingen over de medewerkers gaf een groot deel het antwoord 'weet ik niet'. Dit waren veelal respondenten die alleen een melding via het formulier op de website hebben ingevuld en daardoor geen telefonisch contact hadden met een medewerker. Van de respondenten die de stellingen over vriendelijkheid, deskundigheid en hulpvaardigheid hebben ingevuld, heeft 69% respondenten alleen melding gedaan via het meldformulier op de website van de Fraudehelpdesk. 58% tot 60% van de respondenten die alleen melding heeft gedaan via het meldformulier op de website heeft het antwoord 'neutraal' of 'weet ik niet' ingevuld.

Van de respondenten die contact hebben gehad met een medewerker van de Fraudehelpdesk, wordt de vriendelijkheid van de medewerker beoordeeld met gemiddeld een 7.7, de deskundigheid van de medewerker met een 7.5 en de hulpvaardigheid van de medewerker met een 7.4.¹⁵⁵

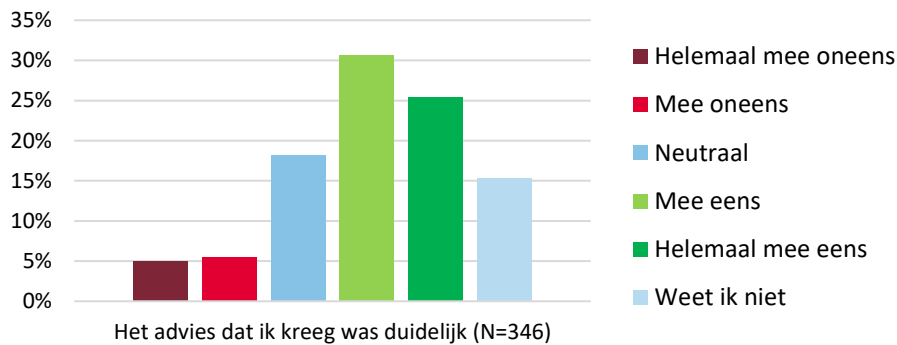
5.3.6 Advies van de Fraudehelpdesk

De laatste stelling over de dienstverlening van de Fraudehelpdesk ging over de duidelijk van het advies dat de melder had ontvangen. Meer dan de helft van de respondenten (56%) vindt dat het advies dat zij kregen duidelijk was. 10% van de respondenten was het (helemaal) oneens met de stelling dat het advies dat de respondent kreeg, duidelijk was.

¹⁵⁴ Akkermans e.a. 2022, par. 4.3.1.

¹⁵⁵ N=338-344; 28 tot 31 procent van de respondenten beantwoordde de stellingen over de medewerker met 'weet ik niet', Respondenten konden stellingen over medewerkers beantwoorden aan de hand van de antwoordcategorieën 'helemaal oneens' tot 'helemaal mee eens'. Dit is omgerekend naar een gemiddeld cijfer waarbij 'helemaal oneens' staat voor een 2 en 'helemaal mee eens' staat voor een 10.

FIGUUR 5.7: STELLING OVER DUIDELIJKHEID VAN HET ADVIES



5.3.7 Doorverwijzingen

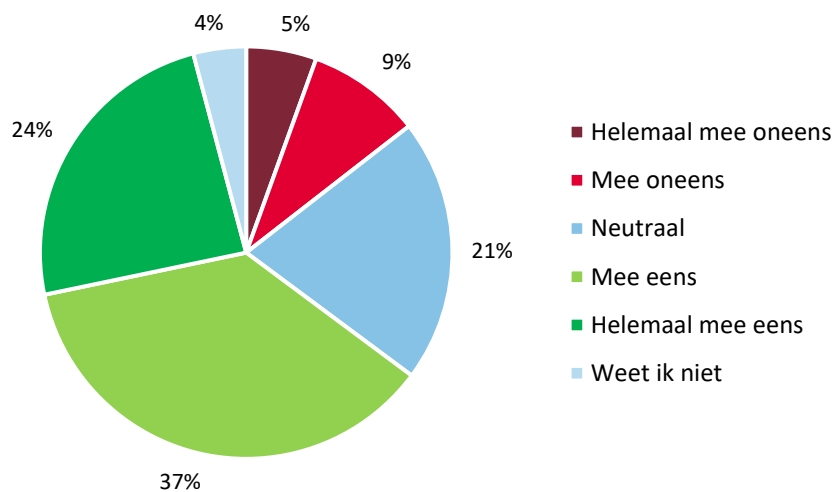
Aan respondenten is de vraag gesteld of de Fraudehelpdesk hen heeft doorverwezen naar een andere organisatie.

TABEL 5.8: DOORVERWIJZINGEN (N=363)

	Aantal	Percentage
Ja	148	41%
Nee	189	52%
Weet ik niet	26	7%

De respondenten die aangaven te zijn doorverwezen is vervolgens gevraagd of zij het gevoel hebben dat zij naar de juiste organisatie zijn doorverwezen. Ruim 60% van de respondenten geeft aan het gevoel te hebben naar de juiste organisatie te zijn doorverwezen.

FIGUUR 5.9: IK HEB HET GEVOEL DAT IK NAAR DE JUISTE ORGANISATIE BEN DOORVERWEZEN (N=145).



Respondenten die aangaven niet het gevoel te hebben naar de juiste organisatie te zijn doorverwezen, konden hun antwoord toelichten. Respondenten zijn het voornamelijk met de stelling oneens omdat er niets met hun melding werd gedaan. Enkele respondenten verwijten de

Fraudehelpdesk of de ketenpartner naar wie zij zijn doorgestuurd, het gebrek aan actie of verdere hulp.

5.3.8 Suggesties ter verbetering van de dienstverlening

Respondenten is in de vragenlijst gevraagd welke suggesties zij hebben ter verbetering van de dienstverlening van de Fraudehelpdesk. Daarnaast is in tien aanvullende interviews met melders ook aandacht besteed aan de vraag welke suggesties respondenten hebben om de dienstverlening te verbeteren. De voorbeelden die door enkele respondenten worden genoemd en hieronder zijn toegelicht, dienen ter illustratie. Hieronder zijn de verbetermogelijkheden gecategoriseerd weergegeven.

Terugkoppeling en verwachtingsmanagement

Er zijn enkele verbetervoorstellen van respondenten over de terugkoppeling naar aanleiding van hun melding. Een van de respondenten geeft aan dat de Fraudehelpdesk adequater kan reageren door het direct toesturen van een automatische antwoordmail met hoe te handelen. Daarnaast geven meerdere respondenten aan dat aan de voorkant beter kan worden aangegeven wat een melder kan verwachten bij het doen van een melding (verwachtingsmanagement). Op die manier is duidelijk wat er met een melding wordt gedaan. De Fraudehelpdesk besteedt hier wel aandacht aan op de website in onder meer een animatiefilmpje. Ook geeft een respondent aan behoefte te hebben aan een periodieke terugkoppeling over de meldingen die de Fraudehelpdesk ontvangt. Dit zou mensen motiveren om melding (te blijven) doen.

Aanpakken van fraudezaken en doorverwijzen

Meerdere respondenten geven aan dat de Fraudehelpdesk zelf actie had moeten ondernemen, in plaats van dat hun melding alleen wordt geregistreerd en dat zij worden doorverwezen. Enkele respondenten geven aan dat het enkel doorverwijzen voor hen geen toegevoegde waarde heeft. Daarnaast geeft een van de respondenten aan dat hij erachter kwam dat de Fraudehelpdesk geen telefoonnummer mag registreren van de persoon die hem probeerde op te lichten. De respondent geeft aan dat de melding bij de Fraudehelpdesk daarom zinloos is. In een van de telefonische interviews geeft een respondent aan dat de drempel om nog een keer een melding hoger is, nu duidelijk is dat de Fraudehelpdesk niets kan doen.

Enkele respondenten zijn door de politie doorverwezen naar de Fraudehelpdesk en andersom. Een respondent had hierdoor het gevoel van het kastje naar de muur te worden gestuurd. Een andere respondent merkt op dat het zinvol zou zijn om in een database meldingen van de Fraudehelpdesk te koppelen aan gegevens van de politie. Daarnaast geeft een respondent aan niet door te hebben dat de Fraudehelpdesk alleen doorverwijst.

Algemene dienstverlening

Enkele respondenten doen een suggestie om de bereikbaarheid te verbeteren. Zo geeft een van de respondenten aan dat de Fraudehelpdesk niet bereikbaar was op een feestdag. Een andere respondent geeft aan dat het wenselijk zou zijn dat de Fraudehelpdesk langer bereikbaar is. Deze respondent heeft, omdat hij geen contact kreeg, de politie gebeld. In een van de telefonische interviews geeft een ondernemer aan dat de Fraudehelpdesk zich in de informatieverstrekking meer op ondernemers zou kunnen richten. Het is voor ondernemers relevant om te weten met welk type fraude zij te maken kunnen krijgen.

5.4 Waardering door ketenpartners

Deze paragraaf bevat de bevindingen op basis van gesprekken die zijn gevoerd met 17 geïnterviewden bij in totaal veertien ketenpartners. In bijlage 3 is een overzicht opgenomen van de gesprekspartners.

5.4.1 Contact met ketenpartners

De Fraudehelpdesk werkt met verschillende ketenpartners samen; daarbij verschilt het per organisatie hoe intensief die samenwerking is. Een merendeel van de ketenpartners heeft geen structureel periodiek contact met de Fraudehelpdesk. Wel vindt er minimaal één keer per jaar op directieniveau overleg plaats over trends en ontwikkelingen en wordt er gekeken op welke gebieden samen kan worden opgetrokken. Het contact tussen ketenpartners en de Fraudehelpdesk vindt verder vooral op ad hoc basis plaats. Daarbij wordt afgestemd over een gezamenlijk op te zetten campagne of de aanwezigheid bij (te organiseren) bijeenkomsten. Ook worden trends en ontwikkelingen besproken.

Alle gesprekspartners zijn positief over het contact dat zij met de Fraudehelpdesk hebben. Vrijwel alle ketenpartners hebben één of meer vaste contactpersonen bij de Fraudehelpdesk om mee af te stemmen; de lijntjes zijn kort en ketenpartners en de Fraudehelpdesk weten elkaar goed te vinden. Het contact wordt ook door alle gesprekspartners als prettig en zinvol ervaren. Een enkele gesprekspartner geeft als kanttekening aan dat het contact de afgelopen jaren iets minder intensief is geworden, doordat het landschap waarbinnen de Fraudehelpdesk functioneert is veranderd (er zijn veel meer meldpunten/organisaties die voorlichting geven bijgekomen) en de Fraudehelpdesk bepaalde gegevens (persoonsgegevens van strafrechtelijke aard) niet meer mag registreren en delen met ketenpartners.

5.4.2 Verhouding taken en werkzaamheden ketenpartners en Fraudehelpdesk

De ketenpartners en de Fraudehelpdesk hebben vaak andere kerntaken en doelstellingen. Uit de interviews blijkt dat het merendeel van de ketenpartners ook aan (enige) registratie en preventie (vooral het geven van voorlichting) doet. De Fraudehelpdesk zit wat betreft het voorkomen en bestrijden van fraude alleen aan het begin van de keten; zij geeft voorlichting, registreert meldingen, verwijst melders door en signaleert ontwikkelingen/trends. Het verschilt per ketenpartner of en zo ja in welke mate hun taken en werkzaamheden met die van de Fraudehelpdesk overeenkomen. Er zijn ketenpartners die inhoudelijk geen fraudezaken oppakken, maar meldingen wel registreren, voorlichting geven en/of aan bemiddeling doen. De voorlichting bestaat dan vaak uit het verstrekken van informatie en het opzetten van campagnes. Wat betreft die taken en werkzaamheden is er enige overlap met de Fraudehelpdesk. Wel zijn de ketenpartners van mening dat, daar waar die overlap zich voordoet, zij en de Fraudehelpdesk elkaar qua werkzaamheden versterken. Er wordt onderling afgestemd over hoe bijvoorbeeld het geven van voorlichting het beste kan worden ingestoken.

Er zijn ook ketenpartners die ook of alleen maar fraudemeldingen inhoudelijk oppakken. Een melding bij die ketenpartner kan dan leiden tot handhaving (het opleggen van bijvoorbeeld een last onder dwangsom of boete) of strafrechtelijke vervolging. Bij deze ketenpartners ligt wat betreft taken en werkzaamheden de nadruk niet op preventie en verschilt hun rol bij het voorkomen en bestrijden van fraude wezenlijk van die van de Fraudehelpdesk.

5.4.3 Beoordeling dienstverlening en draagvlak in de keten

Uit de interviews volgt dat vrijwel alle ketenpartners de dienstverlening door de Fraudehelpdesk positief beoordelen. Volgens meerdere gesprekspartners is er op de Fraudehelpdesk na geen enkel meldpunt dat zoveel kennis over fraude in huis heeft, trends en ontwikkelingen signaleert en daarover rapporteert. De Fraudehelpdesk neemt volgens hen in het landschap een unieke positie in. Ook geven gesprekspartners aan dat de informatie die de Fraudehelpdesk met hen deelt waardevol is, dat die informatie hen helpt om signalen tijdig op te pakken en dat de Fraudehelpdesk aan actuele thema's aandacht besteedt. De valse e-mailcheck wordt door een merendeel van de gesprekspartners ook positief beoordeeld en voor verschillende ketenpartners is de maandmonitor en het jaarverslag interessant. De trends en ontwikkelingen die de Fraudehelpdesk signaleert komen volgens een merendeel van de gesprekspartners overeen met hetgeen de ketenpartners zelf zien.

Doorverwijzingen

Een meerderheid van de ketenpartners ontvangt van de Fraudehelpdesk doorverwijzingen. Slechts drie ketenpartners krijgen, in verband met hun taken en werkzaamheden, geen doorverwijzingen. Vrijwel alle ketenpartners verwijzen ook uit zichzelf naar de Fraudehelpdesk; zij geven dan richting de consument of ondernemer aan dat zij meer informatie kunnen verkrijgen bij de Fraudehelpdesk en/of daar ook een melding kunnen maken.

Met betrekking tot de doorverwijzingen wordt onderscheid gemaakt tussen koude en warme doorverwijzingen. Bij een koude doorverwijzing wordt de burger of ondernemer door de Fraudehelpdesk verwezen naar een ketenpartner. Bij vrijwel alle ketenpartners is sprake van koude doorverwijzingen, wat betekent dat het aan die burger of ondernemer zelf is om contact op te nemen met de ketenpartner. Wanneer de burger of ondernemer contact opneemt, pakt een merendeel van de ketenpartners de meldingen op. Het kan daarbij wel voorkomen dat er (gelet op de prioriteitstelling) eerst meerdere meldingen over een onderwerp binnen moeten komen, voordat een onderzoek wordt ingesteld. Bij een warme doorverwijzing ontvangt de ketenpartner van de Fraudehelpdesk informatie over de melder, zodat daarmee contact kan worden opgenomen. Hierbij worden geen gegevens over bijvoorbeeld de oplichter gedeeld. Slechts één ketenpartner ontvangt van de Fraudehelpdesk warme doorverwijzingen en een medewerker van die ketenpartner neemt dan contact op met de melder.

Expertisecentrum

Alle gesprekspartners benadrukken dat de Fraudehelpdesk veel kennis in huis heeft en goed zicht heeft op de verschillende vormen van fraude die kunnen worden onderscheiden. Het verschilt per ketenpartner of zij de Fraudehelpdesk ook als expertisecentrum zien. Enkele ketenpartners vinden dat de Fraudehelpdesk geen expertisecentrum is; de Fraudehelpdesk heeft volgens die gesprekspartners veel expertise in huis, maar is niet de enige en eerste organisatie waar burgers of ondernemers terecht kunnen en een melding van fraude maken.

Draagvlak Fraudehelpdesk in de keten

Alle ketenpartners zijn van mening dat de Fraudehelpdesk meerwaarde heeft op het gebied van preventie, zeker als het gaat om het geven van voorlichting. Vrijwel alle ketenpartners vinden dat de Fraudehelpdesk ook een belangrijke bijdrage levert wat betreft het signaleren van ontwikkelingen en dat de organisatie meerwaarde heeft doordat zij goed inspringt op

actualiteiten en veel kennis heeft over verschillende vormen van fraude. De interviews laten zien dat er onder ketenpartners veel draagvlak is voor het behouden van de Fraudehelpdesk.

5.4.4 Knelpunten

Ondanks dat er bij ketenpartners veel draagvlak is voor het behouden van de Fraudehelpdesk, zijn er een aantal punten die extra aandacht behoeven. Volgens ketenpartners zijn er vier knelpunten die de bijdrage van de Fraudehelpdesk aan de preventie en bestrijding van fraude hinderen of in de weg staan. Het gaat dan om het ontbreken van een centraal meldpunt, het niet meer mogen registreren en delen van bepaalde informatie door de Fraudehelpdesk, de kwetsbaarheid van de organisatie en het ontbreken van een eenduidige terminologie in de keten.

Knelpunt 1: een centraal meldpunt ontbreekt

De Fraudehelpdesk is één van de vele meldpunten en het ontbreken van een centraal meldpunt wordt door ketenpartners als een belangrijk knelpunt bij het voorkomen en bestrijden van fraude gezien. Gesprekspartners geven aan dat de naam 'Fraudehelpdesk' impliceert dat slachtoffers direct (inhoudelijk) worden geholpen. Dit terwijl de organisatie meldingen niet inhoudelijk mag behandelen en bepaalde informatie (bijvoorbeeld persoonsgegevens van de pleger) niet mag registreren en delen met ketenpartners. Verschillende ketenpartners benadrukken dat het belangrijk is dat slachtoffers van fraude zo snel mogelijk op de juiste plek terecht komen en worden geholpen. Met het huidige landschap is dat volgens hen lastig; volgens ketenpartners is het voor burgers en ondernemers niet altijd duidelijk waar zij als eerste terecht kunnen met hun melding en slachtoffers van fraude hebben behoefte aan concrete hulp. Enkele ketenpartners horen van burgers of ondernemers dat zij hun verhaal al verschillende keren hebben moeten vertellen, hetgeen als ongewenst wordt gezien.

Dat slachtoffers behoefte hebben aan praktische hulp (zoals het invullen van een formulier of het doen van aangifte) beaamen deelnemers aan de expertmeeting. Het lijkt volgens een van de deelnemers in het huidige landschap te ontbreken aan een partij die specifiek slachtoffers van fraude ondersteunt. Slachtoffers kunnen voor praktische hulp terecht bij Slachtofferhulp, maar deze organisatie snijdt zich niet alleen toe op fraude. Homburg en Van den Tillaart constateerden in hun onderzoek uit 2015 ook al dat er destijds organisaties waren ingericht om praktische ondersteuning te bieden, maar dat die organisaties zich niet specifiek richtten op fraudeslachtoffers.¹⁵⁶

Het ontbreken van één centraal meldpunt heeft ook tot gevolg dat informatie die van belang is voor het voorkomen en bestrijden van fraude bij verschillende organisaties ligt. Een meerderheid van de ketenpartners geeft aan dat de informatie van de Fraudehelpdesk zeker relevant is, maar geen compleet beeld geeft van het aantal fraudemeldingen e.d. Enkele ketenpartners vinden dat de Fraudehelpdesk wat dat betreft een rol en meerwaarde kan hebben, in die zin dat de organisatie de verschillende betrokken partijen en de bij hen beschikbare informatie bij elkaar brengt. Nu de online (digitale) criminaliteit steeds groter wordt, is er volgens gesprekspartners behoefte aan één coördinatiepunt wat betreft meldingen en informatie, zodat voldoende zicht en grip op verschillende vormen van fraude kan worden gehouden.

¹⁵⁶ Homburg en Van den Tillaart 2015, p. 19.

Knelpunt 2: het niet mogen registreren en delen van bepaalde informatie

Verschillende ketenpartners zien de omstandigheid dat de Fraudehelpdesk geen persoonsgegevens van strafrechtelijke aard mag delen ook als knelpunt bij het voorkomen en bestrijden van fraude. Deze gesprekspartners vinden dat de effectiviteit van de Fraudehelpdesk hierdoor wordt beperkt. Voor een enkele ketenpartner in de strafrechtelijke keten is de Fraudehelpdesk, vanwege het niet mogen delen van die informatie, een minder interessante samenwerkingspartner geworden. Die ketenpartners hebben behoefte aan concrete informatie over de pleger om meldingen (eventueel na een doorverwijzing) efficiënt op te kunnen pakken en zijn nu afhankelijk van de informatie die de burger of ondernemer aan hen verstrekt. Tijdens de expertmeeting hebben enkele ketenpartners aangegeven dat zij niet direct echt een taak voor de Fraudehelpdesk zien weggelegd in het aanpakken van fraudezaken door het delen van persoonsgegevens van strafrechtelijke aard. Deze ketenpartners vinden dat de Fraudehelpdesk zich beter kan richten op het verbeteren van de huidige dienstverlening, en op die manier de bijdrage aan fraudepreventie in Nederland kan verbeteren.

Knelpunt 3: kwetsbaarheid organisatie

Meerdere ketenpartners vinden de Fraudehelpdesk wat betreft het aantal werknemers en/of de subsidierelatie kwetsbaar. Zij maken zich zorgen over het budget dat de Fraudehelpdesk heeft om voorlichting te geven over bepaalde vormen van fraude en het voortbestaan van de organisatie. Verschillende ketenpartners vinden dat meer aandacht vanuit de overheid en financiële ondersteuning van de Fraudehelpdesk nodig is. Ook benadrukken ketenpartners dat de Fraudehelpdesk met een kleine groep werknemers ontzettend veel werk verricht en dat voldoende slagkracht in de toekomst bij het voorkomen en bestrijden van fraude belangrijk is.

Knelpunt 4: het ontbreken van eenduidige terminologie

Verschillende ketenpartners geven aan dat in de praktijk wat betreft fraude verschillende categorieën worden aangehouden en vaak ook andere termen worden gebruikt dan bijvoorbeeld in het strafrecht het geval is. Hierdoor is het lastig om de informatie die bij de verschillende organisaties voorhanden is met elkaar te vergelijken en te interpreteren. Het ontbreken van een eenduidige terminologie levert volgens ketenpartners dan ook een knelpunt op bij de preventie en bestrijding van fraude; het betreft in dit geval geen knelpunt ten aanzien van de Fraudehelpdesk, maar een knelpunt dat zich in de gehele keten voordoet.

Behoeftte aan eenduidige terminologie

In het kader van de integrale aanpak online fraude wordt gekeken of in ieder geval tussen de betrokken organisaties intern dezelfde terminologie kan worden gebruikt. Op die manier kunnen databestanden met elkaar worden vergeleken en daaruit relevante informatie worden verkregen. Gesprekspartners geven aan dat het verstandig is om met betrokken organisaties in algemene zin afspraken te maken, zodat intern en extern dezelfde categorieën worden aangehouden en dezelfde begrippen worden gebruikt. Enkele ketenpartners zien in dit kader ook een rol voor de Fraudehelpdesk weggelegd.

5.4.5 Uitdagingen en neveneffecten

Naast de knelpunten zien ketenpartners een aantal uitdagingen voor de Fraudehelpdesk. Meer dan ooit is, mede gelet op de digitalisering, volgens gesprekspartners het voorkomen van fraude belangrijk. De Fraudehelpdesk heeft daarin een rol, maar het voldoende zichtbaar blijven is en blijft volgens ketenpartners een uitdaging. Een enkele gesprekspartner geeft aan

dat de Fraudehelpdesk via allerlei kanalen zichtbaar moet zijn om in de toekomst voldoende vindbaar te zijn. Ook zou de Fraudehelpdesk via sociale media meer actief en gerichte voorlichting kunnen geven. Tijdens de expertmeeting is aangegeven dat de Fraudehelpdesk in het kader van preventie ook specifieke training zou kunnen aanbieden. Daarnaast is door een van de gesprekspartners opgemerkt dat een neveneffect van het opzetten en uitvoeren van campagnes over een bepaald onderwerp voor meer bewustzijn en aandacht zorgen waardoor het aantal meldingen over die vorm van fraude ook zou kunnen toenemen. Het zou kunnen zijn dat het door een toenemend aantal registraties lijkt dat een bepaalde vorm van fraude meer voorkomt, maar dat dit een vertekend beeld is.

5.5 Conclusie

Dit hoofdstuk beschrijft de waardering van de dienstverlening van de Fraudehelpdesk door melders en ketenpartners. Uit de vragenlijst onder respondenten die een melding hebben gemaakt bij de Fraudehelpdesk blijkt dat het overgrote deel (95%) dit als particulier heeft gedaan. De helft van de respondenten is tevreden is over de wijze waarop ze door de Fraudehelpdesk zijn geholpen. De vriendelijkheid van de medewerker wordt gemiddeld met een 7.7 beoordeeld, de deskundigheid met een 7.5 en de hulpvaardigheid met een 7.4. Iets meer dan 20% van de respondenten is niet tevreden over de wijze waarop ze door de Fraudehelpdesk zijn geholpen en bij een kwart (26%) voldeed het contact niet aan de verwachtingen. Uit de toelichting van de respondenten blijkt dat dit mede te maken heeft met het feit dat de Fraudehelpdesk zelf geen zaken oppakt of actie kan ondernemen en melders van tevoren een andere verwachting hadden van de dienstverlening van de Fraudehelpdesk. Daarnaast blijkt uit de resultaten van het vragenlijst onderzoek dat meer dan de helft van de respondenten (61%) die zijn doorverwezen, het gevoel had te zijn doorverwezen naar de juiste organisatie. Verbetersuggesties van respondenten hebben met name betrekking op de terugkoppeling na het doen van een melding en het aanpakken van fraudezaken.

Met betrekking tot de waardering van ketenpartners is gebleken dat alle ketenpartners positief zijn over het contact dat zij met de Fraudehelpdesk hebben en dat vrijwel alle ketenpartners de dienstverlening door de Fraudehelpdesk ook positief beoordelen. De Fraudehelpdesk heeft volgens hen veel kennis en expertise over uiteenlopende fraudevormen in huis en heeft meerwaarde op het gebied van preventie.

Ketenpartners signaleren wel een aantal punten dat extra aandacht behoeft en op dit moment een knelpunt oplevert. De omstandigheid dat de Fraudehelpdesk opereert in een landschap met veel meldpunten kan een knelpunt opleveren voor burgers en ondernemers om bij de juiste organisatie terecht te komen. Ook vormt volgens een deel van de ketenpartners de omstandigheid dat de Fraudehelpdesk geen persoonsgegevens van strafrechtelijke aard mag verwerken en delen een belemmering op in het effectief bestrijden van fraude. Verder signaleren ketenpartners dat de Fraudehelpdesk op dit moment een kwetsbare organisatie met beperkte capaciteit is en dat het ontbreken van een eenduidige terminologie bij de preventie en bestrijding van fraude een knelpunt in de gehele keten vormt.

Volgens ketenpartners levert het in de toekomst voldoende zichtbaar blijven in een landschap vol meldpunten en digitale ontwikkelingen een uitdaging en aandachtspunt op voor de Fraudehelpdesk. De organisatie speelt volgens ketenpartners een belangrijke rol in het voorkomen

van fraude, maar kan wellicht verder innoveren op het gebied van informatieverstrekking. Ketenpartners noemen hierbij onder meer het (nog meer) inzetten op sociale media. Deelnemers aan de expertmeeting geven ten slotte aan dat diensten op het gebied van doorverwijzen en het ondersteunen van slachtoffers kunnen worden verbeterd. Een meer warme in plaats van koude doorverwijzing zou vanuit het perspectief van het slachtoffer meerwaarde hebben. Daarnaast zou er winst te behalen zijn in het verrijken van registraties van de Fraudehelpdesk, door het valideren, aanvullen en duiden van cijfers op basis van informatie bij ketenpartners.

6 Landschap van fraudemeldpunten

6.1 Inleiding

In dit hoofdstuk brengen we de verschillende meldpunten voor het melden van slachtofferschap en het verkrijgen van informatie over horizontale fraude en oplichting in Nederland in beeld. De inventarisatie geeft antwoord op de vraag welke meldpunten er naast de Fraudehelpdesk in Nederland zijn voor het melden van slachtofferschap en het verkrijgen van informatie over horizontale fraude en oplichting (deelvraag 12). In paragraaf 6.2 lichten we de onderzoeksverantwoording toe. In paragraaf 6.3 komen verschillende type meldpunten aan bod. Paragraaf 6.4 bevat een beschrijving van instanties en websites die geen meldingen registreren, maar wel informatie verstrekken over horizontale fraude. In paragraaf 6.5 komen de verschillende diensten die meldpunten verlenen aan bod. Het hoofdstuk sluit af met een vergelijking tussen de diensten van de Fraudehelpdesk en andere meldpunten in paragraaf 6.6.

6.2 Verantwoording

Om het landschap van fraudemeldpunten in kaart te brengen hebben we gebruik gemaakt van een eerder onderzoek waarbij meldpunten voor horizontale fraude zijn geïnventariseerd. In 2015 hebben Homburg en Van den Tillaart meldpunten voor horizontale fraude in beeld gebracht, in het kader van hun onderzoek naar de mogelijkheden om tot meer synergie te komen tussen fraudemeldpunten.¹⁵⁷ Bij de categorisering van meldpunten is aansluiting gezocht bij het type diensten uit het onderzoek van Homburg en Van den Tillaart (2015), waarbij enkele categorieën zijn uitgesplitst. Een overzicht van de geïnventariseerde meldpunten is opgenomen in bijlage 7.

Omdat deze lijst enige jaren verouderd is, hebben we de lijst van Homburg en Van den Tillaart als uitgangspunt genomen en geactualiseerd. In totaal bleken 19 meldpunten uit het onderzoek van Homburg en Van den Tillaart niet meer te bestaan, was het onduidelijk of ze nog actief waren of waren dubbel opgenomen. Voor meldpunten van bedrijven, banken, woningcorporaties, zorgverzekeraars, verzekeringsmaatschappijen en netbeheerders hebben we drie willekeurige bedrijven/organisaties geselecteerd, omdat het te ver voor dit onderzoek voerde

¹⁵⁷ Homburg en Van den Tillaart, 2015.

hier een uitputtende lijst voor op te stellen.¹⁵⁸ Wel is op deze manier een algemeen beeld verkregen van de diensten die deze bedrijven of organisaties aanbieden.

Ten slotte hebben we de lijst aangevuld met nieuwe meldpunten. Hiervoor is gebruik gemaakt van een lijst met 153 zoektermen over fraude.¹⁵⁹ Op elke eerste resultatenpagina van Google is gekeken of er nieuwe meldpunten tussenstonden. Daarnaast zijn nog enkele meldpunten toegevoegd die zijn gevonden via andere meldpunten. Dit leverde vijftien nieuwe meldpunten op.

Er kunnen verschillende opvattingen bestaan over wat precies een meldpunt is. Bij sommige organisaties of platformen is het doen van een melding niet mogelijk, maar wordt wel voorlichting over fraude gegeven of worden eventuele slachtoffers wel doorverwezen naar andere organisaties. Een voorbeeld hiervan is de KvK. Via de website verstrekt de KvK veel informatie aan ondernemers over onder andere actuele phishingmails, maar het is niet mogelijk om bij de KvK een melding te doen van fraude. Onder een meldpunt wordt in dit onderzoek verstaan dat het voor burgers en/of bedrijven mogelijk moet zijn om via een e-mailadres, chatfunctie, meldformulier of op telefonische wijze een melding te doen van fraude.

Omdat het doel van dit deelonderzoek is om in beeld te brengen welke positie de Fraudehelpdesk in het veld van Nederlandse fraudepreventie bekleedt en welke andere loketten er naast de Fraudehelpdesk nog meer zijn voor het melden van slachtofferschap en verkrijgen van informatie, zal ook aandacht worden besteed aan instanties, en websites die geen meldfunctie kennen, maar wel algemene informatie verstrekken over fraude of slachtoffers doorverwijzen.

In totaal zijn 50 meldpunten geïnventariseerd en 15 instanties en/of websites die informatie over fraude verstrekken of slachtoffers doorverwijzen.¹⁶⁰ Zoals gezegd is dit geen uitputtende lijst. Wel zijn de meest belangrijke en grootste meldpunten meegenomen. Via het bestuderen van websites van de meldpunten en loketten is nagegaan welke diensten worden aangeboden. Deze informatie is verzameld en geordend in een tabel die is opgenomen in bijlage 7 en als input diende voor onderstaande paragrafen.

6.3 Type meldpunten

Om inzicht te krijgen in welke overlap er is in diensten die meldpunten aanbieden en welke diensten van de Fraudehelpdesk uniek zijn, is het behulpzaam eerst inzicht te krijgen in de type meldpunten en de beheerders of initiatiefnemers van de meldpunten. Op basis van de inventarisatie kan onderscheid worden gemaakt tussen meldpunten van bedrijven of instellingen, meldpunten van (branche)verenigingen, meldpunten die een publiek initiatief zijn of worden gefinancierd met publieke middelen en particuliere initiatieven.

¹⁵⁸ Homburg en Van den Tillaart hebben ook meldpunten van gemeenten geïnventariseerd. Deze meldpunten hebben wij buiten beschouwing gelaten, omdat daar met name fraude met gemeenschapsgeld (bijvoorbeeld fraude met uitkeringen) kan worden gemeld en dit valt onder verticale fraude.

¹⁵⁹ De lijst met zoektermen is ook gebruikt in het onderzoek naar de vindbaarheid van de website van de Fraudehelpdesk. De lijst met zoektermen is opgenomen in bijlage 7.

¹⁶⁰ Het totaal aantal geïnventariseerde meldpunten is inclusief de Fraudehelpdesk.

Meldpunten van bedrijven of instellingen

Een groot deel van de geïnventariseerde meldpunten is verbonden aan bedrijven of instellingen, zoals banken, woningcorporaties, netbeheerders en (zorg)verzekeraars. In dit onderzoek is geen uitputtend overzicht gemaakt van dit type meldpunten, maar vanzelfsprekend bestaan er nog meer van deze meldpunten dan in bijlage 7 zijn opgenomen. Deze meldpunten registreren veelal meldingen om ze te onderzoeken en eventueel maatregelen te treffen om schade voor zichzelf en/of voor andere klanten te beperken. Meldpunten van bedrijven of instellingen zijn met name gericht op fraude met betaalmiddelen, hypotheekfraude (banken), energiefraude (netbeheerders), verzekeringsfraude ((zorg)verzekeraars) en woonfraude (woningcorporaties).¹⁶¹ Voorbeelden zijn (zorg)verzekeringsmaatschappijen zoals Nationale Nederlanden en Zilveren Kruis die in veel gevallen ook een meldpunt voor fraude kennen. Als de verzekeraar fraude constateert kunnen verschillende maatregelen worden genomen. Een aanvraag om een verzekering kan worden geweigerd, de verzekeraar kan aangifte doen, uitbetaalde schadebedragen kunnen worden teruggevorderd en eventuele andere verzekeringen kunnen worden beëindigd.

Meldpunten van (branche)verenigingen

Een tweede categorie van meldpunten is een initiatief van een (branche)vereniging. Een deel van deze meldpunten is voornamelijk gericht op het melden van fraude door ondernemers of organisaties in een bepaalde branche. Het Centrum Bestrijding Verzekeringsscrimnaliteit is hier een voorbeeld van. Het centrum is onderdeel van het Verbond van Verzekeraars en ondersteunt verzekeraars bij het voorkomen en aanpakken van verzekeringscrimnaliteit. Dit doet het centrum op zowel operationeel als op beleidsniveau.¹⁶² Het centrum is primair gericht op het ondersteunen van verzekeraars maar ook particulieren kunnen melding maken bij het centrum. Ook bestaan er incidentenwaarschuwingssystemen voor financiële instellingen. In een incidentenwaarschuwingssysteem kan iemand die misbruik maakt van een financiële instelling worden vastgelegd. Financiële instellingen kunnen elkaar op die manier waarschuwen voor fraudeurs. Deze systemen zijn dus niet gericht op consumenten. De Koninklijke Vereniging Bloemist Winkeliers is een voorbeeld van een kleinere (branche)vereniging en waarschuwt ondernemers voor spookfacturen en biedt juridische ondersteuning aan gedupeerden.

Meldpunten van (branche)verenigingen richten zich op fraude in een specifieke sector en proberen fraude tegen te gaan en te voorkomen door het ondersteunen van aangesloten organisaties of bedrijven. Bovendien hebben zij door het verzamelen van meldingen zicht op de omvang van fraudesignalen in een bepaalde sector.

Publieke beheerders

In ons onderzoek zijn wij ook meerdere meldpunten tegengekomen die (gedeeltelijk) een publiek initiatief zijn. Bij organisaties als de ACM, de AFM, de Kansspelautoriteit, de FIOD en de NZA kunnen particulieren en/of (kleine) bedrijven melding doen van fraude. Het meldpunt bij deze organisaties maakt deel uit van een grotere toezichts- of opsporingsinstantie. Bij deze meldpunten kunnen bepaalde categorieën fraudevormen worden gemeld, zoals fraude met betaalmiddelen en online handel, telecomfraude, beleggingsfraude en faillissementsfraude. Deze meldpunten gebruiken de meldingen veelal als aanleiding voor een eventueel onderzoek en kunnen in het geval van een overtreding, maatregelen treffen. Zoals Homburg en Van den

¹⁶¹ Energiefraude en woonfraude vallen onder de categorie 'overig'.

¹⁶² <https://www.verzekeraars.nl/branche/verzekeringscrimnaliteit>.

Tillaart in hun onderzoek ook constateerden, lijken de voorgaande organisaties gedeeltelijk gericht op het aanpakken van specifieke vormen van fraude die in mindere mate direct burgers of kleine ondernemers raken.

Daarnaast zijn er nog (gedeeltelijk) publieke meldpunten die specifiek zijn opgericht op het verwerken van meldingen. Het gaat daarbij om het LMIO, het CMI, Meld Misdaad Anoniem en Slachtofferhulp. Ook de Fraudehelpdesk valt onder deze groep van meldpunten. Deze meldpunten zijn gericht op fraudevormen waar burgers of kleine met name direct door worden geraakt. Homburg en Van den Tillaart gaven in hun onderzoek aan dat burgers en kleine bedrijven met name geraakt worden door fraude met online handel, voorschotfraude, beleggingsfraude, identiteitsfraude en acquisitiefraude (ondernemers).¹⁶³ Dit komt grotendeels overeen met een recent onderzoek uit 2022, waaruit blijkt dat de meeste Nederlanders in dat jaar slachtoffer werden van aankoopfraude, verkoopfraude, fraude met betalingsverkeer, phishing en identiteitsfraude.¹⁶⁴

Het LMIO is een publiek-private samenwerking tussen de Politie, het OM en Marktplaats. Het doel is internetoplichting te bestrijden en aan te pakken. Melders kunnen via de website van de politie melding doen van een oplichting. Een deel van de informatie wordt naar Marktplaats doorgestuurd, zodat Marktplaats bijvoorbeeld de advertentie kan verwijderen. Het LMIO verzamelt meldingen van mogelijke oplichting en analyseert deze en brengt meldingen met elkaar in verband. Het CMI is onderdeel van de Rijksdienst voor Identiteitsgegevens. Het CMI richt zich op voorlichting en preventie en helpt en adviseert melders om het misbruik van gegevens te stoppen en eventuele gevolgen te herstellen. Bij Meld Misdaad Anoniem kunnen meldingen op het gebied van criminaliteit worden gedaan, waarna deze worden doorgezet naar relevante ketenpartners. Slachtofferhulp ondersteunt slachtoffers van onder andere fraude op praktisch, financieel, juridisch en emotioneel gebied.

Particuliere initiatieven

De laatste categorie meldpunten betreffen particuliere initiatieven zoals Stichting Publeaks. Dit is een platform waar mensen meldingen van onder meer fraude kunnen doen, waarbij anoniem informatie wordt doorgegeven aan de pers. Het doel van het platform is het versterken van het controlerend vermogen van de media. Andere stichtingen zijn Stichting Brein en ServiceOrganisatie Directe Aansprakelijkheidsstelling (SODA). Stichting Brein doet onderzoek naar grootschalige auteursrechtinbreuk van onder meer muziek, films en boeken. SODA ondersteunt consumenten bij het verhalen van het aankoopbedrag en een schadevergoeding op de dader.

6.4 Doorverwijs- en preventiepunten

Naast het registreren van meldingen, verwijst de Fraudehelpdesk melders ook door en verstrekt zij algemene informatie. Hoewel dit deelonderzoek voornamelijk is gericht op het in kaart brengen van meldpunten, is er ook een aantal organisaties, instellingen of websites dat

¹⁶³ Homburg en Van den Tillaart 2015, p. 13-14.

¹⁶⁴ Zie het onderzoek van Akkermans e.a. 2022, par. 4.1.5. Uit het onderzoek blijkt dat in 2022 8 procent van de Nederlanders van 15 jaar of ouder slachtoffer werd van een of meerdere vormen van online oplichting en fraude. De meeste mensen werden slachtoffer van aankoopfraude (6 procent), waarbij betaalde producten of diensten niet werden geleverd.

potentiële slachtoffers wel doorverwijst maar geen meldingen registreert. Voorbeelden hiervan zijn: de Hackhelpdesk, maakhetzenietmakkelijk.nl, seniorweb.nl en slachtofferwijzer.nl

Ondernemers en particulieren kunnen bij deze organisaties en of websites terecht voor specifieke vragen op het gebied van fraude. Er wordt op de websites informatie verstrekt over het voorkomen van fraude, er worden waarschuwingen gegeven en/of er wordt doorverwezen naar andere organisaties. Daarnaast worden slachtoffers op de website van Slachtofferwijzer en de Hackhelpdesk ook begeleid in het geval zij slachtoffer zijn geworden. Op de website van de Hackhelpdesk kunnen mensen bijvoorbeeld een handleiding verkoopfraude vinden, waarin een stappenplan met betrekking tot verkoopfraude is opgenomen voor slachtoffers.

6.5 Type diensten

Meld-, doorverwijs- en preventiepunten (hierna: meld/hulp punt) bieden verschillende soorten diensten aan. Sommige meld/hulp punten analyseren en onderzoeken meldingen maar ondersteunen geen slachtoffers, terwijl andere meld/hulp punten zich juist richten op het doorverwijzen en begeleiden van slachtoffers. Weer andere meld/hulp punten bieden een combinatie van diensten aan. Per meld/hulp punt is in kaart gebracht welk type diensten wordt aangeboden. In bijlage 7 is een overzicht van de meldpunten en hun diensten opgenomen.

De volgende type diensten worden onderscheiden:

- Meldingen registreren, monitoren en signaleren
- Analyseren en onderzoeken
- Voorlichting met het oog op preventie
- Begeleiding/ondersteuning van slachtoffers
- Doorverwijzen van slachtoffers naar andere organisaties
- Aanpakken van fraudezaken (vervolgen/schade verhalen/maatregelen treffen)

Meldingen registreren, monitoren en signaleren

Van de 65 meld/hulp punten, registreren 50 daarvan meldingen. Een deel van die meldpunten gebruikt de meldingen om fraudevormen te monitoren (14) of te signaleren (17). Voorbeelden van organisaties die dit wel doen zijn de AFM, die ieder half jaar een Signalenmonitor publiceert met daarin een overzicht van signalen op basis van meldingen van consumenten en ondernemingen. Een ander platform dat meldingen gebruikt om misstanden te signaleren is Publeaks. Deze website gebruikt meldingen dan weer niet om bepaalde misstanden ook te monitoren. Bij de Nederlandse Vereniging van Banken kunnen geen meldingen over fraude worden gedaan, maar de NVB publiceert twee keer per jaar een persbericht over omvang van schade in het betalingsverkeer en signaleert opkomende fraudevormen.

Uit de maandmonitoren en de interviews met ketenpartners en de Fraudehelpdesk blijkt dat de Fraudehelpdesk registraties gebruikt om fraudevormen te monitoren en nieuwe trends en ontwikkelingen in een vroeg stadium te signaleren.

Analyseren en onderzoeken

Iets meer dan de helft van de meldpunten gebruikt meldingen om deze te analyseren en verder te onderzoeken (27 van de 50 meldpunten). Meldingen analyseren en onderzoeken wordt met name gedaan door instanties die belast zijn met toezicht en/of opsporing zoals de ACM,

de AFM, de FIOD, de NZA, en (zorg)verzekeraars. Meldingen kunnen voor de toezichthoudende instanties en (zorg)verzekeraars aanleiding vormen voor een onderzoek. Onderzoek wordt gedaan met als doel na te gaan of regels waar de toezichthouder toezicht op houdt worden overtreden. (Zorg)verzekeraars analyseren en onderzoeken meldingen om na te gaan of er verzekeringsfraude wordt gepleegd. De AFM kan bijvoorbeeld onderzoek doen naar financiële ondernemingen naar aanleiding van meldingen over beleggingsfraude.

De Fraudehelpdesk onderzoekt geen meldingen om vervolgens maatregelen te kunnen treffen. Wel analyseert de Fraudehelpdesk meldingen met als doel om veel voorkomende of nieuwe vormen van fraude te signaleren en hiervoor te waarschuwen.

Voorlichting met het oog op preventie

Het voorlichten van burgers en bedrijven wordt door veel verschillende partijen opgepakt (37 van de 65 meld/hulppunten). Websites van Marktplaats.nl en Autoscout24 bieden informatie over hoe verdachte advertenties kunnen worden herkend, maar ook websites van banken bevatten uitgebreide uitleg over verschillende vormen van fraude en hoe fraude kan worden herkend en voorkomen. Ook verschillende brancheverenigingen en de KvK waarschuwen ondernemers op met name het gebied van acquisitiefraude. Daarnaast geven websites als seniorweb.nl, zowerktfraude.nl, maakhetzenietmakkelijk.nl, opgelicht.nl en consuwijzer.nl tips, met name gericht op burgers, en waarschuwingen over hoe fraude kan worden voorkomen. Het LMIO probeert preventief fraude te voorkomen door middel van het aanbieden van een dienst waar burgers verkopers kunnen checken. Via een link kunnen mensen zoeken op IBAN-rekeningnummers, e-mailadressen, telefoonnummers of een url van bijvoorbeeld een webwinkel. Als de checkfunctie de uitslag 'er zijn meldingen over deze partij bekend' geeft, dan is iemand gewaarschuwd.

Uit de jaarverslagen en interviews met de Fraudehelpdesk en ketenpartners blijkt dat de Fraudehelpdesk algemene informatie verstrekt over fraude met het oog op preventie.

Begeleiding/ondersteuning van slachtoffers

Een deel van de slachtoffers van fraude heeft behoefte aan begeleiding of ondersteuning op emotioneel, praktisch, juridisch of financieel gebied. Dit zal mede afhankelijk zijn van het type fraude waar een slachtoffer mee te maken heeft gehad. Slachtofferhulp is een organisatie die slachtoffers emotionele ondersteuning biedt, praktische hulp biedt en kan helpen bij juridisch advies. Slachtoffers kunnen bij Slachtofferhulp terecht met een breed scala aan fraudevormen zoals datingfraude maar ook voor beleggingsfraude. Slachtoffers van online grensoverschrijdend gedrag kunnen, als zij slachtoffer zijn van identiteitsfraude chatten voor eerste hulp. De website van de Consumentenbond ondersteunt slachtoffers door de mogelijkheid om met juridische experts te bellen. Deze advieslijn is alleen beschikbaar voor aangesloten leden. Consumenten of bedrijven die slachtoffer zijn van fraude kunnen daarnaast ondersteuning vinden bij SODA om schade te verhalen via het civiel recht. Om schade te verhalen kunnen slachtoffers ook de hulp van juridisch dienstverleners inschakelen. 12 van de 65 geïnterviewde meld/hulppunten bieden slachtoffers begeleiding en/of ondersteuning.

De Fraudehelpdesk biedt, zo blijkt uit interviews met medewerkers van de Fraudehelpdesk en ketenpartners, een luisterend oor aan slachtoffers en probeert hen te ondersteunen door het geven van tips.

Doorverwijzen van slachtoffers

Slachtoffers kunnen worden doorverwezen omdat zij een melding doen bij een meldpunt en het meldpunt hen doorverwijst naar een andere organisatie of instelling, maar ook websites verwijzen slachtoffers naar talloze organisaties door. De website van slachtofferwijzer.nl biedt slachtoffers bijvoorbeeld informatie over instanties waar zij terecht kunnen voor praktische, juridische, emotionele of financiële hulp. De website zowerktfraude.nl van de NVB verwijst slachtoffers door naar de websites van Nederlandse banken. Ook de website van helpwanted.nl verwijst slachtoffers, in het geval helpwanted.nl niet genoeg hulp kan bieden, naar andere hulplijnen en informatiepagina's. 29 van de 65 geïnventariseerde meld/hulppunten wijzen slachtoffers door.

De Fraudehelpdesk kan slachtoffers doorverwijzen naar andere instanties. Medewerkers van de Fraudehelpdesk hebben de onderzoekers laten zien dat melders in dat geval na afloop van een melding een overzicht ontvangen met organisaties waar zij terecht kunnen.

Aanpakken van fraudezaken (vervolgen/schade verhalen)

Verzekeraars en toezichthoudende instanties zijn met name gericht op het aanpakken van fraudeurs door het opleggen van maatregelen of sancties. Wanneer een slachtoffer schade wil verhalen op de fraudeur, kan hulp worden ingeschakeld van juridisch adviseurs of een organisatie als SODA. Het LMIO probeert nieuwe fraude te voorkomen door het aanbieden van de mogelijkheid om potentiële (ver)kopen te controleren door na te gaan of bepaalde gegevens van de andere partij reeds bij de politie bekend zijn. Daarnaast kunnen meldingen bij LMIO worden omgezet in aangiftes en kan verder onderzoek worden gedaan en kunnen malafide partijen in overleg met bijvoorbeeld Marktplaats offline worden gehaald.

De Fraudehelpdesk pakt geen fraudezaken aan. De Fraudehelpdesk verwijst slachtoffers wel door naar partijen die dit wel doen.

6.6 Type fraudevormen

Ten slotte is in het kader van dit onderzoek gekeken op welke fraudevormen een meldpunt zich richt. Uit bijlage 7 blijkt dat een groot deel van de meld/hulppunten zich op meerdere vormen van fraude richt. Voorbeelden van meld/hulppunten waarbij burgers en/of ondernemers voor meerdere vormen van fraude terecht kunnen zijn: Consuwijzer, Meld Misdaad Anoniem, Slachtofferhulp en de Fraudehelpdesk. (Zorg)verzekeringsmaatschappijen richten zich (met name) op verzekeringsfraude en banken op fraude met betaalmiddelen. Voor enkele vormen van fraude bestaan speciale meldpunten, zoals het CMI voor identiteitsfraude. Uit bijlage 7 blijkt dat burgers en bedrijven voor alle categorieën fraude bij een of meerdere meld/hulppunten terecht kunnen.

6.7 Conclusie

Centraal in dit hoofdstuk stond de vraag of er overlap bestaat in de diensten die verschillende meldpunten aanbieden en welke diensten van de Fraudehelpdesk uniek zijn. Om dit in beeld te brengen is een (niet uitputtend) overzicht gemaakt van horizontale fraudemeldpunten. In totaal zijn 50 meldpunten geïnventariseerd en 15 instanties en/of websites die informatie over fraude verstrekken of slachtoffers doorverwijzen. Het landschap is, zoals ook in 2015 door Homburg en Van den Tillaart werd geconstateerd, door de veelheid en verschillende vormen en functies van meldpunten, diffuus.¹⁶⁵

Een groot deel van de meldpunten in Nederland is onderdeel van een bedrijf of instelling, zoals een bank, een verzekeraar of een netbeheerder. Organisaties die deze meldpunten beheren kunnen barrières opwerpen om nieuwe fraude tegen te gaan (bijvoorbeeld door het blokkeren van een bankrekening), sancties treffen (bijvoorbeeld door boetes op te leggen) en meldingen gebruiken voor toekomstig beleid op het gebied van fraude. Ook verschillende (branche)verenigingen bieden de mogelijkheid om fraude te melden met als doel aangesloten organisaties te ondersteunen, te waarschuwen en trends en ontwikkelingen te signaleren. Daarnaast zijn er ook meldpunten bij toezichthoudende instanties zoals de AFM, NZA en ACM. Deze meldpunten gebruiken meldingen voornamelijk als aanleiding voor onderzoek om eventuele overtreders van wet- en regelgeving op te sporen. De Fraudehelpdesk onderscheidt zich ten opzichte van de hiervoor genoemde meldpunten, omdat de Fraudehelpdesk meldingen primair gebruikt om een bijdrage te leveren aan de voorkant van de fraudebestrijdingsketen (preventie en ondersteuning van burgers en mkb'ers) en niet gericht is op de achterkant van de keten (aanpakken en onderzoeken van fraudezaken).

Zoals Homburg en Van den Tillaart constateren zijn de meldpunten die verbonden zijn aan het merendeel van de voorgaande organisaties gedeeltelijk gericht op het aanpakken van specifieke vormen van fraude die in mindere mate direct burgers of kleine ondernemers raken.¹⁶⁶ Zij worden volgens hen met name geraakt door fraude met online handel, voorschotfraude, beleggingsfraude, identiteitsfraude en acquisitiefraude. Er zijn twee meldpunten die zich op twee van deze vormen richten, namelijk het LMIO en het CMI. Dit zijn meer gespecialiseerde meldpunten die in het leven zijn geroepen om specifieke vormen van fraude (internetoplichting en identiteitsfraude) tegen te gaan, in te zetten op preventie en slachtoffers te ondersteunen. Burgers kunnen als zij slachtoffer zijn geworden ook terecht bij Slachtofferhulp Nederland en Meld Misdaad Anoniem. Deze organisaties richten zich niet op een specifieke vorm van fraude, maar op alle soorten criminaliteit of ingrijpende gebeurtenissen. Slachtofferhulp verschilt ten opzichte van de Fraudehelpdesk omdat met name wordt ingezet op het ondersteunen van slachtoffers op financieel, emotioneel, juridisch en praktisch gebied. Bij Meld Misdaad Anoniem kunnen anonieme tips over fraude worden gemeld, die worden doorgestuurd naar de Politie en andere opsporingsdiensten. Meld Misdaad Anoniem is in mindere mate gericht op preventie door het verstrekken van algemene informatie.

Er zijn geen diensten van de Fraudehelpdesk die uniek zijn, maar de combinatie van diensten en de brede oriëntatie op alle vormen van fraude zijn in het landschap van fraudemeldpunten wel uniek. De Fraudehelpdesk is de enige organisatie die speciaal in het leven is geroepen om

¹⁶⁵ Homburg en Van den Tillaart 2015, p. 23.

¹⁶⁶ Met een 'specifieke' vorm van fraude wordt bedoeld dat het om één of enkele vormen van fraude gaat.

zich specifiek bezig te houden met alle vormen van fraude. Melders kunnen telefonisch en digitaal bij de Fraudehelpdesk terecht voor informatie of het doen van een melding. De Fraudehelpdesk kan geen zaken aanpakken, maar verwijst in die gevallen melders door naar ketenpartners zoals de Politie, juridische dienstverleners, het LMIO of het CMI. De Fraudehelpdesk gebruikt meldingen over (potentiële) fraude dus om een bijdrage te leveren aan de voorkant van de fraudebestrijdingsketen (preventie en ondersteuning slachtoffers) en niet aan de achterkant van de keten (aanpakken en onderzoeken van fraudezaken). Wel zijn er andere meldpunten en platforms die (een deel van) deze of andere diensten verlenen, maar zich dan op één of een aantal vormen van fraude richten. Bovendien blijkt dat bij een groot deel van de meldpunten of websites digitaal melding kan worden gedaan en slachtoffers door middel van informatie op de websites worden doorverwezen naar ketenpartners. Laagdrempelig persoonlijk contact met een medewerker is dus niet bij alle meldpunten mogelijk, terwijl slachtoffers hier mogelijk wel behoefte aan hebben. De Fraudehelpdesk en bijvoorbeeld ook Slachtofferhulp en ConsuWijzer bieden wel deze mogelijkheid doordat burgers en/of bedrijven telefonisch contact kunnen opnemen, maar bij het CMI kan alleen digitaal een formulier worden ingevuld.

7 Synthese en conclusie

7.1 Inleiding

We beantwoorden in paragraaf 7.2 de vijf hoofdvragen van het onderzoek. Dat doen we aan de hand van de bevindingen uit de voorgaande hoofdstukken. In hoofdstuk 2 stond de beleidstheorie van de fraudehelpdesks centraal: wat waren de doelen van het oprichten van een helpdesk en kunnen die doelen in theorie worden bereikt? Hoofdstuk 3 schetste (ontwikkelingen in) de financiering, organisatie en activiteiten van de Fraudehelpdesk. Hoofdstuk 4 presenteerde de bevindingen van het naamsbekendheid- en zichtbaarheidsonderzoek. In hoofdstuk 5 was de waardering van de Fraudehelpdesk door melders en ketenpartners aan de orde en in hoofdstuk 6 stond het landschap van fraudemeldpunten centraal. Dit hoofdstuk sluit af met een conclusie in paragraaf 7.3.

7.2 Beantwoording centrale onderzoeksvragen

- 1. In hoeverre kunnen de doelen die de Fraudehelpdesk nastreeft in theorie via de geldende subsidievoorwaarden en het inrichtingsplan van de Fraudehelpdesk worden bereikt?**

Met het oprichten van een helpdesk wilde het kabinet, zoals in hoofdstuk 2 aan de orde is gekomen, een frontoffice creëren waar consumenten en kleine ondernemers terecht konden

met vragen over fraude en oplichting.¹⁶⁷ De aanleiding voor het oprichten van een helpdesk is mede terug te voeren op een Tweede Kamermotie, waarin de Kamerleden constateerden dat er tot op dat moment (2007) onvoldoende aandacht was voor de schade van slachtoffers van financieel-economische misdaad.¹⁶⁸ Daarnaast bleek uit onderzoek onder burgers dat er behoefte was aan een helpdesk waar mensen informatie konden krijgen over oplichting.¹⁶⁹

Het kabinet streefde met het oprichten van een helpdesk twee doelen na. Het eerste doel was het zo goed mogelijk ondersteunen van slachtoffers en het tweede doel was het weerbaarder maken van burgers en bedrijven tegen pogingen tot oplichting en fraude. Om deze doelen te bereiken moest de helpdesk – zoals vastgelegd in de subsidievoorwaarden van 2010 – drie (basis)diensten verlenen: (1) het registreren van aantallen en soorten meldingen, (2) het verstrekken van algemene informatie over bestaande vormen van fraude en (3) het doorverwijzen van slachtoffers naar de juiste organisaties. Zoals in hoofdstuk 3 is toegelicht zijn de subsidievoorwaarden uit 2010 niet meer van toepassing. Een inrichtingsplan hebben de onderzoekers niet ontvangen.

De reconstructie van de beleidstheorie laat zien dat er een tweetal veronderstellingen ten grondslag ligt aan de beleidstheorie. Kortgezegd zou het verstrekken van algemene kennis over fraude burgers en bedrijven weerbaarder moeten maken tegen fraude en zou het doorverwijzen van slachtoffers hen beter ondersteunen. De beleidstheorie ziet er op papier aannemelijk en consistent uit, maar empirische onderbouwing op basis van wetenschappelijke inzichten of ervaringen met andere meldpunten in een andere context ontbreekt.

Op basis van wetenschappelijke literatuur zijn kritische kanttekeningen te plaatsen bij de veronderstelling dat het verstrekken van algemene informatie door middel van bijvoorbeeld campagnes effectief is. In een artikel naar aanleiding van een onderzoek over cybergedrag geven de onderzoekers aan dat het belang van meer kennis bij het bestrijden van online criminaliteit door de overheid wordt overschat. Bewustmakingscampagnes worden vaak opgezet vanuit de veronderstelling dat kennis over cybersecurity ontbreekt, terwijl volgens de onderzoekers in feite andere factoren leiden tot onveilig digitaal gedrag.¹⁷⁰ Of campagnes en waarschuwingsberichten echt tot een gedragsverandering bij burgers en ondernemers leiden is zeer de vraag.¹⁷¹ Uit verschillende onderzoeken blijkt dat bij interventies om gedrag te veranderen onder meer sprake moet zijn van een goede timing, interactie en op een specifieke doelgroep gerichte informatie.¹⁷² Experts op het terrein van onderzoek naar cybergedrag geven bijvoorbeeld aan dat advies over veilig cybergedrag leerzamer is en sneller wordt overgenomen, wanneer dat gegeven wordt op het moment dat de onveilige gedraging (bijna) plaatsvindt.¹⁷³

Ten aanzien van de veronderstelling dat een centraal meldpunt slachtoffers van fraude zou moeten ondersteunen is in de literatuur wel onderbouwing gevonden. Slachtoffers van fraude lijken behoefte te hebben aan een centraal meldpunt, waarbij zij informatie krijgen over wat hun mogelijkheden zijn en hoe hun melding wordt opgepakt.¹⁷⁴ Voor veel slachtoffers is het

¹⁶⁷ *Kamerstukken II 2009/10*, 29 911, nr. 41, p.2.

¹⁶⁸ *Kamerstukken II 2007/08*, 31 200 VI, nr. 48.

¹⁶⁹ Oudejans en Vis, 2008.

¹⁷⁰ Van der Kleij e.a. 2020.

¹⁷¹ Van 't Hoff-de Goede e.a. 2019; p. 123; Jansen e.a. 2019, p. 59.

¹⁷² Bullée en Junger, *Information and Computer Security*, 2020/5; Van 't Hoff- de Goede e.a. p.123.

¹⁷³ Van 't Hoff- de Goede e.a. p.123.

¹⁷⁴ Button e.a. 2009, p. 68, 78.

dan ook wenselijk dat zij een melding kunnen doen en hierop duidelijke informatie krijgen over wat er kan worden gedaan in hun situatie en wat zij mogen verwachten in het proces.¹⁷⁵

Ten slotte blijkt uit de beleidsreconstructie dat er destijds in een Kamerbrief een vijftal randvoorwaarden is geformuleerd door de minister.¹⁷⁶ In het onderzoek is niet duidelijk geworden wat precies de achterliggende gedachte was van deze randvoorwaarden en het merendeel van deze randvoorwaarden werd ook niet door gesprekspartners herkend of als relevant gezien. Een van de randvoorwaarden is dat er een zodanige infrastructuur aanwezig diende te zijn dat fraudemeldingen aan Politie en Openbaar Ministerie konden worden doorgegeven. De Fraudehelpdesk mag (tot op heden) door het ontbreken van de vergunning van de AP geen persoonsgegevens van strafrechtelijke aard verwerken, waardoor het nu niet mogelijk is om aan de randvoorwaarde te voldoen. Enkele ketenpartners geven aan dat wanneer de Fraudehelpdesk die persoonsgegevens wel mag delen, fraude beter bestreden kan worden. De vraag is wel of dit een taak is die past bij de doelen waarvoor de Fraudehelpdesk is opgericht.

2. In welke mate volstaat de praktische invulling van het inrichtingsplan van de Fraudehelpdesk in het bereikbaar maken van deze doelen?

De tweede hoofdvraag van dit onderzoek wordt beantwoord aan de hand van deelvragen 3, 4 en 5. Deze deelvragen gaan over (ontwikkelingen in) de financiering van de Fraudehelpdesk, in welke mate aan de in 2010 gestelde subsidievoorwaarden wordt voldaan en de inrichting van de organisatie.

Financiering

In hoofdstuk 3 is toegelicht dat om de basisdiensten (registreren, verstrekken van algemene informatie en doorwijzen) te verlenen de Fraudehelpdesk de afgelopen jaren subsidie van het ministerie van EZK en het ministerie van JenV ontving. Het ministerie van EZK heeft de subsidieverlening in 2021 en 2022 afgebouwd, waardoor de Fraudehelpdesk vanaf 2023 alleen subsidie van het ministerie van JenV ontvangt. Het ministerie van JenV heeft voor 2023 een subsidiebedrag van ruim een miljoen euro toegekend voor het verlenen van de basisdiensten. Het ministerie van JenV vindt het onwenselijk de enige subsidieverstrekker te zijn. De Fraudehelpdesk benadrukt de behoefte aan structurele financiering in een meerjarenplanning, met het oog op ontwikkelambities en aantrekkelijk werkgeverschap. Voor nieuwe projecten (zoals Fraudehub) is de Fraudehelpdesk nu genoodzaakt tot het aanboren van nieuwe financieringsbronnen, zoals bij gemeenten of andere partijen. Hier zet de Fraudehelpdesk de afgelopen jaren ook op in.

Hoewel de Fraudehelpdesk een private stichting is (Safecin) is de Fraudehelpdesk voornamelijk afhankelijk van publieke middelen. Het verminderen van de afhankelijkheid van het ministerie van JenV als enige subsidieverstrekker, door het aanboren van andere financieringsbronnen maakt de organisatie minder kwetsbaar. Tegelijkertijd zal publieke financiering wel noodzakelijk zijn, omdat het gaat om publieke diensten waar marktpartijen waarschijnlijk niet in zullen voorzien.

¹⁷⁵ Cross e.a. 2016, p. 56, Leukfeldt e.a. 2018, p. 100.

¹⁷⁶ *Kamerstukken II 2009/10, 29 911, nr. 41, p.2.*

Dat de organisatie van de Fraudehelpdesk kwetsbaar is wordt ook, zoals in hoofdstuk 5 aan de orde is gekomen, in meerdere gesprekken met ketenpartners aangegeven. Ketenpartners geven aan dat de kwetsbaarheid wordt veroorzaakt door het beperkte budget dat de Fraudehelpdesk ter beschikking staat. Ketenpartners zien wel dat de Fraudehelpdesk met een kleine groep werknemers veel werk verricht. Voldoende slagkracht is bij het voorkomen en bestrijden van fraude volgens meerdere ketenpartners van belang.

Subsidievoorwaarden

Uit de evaluatie blijkt dat de subsidievoorwaarden zoals die in 2010 zijn opgesteld niet meer van toepassing zijn. Wel wordt aan het merendeel van de destijds relevant geachte voorwaarden nog voldaan (zie bijlage 8). De voorwaarden hadden betrekking op de inrichting van de organisatie, ervaring en expertise van werknemers en het netwerk van de helpdesk.

Er zijn twee voorwaarden waar niet volledig aan wordt voldaan. Uit de subsidievoorwaarden volgt dat het destijds van belang werd geacht dat continuïteit en capaciteit van de helpdesk was gewaarborgd op werkdagen tussen 9.00 en 17.00 uur. Uit deze evaluatie blijkt dat digitale meldingen 24/7 kunnen worden ingediend, maar dat de telefonische helpdesk op woensdagochtend en iedere werkdag na 15.00 uur gesloten is. Woensdagochtenden worden door de Fraudehelpdesk gebruikt voor intern overleg. Daarnaast volgt uit de resultaten van het vragenlijstonderzoek dat niet alle melders binnen twee dagen een reactie krijgen, terwijl deze termijn volgens de subsidievoorwaarden wel in acht diende te worden genomen.¹⁷⁷

Bedrijfsvoering

Ten slotte kan ten aanzien van de bedrijfsvoering van de organisatie worden opgemerkt dat daarin de laatste jaren een professionaliseringsslag is gemaakt. Zo zijn er functieprofielen en een organogram opgesteld en zijn werkprocessen beschreven met het oog op de aanvraag van een vergunning voor het mogen verwerken van persoonsgegevens van strafrechtelijke aard.

De wijze waarop de Fraudehelpdesk de basisdiensten verleent, lijkt in grote mate te voldoen aan de voorwaarden die in de subsidievoorwaarden van 2010 zijn gesteld en het idee dat de regering had met het oprichten van een helpdesk. De bedrijfsvoering heeft de laatste jaren een professionaliseringsslag doorgemaakt. Voor de uitvoering van de basisdiensten die de Fraudehelpdesk verleent, zal de organisatie, vanwege het publieke karakter, afhankelijk blijven van publieke financiering.

3. Welke bijdrage heeft de Fraudehelpdesk geleverd aan de preventie en bestrijding van horizontale fraude?

Uit de reconstructie van de beleidstheorie blijkt dat de doelstelling van het oprichten van een helpdesk tweeledig was. Enerzijds was het doel het zo goed mogelijk ondersteunen van slachtoffers en anderzijds was het doel het weerbaarder maken van burgers en bedrijven tegen (poging) tot oplichting en fraude. De vraag welke bijdrage de Fraudehelpdesk heeft geleverd aan deze doelstellingen is niet eenduidig en nauwkeurig te beantwoorden. De Fraudehelpdesk verleent uiteenlopende diensten die slachtoffers dienen te ondersteunen en burgers en bedrijven weerbaarder dienen te maken tegen fraude. Het beoordelen van de effectiviteit van die

¹⁷⁷ 43% van de respondenten ontving wel binnen twee werkdagen reactie op hun melding.

diensten is in de praktijk ingewikkeld. De weerbaarheid van burgers en de ondersteuning van slachtoffers is nauwelijks meetbaar; beide worden beïnvloed door een groot aantal factoren. Bovendien ontbreekt een nulmeting, waardoor de maatregelen niet op effectiviteit kunnen worden beoordeeld. Het toetsen van de beleidstheorie is om deze redenen niet mogelijk. Wel kan worden gekeken naar de wijze waarop de Fraudehelpdesk invulling geeft aan het bereiken van de doelen en hoe de dienstverlening wordt beoordeeld door melders en ketenpartners (deelvraag 6 tot en met 9).

Naamsbekendheid en vindbaarheid website

De Fraudehelpdesk wil een centraal meldpunt zijn op het gebied van fraude om burgers en kleine ondernemers te kunnen ondersteunen. Uit hoofdstuk 4 blijkt dat de naamsbekendheid onder burgers en het aantal websitebezoekers van de Fraudehelpdesk de afgelopen jaren is toegenomen. Hierbij wordt ten aanzien van de bevindingen over de naamsbekendheid de kanttekening gemaakt dat die zijn gebaseerd op onderzoeken in opdracht van de Fraudehelpdesk en dat daarbij een volledige methodische verantwoording over het panel waarop dit onderzoek is gebaseerd ontbreekt. Hierdoor valt de betrouwbaarheid van deze onderzoeken niet te toetsen. Aan de andere kant lijkt de toename van de naamsbekendheid wel in lijn te zijn met andere bevindingen van dit onderzoek, zoals de bevinding dat website van de Fraudehelpdesk over het algemeen goed vindbaar is (paragraaf 4.4) en er sprake is van een groei van het aantal websitebezoekers in de loop der jaren (paragraaf 4.5). Naamsbekendheidsonderzoek onder ondernemers is alleen in 2020 uitgevoerd, waardoor geen uitspraken kunnen worden gedaan over de ontwikkeling van de naamsbekendheid van de Fraudehelpdesk onder ondernemers.

De website van de Fraudehelpdesk is over het algemeen goed zichtbaar. Van de 153 zoektermen die zijn onderzocht verschijnt de website van de Fraudehelpdesk bij 90 zoektermen (bijna 60%) op de eerste resultatenpagina. De website van de Fraudehelpdesk is met name goed zichtbaar op zoektermen over een bepaalde vorm van fraude in combinatie met het woord 'melden'. De website is minder goed zichtbaar als wordt gezocht op algemene termen als: 'hacking', 'malware' en 'spoofing'.¹⁷⁸ Een verklaring hiervoor zou kunnen zijn dat op deze termen een hoog zoekvolume zit en de concurrentie om op een hoge positie te komen daar groter is en het daardoor dus moeilijker is om hoog in de zoekresultaten te verschijnen.

Het aantal websitebezoekers van de Fraudehelpdesk was in 2022 ongeveer drie keer zo groot als het aantal websitebezoekers in 2014. Wel lijkt het aantal bezoekers en de bezochte pagina's de laatste jaren te zijn gestabiliseerd dan wel licht te zijn gedaald. Ten slotte blijkt uit hoofdstuk 3 dat bij het merendeel van de websites van ketenpartners wel een link is opgenomen op een pagina naar de website van de Fraudehelpdesk, maar geen van de ketenpartners verwijst op de eerste pagina naar de Fraudehelpdesk.

Waardering door melders

In hoofdstuk 5 zijn de bevindingen van het vragenlijstonderzoek onder melders gepresenteerd. De helft van de respondenten is tevreden over de wijze waarop ze door de Fraudehelpdesk zijn geholpen. Respondenten beoordelen de vriendelijkheid van de medewerker gemiddeld met een 7.7, de deskundigheid met een 7.5 en de hulpvaardigheid met een 7.4. Toch is ook bijna een kwart van de respondenten (22%) niet tevreden over de wijze waarop ze door

¹⁷⁸ In bijlage 9 is een overzicht opgenomen van definities van verschillende fraudevormen.

de Fraudehelpdesk zijn geholpen en bij een kwart (25%) voldeed het contact niet aan de verwachtingen. Dit lijkt met name te komen door het feit dat de Fraudehelpdesk zelf geen zaken oppakt of actie kan ondernemen tegen daders, wat een deel van de melders wel lijkt te verwachten.

Doorverwijzen

Het aantal doorverwijzingen van slachtoffers naar andere organisaties nam in de periode 2015 tot 2020 bijna jaarlijks toe. In 2021 en 2022 is een lichte afname te zien in het aantal doorverwijzingen en binnengekomen meldingen. Het is niet mogelijk om precieze uitspraken te doen over de mate waarin doorverwijzingen worden opgepakt door ketenpartners, omdat er in nagenoeg alle gevallen sprake is van een 'koude' doorverwijzing. Ketenpartners zelf geven aan dat als melders contact opnemen na een doorverwijzing zij die melding oppakken en kijken of en zo ja hoe zij de melding inhoudelijk kunnen afhandelen.

Een risico van het 'koud' doorverwijzen van meldingen is dat slachtoffers het idee kunnen krijgen dat zij van het kastje naar de muur worden gestuurd. Dat kan volgens een onderzoek naar de behoeften van slachtoffers van online fraude stress opleveren bij slachtoffers.¹⁷⁹ Uit dit onderzoek blijkt niet in hoeverre melders bij de Fraudehelpdesk problemen ervaren bij 'koud' doorverwijzen. Wel wordt door ketenpartners aangegeven dat dit gevaar op de loer ligt bij het systeem van doorverwijzen. Uit het vragenlijstonderzoek blijkt dat 61% van de respondenten die zijn doorverwezen het gevoel hebben naar de juiste organisatie te zijn doorverwezen. 14% van de respondenten had het gevoel niet naar de juiste organisatie te zijn doorverwezen. Van deze laatste groep respondenten heeft wellicht een deel het gevoel van het kastje naar de muur te zijn gestuurd.

Registratie van meldingen

De Fraudehelpdesk signaleert nieuwe vormen van fraude en trends en ontwikkelingen in een maandmonitor die sinds 2022 wordt verspreid onder geïnteresseerden. Deze monitor is gebaseerd op registraties van meldingen.

Uit hoofdstuk 3 blijkt dat het aantal meldingen bij de Fraudehelpdesk tussen 2015 en 2018 stabiel was, in 2019 en 2020 het aantal meldingen fors toenam, en in 2021 en 2022 er een afname te zien was van het aantal geregistreerde meldingen (met name via het verkorte meldformulier). Het hogere aantal meldingen vanaf 2019 ten opzichte van de jaren ervoor kan te maken hebben met de coronacrisis. De ontwikkeling van het aantal meldingen vanaf 2019 bij de Fraudehelpdesk komt in grote mate overeen met de ontwikkeling van het aantal aangiften bij de Politie van horizontale fraude.

Uit gesprekken met ketenpartners blijkt dat de trends en de ontwikkelingen die de Fraudehelpdesk signaleert over het algemeen worden herkend. Op dit moment lijkt alleen niet optimaal gebruik te worden gemaakt van de informatie waarover de Fraudehelpdesk beschikt. Ten eerste lijkt er beleidsinhoudelijk nauwelijks afstemming plaats te vinden tussen de Fraudehelpdesk en het ministerie, terwijl de kennis over trends en ontwikkelingen een belangrijke bijdrage kan leveren aan een van de belangrijkste pijlers van het fraudebeleid: preventie. Ten tweede wordt aangegeven dat de Fraudehelpdesk slechts zicht heeft op een deel van de puzzel. Ook ketenpartners als banken, verzekeraars, de politie, de AFM en ACM beschikken over

¹⁷⁹ Cross e.a. 2016, p. 9; Leukfeldt e.a. 2018, p. 86.

informatie over schadebedragen en aantallen slachtoffers. Het zou volgens ketenpartners waardevol zijn om de registraties van de Fraudehelpdesk te valideren, aan te vullen en te duiden op basis van informatie van ketenpartners.

Verstrekken van algemene kennis en informatie

Uit hoofdstuk 3 volgt dat de Fraudehelpdesk jaarlijks meerdere campagnes (met ketenpartners) opzet en uitvoert om aandacht te vragen voor specifieke vormen van fraude. Daarnaast worden burgers en ondernemers ook gewaarschuwd door berichten die de Fraudehelpdesk verspreidt over veel voorkomende fraude en modus operandi, worden mensen naar aanleiding van een melding geadviseerd en brengt de Fraudehelpdesk een maandmonitor met actuele informatie over fraude uit. Zoals gezegd wordt de effectiviteit van het verstrekken van algemene informatie door bewustwordingscampagnes in de literatuur kritisch beoordeeld. Een van de ketenpartners geeft aan dat ook een neveneffect kan optreden bij het opzetten en uitvoeren van campagnes. Het opzetten en uitvoeren van campagnes over een bepaald onderwerp kan voor meer bewustzijn en aandacht zorgen waardoor het aantal meldingen over die vorm van fraude ook zou kunnen toenemen. Door een toenemend aantal meldingen en registraties lijkt het dan dat een bepaalde vorm van fraude meer voorkomt, maar in werkelijkheid is dat dan een vertekend beeld.

Waardering ketenpartners

Vrijwel alle ketenpartners beoordelen de dienstverlening door de Fraudehelpdesk positief, zo blijkt uit hoofdstuk 5. De Fraudehelpdesk heeft volgens ketenpartners veel kennis en expertise over veel verschillende vormen van fraude in huis. Alle ketenpartners zijn van mening dat de Fraudehelpdesk meerwaarde heeft op het gebied van preventie, zeker als het gaat om het geven van voorlichting. Ketenpartners signaleren wel een aantal knelpunten, zoals dat het in het huidige landschap van vele meldpunten lastig is voor mensen om bij de juiste organisatie terecht te komen en het niet mogen verwerken van persoonsgegevens van strafrechtelijke aard door de Fraudehelpdesk. Daarnaast zien ketenpartners dat de Fraudehelpdesk op dit moment een kwetsbare organisatie is met beperkte capaciteit. Ook geven zij aan dat het ontbreken van een eenduidige terminologie bij de preventie en bestrijding van fraude een knelpunt in de gehele keten vormt. Ten slotte geven ketenpartners aan dat het voor de Fraudehelpdesk een uitdaging zal zijn om in de toekomst voldoende zichtbaar te blijven in het landschap van meldpunten.

Hoewel de vraag welke bijdrage de Fraudehelpdesk heeft geleverd aan het zo goed mogelijk ondersteunen van slachtoffers en het weerbaarder maken van burgers en bedrijven tegen (poging) tot oplichting niet nauwkeurig te beantwoorden is, lijkt de Fraudehelpdesk wel meerwaarde te hebben. Bevindingen uit het vragenlijstonderzoek geven een indicatie van de mate waarin slachtoffers van fraude zich ondersteund voelen. De uitkomsten van het vragenlijstonderzoek ondersteunen gedeeltelijk de veronderstelling dat slachtoffers ondersteund worden, aangezien de helft van de respondenten tevreden is over de wijze waarop ze door de Fraudehelpdesk zijn geholpen en 61% van de respondenten het gevoel heeft naar de juiste organisatie te zijn doorverwezen. Toch blijkt uit het vragenlijstonderzoek ook dat lang niet alle respondenten tevreden zijn over de wijze waarop ze door de Fraudehelpdesk zijn geholpen. Dit lijkt met name te komen door het feit dat een deel van de melders een andere verwachting had van de Fraudehelpdesk, namelijk dat er actie zou worden ondernomen tegen de fraudeur.

Er is geen directe informatiebron gevonden die inzicht geeft in de bijdrage van de Fraudehelpdesk aan het weerbaarder maken van burgers en bedrijven tegen (poging) tot oplichting. Afgaande op interviews met ketenpartners is het aannemelijk dat de Fraudehelpdesk bijdraagt aan het weerbaarder maken van burgers en bedrijven, zeker als het gaat om het geven van voorlichting. Zoals gezegd kunnen op basis van de literatuur wel enkele kritische kanttekeningen worden gemaakt over de effectiviteit van het verstrekken van algemene informatie door bijvoorbeeld campagnes.

4. Welke positie bekleedt de Fraudehelpdesk in het veld van de Nederlandse fraudepreventie en -bestrijding?

Hoofdstuk 6 bevat een verslag van het onderzoek naar het landschap van horizontale meldpunten in Nederland en geeft antwoord op deelvraag 12. Uit het onderzoek blijkt dat er tal van organisaties zijn waar slachtoffers van fraude zich kunnen melden. Daarnaast zijn er ook hulppunten waar geen melding kan worden gedaan, maar die voornamelijk inzetten op preventie door voorlichting. In dit onderzoek zijn in totaal 65 meld- en hulppunten geïventariseerd. Uit de reconstructie van de beleidstheorie blijkt dat het idee van het oprichten van een helpdesk was dat er één laagdrempelig centraal meldpunt zou worden opgericht waardoor slachtoffers ondersteund worden. Van één centraal meldpunt lijkt geen sprake. Zoals ook in 2015 werd geconstateerd in een onderzoek naar de synergie van horizontale meldpunten, blijkt ook uit deze evaluatie dat het huidige landschap, door de veelheid en verschillende vormen en functies van meldpunten, diffuus is.

De Fraudehelpdesk gebruikt meldingen over (potentiële) fraude om een bijdrage te leveren aan de voorkant van de fraudebestrijdingsketen (preventie en ondersteuning slachtoffers) en niet aan de achterkant van de keten (aanpakken en onderzoeken van fraudezaken). Hierin onderscheidt de Fraudehelpdesk zich van een groot aantal meldpunten dat onderdeel uitmaakt van grotere bedrijven, instellingen of publieke meldpunten die meldingen verzamelen als aanleiding voor onderzoek en opsporing of om maatregelen tegen fraudeurs te kunnen treffen. Daarnaast richt het merendeel van de meldpunten verbonden aan een groter bedrijf of instelling zich op specifieke vormen van fraude die niet altijd direct burgers of kleine ondernemers raken.

Twee meldpunten die zich wel op specifieke vormen van fraude richten en burgers direct raken zijn het LMIO (internetoplichting) en het CMI (identiteitsfraude). Deze meldpunten hebben echter geen overkoepelend beeld van ontwikkelingen op het gebied van horizontale fraude. Burgers kunnen als zij slachtoffer zijn geworden, ook terecht bij Slachtofferhulp Nederland en Meld Misdaad Anoniem. Deze organisaties richten zich niet op een specifieke vorm van fraude, maar op alle soorten criminaliteit of ingrijpende gebeurtenissen. De doelen van deze organisaties verschillen van de Fraudehelpdesk, in die zin dat Slachtofferhulp zich vooral richt op de ondersteuning van slachtoffers. Meld Misdaad Anoniem stuurt meldingen door naar de Politie en andere opsporingsdiensten en is minder gericht op preventie.

Uit de inventarisatie volgt dat naast de Fraudehelpdesk veel andere organisaties en platforms waarschuwen voor fraude. Uit de gesprekken met ketenpartners blijkt dat ketenpartners die zich ook op preventie van fraude richten elkaar onderling steeds beter weten te vinden en elkaar daarin versterken.

Kortgezegd bekleedt de Fraudehelpdesk een unieke positie in het veld van Nederlandse fraudepreventie, door het feit dat er geen enkele instelling of organisatie is die specifiek op alle vormen van fraude is toegesneden. Wel zijn er ander meldpunten en platformen die een deel van deze of andere diensten verlenen, maar die richten zich dan op één of enkele vormen van fraude. Ten slotte is het beeld dat bij een groot deel van de meldpunten of websites digitaal melding kan worden gemaakt en slachtoffers door middel van informatie op de websites worden doorverwezen naar ketenpartners. Laagdrempelig persoonlijk contact met een medewerker, zoals de Fraudehelpdesk biedt, is dus niet bij alle meldpunten mogelijk, terwijl slachtoffers hier mogelijk wel behoefte aan hebben.

5. Hoe zou de toekomstige doelbereiking van de Fraudehelpdesk (verder) kunnen worden verbeterd? Zijn er structurele of procesmatige aanpassingen nodig om de toekomstige bijdrage van de Fraudehelpdesk aan fraudepreventie en bestrijding in Nederland te verbeteren?

In de interviews met de Fraudehelpdesk, ketenpartners en de expertmeeting is aandacht besteed aan de knelpunten op het gebied van de dienstverlening van de Fraudehelpdesk en de neveneffecten die daar eventueel aan verbonden zijn (deelvraag 10 en 11).

Van ‘melddesk’ naar ‘helpdesk’

In de gesprekken met ketenpartners is aangegeven dat de naam ‘Fraudehelpdesk’ impliceert dat slachtoffers (inhoudelijk) worden geholpen. Dit is in beperkte mate het geval, waardoor de Fraudehelpdesk meer lijkt op een ‘melddesk’ dan op een ‘helpdesk’. Uit het vragenlijst onderzoek blijkt dat 22% van de respondenten (zeer) ontevreden is over de wijze waarop ze door de Fraudehelpdesk zijn geholpen. Een van de belangrijkste oorzaken hiervan lijkt dat de melders een andere verwachting hadden van de dienstverlening door de Fraudehelpdesk; ze hadden verwacht dat er door de Fraudehelpdesk actie zou worden ondernomen. In de expertmeeting gaven ketenpartners aan dat de Fraudehelpdesk de dienstverlening kan verbeteren door slachtoffers niet alleen door te verwijzen maar ook te begeleiden. Aan praktische ondersteuning voor slachtoffers, toegesneden op fraude, lijkt het te ontbreken.¹⁸⁰ Sommige slachtoffers hebben wellicht behoefte aan ondersteuning bij het doen van aangifte of het invullen van een formulier bij een instantie. Ketenpartners zien een doorontwikkeling van de Fraudehelpdesk van koude overdracht naar warme of tenminste lauwwarme overdracht als meerwaarde.

De Fraudehelpdesk beschikt over waardevolle data, maar kan daar meer mee doen

De Fraudehelpdesk beschikt volgens de meerderheid van de ketenpartners over relevante en waardevolle informatie. De trends en ontwikkelingen die de Fraudehelpdesk signaleert worden over het algemeen ook herkend door ketenpartners. Wel geeft de informatie van de Fraudehelpdesk geen compleet beeld als het gaat om onder meer schadebedragen en aantallen slachtoffers. In de expertmeeting is aangegeven dat het waardevol zou zijn informatie van verschillende ketenpartners samen te brengen, zodat een meer compleet beeld ontstaat van de actuele stand van zaken rondom fraude. Daarnaast zou het inzicht van de Fraudehelpdesk

¹⁸⁰ Zie ook Homburg en Van den Tillaart 2015, p. 19 die in hun onderzoek uit 2015 hetzelfde constateerden.

in modus operandi ketenpartners kunnen helpen om barrières op te werpen tegen (potentiële) fraudeurs.

Versterken van de beleidsinhoudelijke relatie tussen het ministerie en de Fraudehelpdesk

Al jaren is preventie een van de belangrijkste pijlers van het fraudebeleid van het ministerie van JenV. In het kader van preventie verleent het ministerie subsidie aan de Fraudehelpdesk. Uit onder meer gesprekken met de Fraudehelpdesk volgt dat er de laatste jaren nauwelijks inhoudelijke afstemming is tussen het ministerie en de Fraudehelpdesk. Ook lijkt sturing vanuit het ministerie door middel van het stellen van subsidievoorwaarden de laatste jaren beperkt te zijn. Er zijn geen output/outcome-afspraken over de geleverde diensten. De doelbereiking van de Fraudehelpdesk kan verder worden verbeterd door in te zetten op structurele inhoudelijke afstemming met het ministerie over onder meer trends en ontwikkelingen, zodat deze informatie een bijdrage levert aan toekomstig beleid. Het ministerie heeft aangegeven dat het passend is om in de toekomst meer vraaggestuurd te gaan samenwerken vanuit een meerjarige beleidsvisie, maar eerst onderzoek te willen laten doen naar de bijdrage van de inrichting van de Fraudehelpdesk aan het behalen van de doelstellingen.¹⁸¹ De Fraudehelpdesk en het ministerie lijken het erover eens dat de beleidsinhoudelijke relatie voor verbetering vatbaar is.¹⁸²

Continuïteit en stabiliteit in de financiering van de Fraudehelpdesk

De Fraudehelpdesk geeft aan dat de jaarlijkse subsidietoekenning veel financiële onzekerheid oplevert over de continuïteit van de organisatie en de Fraudehelpdesk beperkt in ontwikkelambities. Het is begrijpelijk dat de subsidiesystematiek een jaarlijkse cyclus kent, maar de inbedding in een meerjarenrelatie zou de Fraudehelpdesk meer stabiliteit geven en minder kwetsbaar maken.

Persoonsgegevens van strafrechtelijke aard

Zoals in hoofdstuk 3 is toegelicht is voor het mogen verwerken van persoonsgegevens van strafrechtelijke aard ten behoeve van derden een vergunning van de AP vereist. De aanvraag voor een vergunning door de Fraudehelpdesk voor het mogen verwerken van deze persoonsgegevens ten behoeve van de helpdeskfunctie heeft de AP afgewezen. Ten tijde van dit onderzoek loopt een beroepszaak tegen het besluit van de AP. De AP is van oordeel dat de Fraudehelpdesk melders ook kan adviseren door alleen gebruikt te maken van informatie over de modus operandi. Met informatie over de wijze waarop de (vermeende) fraude heeft plaatsgevonden, moet de Fraudehelpdesk de melder zodanig kunnen adviseren en informeren dat de melder weet of hij slachtoffer is geworden van fraude, welk type fraude het betreft, of hoe hij daar met behulp van informatie van de Fraudehelpdesk achter kan komen.

De Fraudehelpdesk ervaart het niet mogen verwerken van persoonsgegevens van strafrechtelijke aard aan de andere kant als een belemmering voor het kunnen bieden van een optimale dienstverlening. De Fraudehelpdesk geeft aan dat de melders beter zouden kunnen worden geholpen als ook persoonsgegevens van strafrechtelijke aard zouden mogen worden verwerkt. Voor het behandelen van een melding is het nodig een goed beeld te krijgen van de situatie. Daarvoor is volgens de Fraudehelpdesk kennis van de onderliggende stukken van de melding (die persoonsgegevens van strafrechtelijke aard kunnen bevatten) noodzakelijk. Die

¹⁸¹ Subsidietoekenning, 26 januari 2023.

¹⁸² Subsidietoekenning, 26 januari 2023.

informatie is nodig om vast te stellen of de melder te maken heeft met een legitiem bericht en om de melder op de juiste wijze te kunnen adviseren.¹⁸³ Uit het vragenlijstonderzoek blijkt dat meer dan de helft van de respondenten (56%) tevreden is over het advies van de Fraudehelpdesk. In die zin lijkt, ondanks dat de Fraudehelpdesk op dit moment geen gegevens over de (mogelijke) fraudeur mag verwerken, geen sprake te zijn van een grote ontevredenheid over de adviezen van de Fraudehelpdesk.

De meningen van ketenpartners over de meerwaarde van het delen van persoonsgegevens tussen organisaties zijn verdeeld. Een aantal ketenpartners is met de Fraudehelpdesk van mening dat door het delen van gegevens over fraudeurs, fraude beter kan worden bestreden. Enkele ketenpartners die deelnamen aan de expertmeeting zagen niet direct die noodzaak en wierpen de vraag op in hoeverre het bestrijden van fraude door de Fraudehelpdesk past bij de doelstellingen waarvoor de Fraudehelpdesk is opgericht. Zij gaven aan dat het passender zou zijn om eerst de huidige dienstverlening te verbeteren.

Persoonsgegevens van strafrechtelijke aard zijn gevoelige gegevens. Het delen van persoonsgegevens van strafrechtelijke aard met andere partijen kan een aanzienlijke inbreuk maken op de persoonlijke levenssfeer van betrokkenen. Uit de beleidsreconstructie volgt dat de Fraudehelpdesk is opgericht om met name aan de voorkant van de fraudebestrijdingsketen (preventie en ondersteuning van slachtoffers) een bijdrage te leveren. Met het delen van persoonsgegevens over fraudeurs aan andere organisaties zal de Fraudehelpdesk meer aan de achterkant (aanpakken van fraude) actief worden. Gelet op de doelstellingen die uit de beleidsreconstructie naar voren kwamen lijkt die inzet aan de achterkant dus niet voor de hand te liggen.

Duidelijk is dat wanneer er een politieke en maatschappelijke wens bestaat voor het verwerken van persoonsgegevens van strafrechtelijke aard door de Fraudehelpdesk, en de AP geen vergunning verleent, het nodig is hiervoor een expliciete wettelijke grondslag te creëren.

7.3 Conclusie

De Fraudehelpdesk is ruim tien jaar geleden opgericht. Aanleiding voor het oprichten van een helpdesk was dat inzicht in aard en omvang van fraude ontbrak. Er was behoefte aan meer inzicht in soorten horizontale fraude en modus operandi. Daarnaast werd het noodzakelijk geacht meer fraudebewustzijn onder burgers en kleine ondernemers te creëren en slachtoffers te ondersteunen. In de loop der jaren is (horizontale) fraude steeds hoger op de politieke en beleidsmatige agenda's terecht gekomen en ziet het ministerie preventie als de meest effectieve inzet voor het voorkomen van fraude. In dat kader zijn verschillende beleidsinitiatieven opgezet zoals de integrale aanpak cybercrime in 2018 en de integrale aanpak online fraude in 2022.

Het idee in 2010 was dat de helpdesk burgers en kleine ondernemers zou doorverwijzen als zij slachtoffer van fraude waren geworden, algemene informatie zou verstrekken om burgers en ondernemers weerbaarder te maken tegen pogingen tot fraude en meldingen zou registreren. De wijze waarop de Fraudehelpdesk ruim tien jaar na de oprichting deze diensten in de

¹⁸³ Fraudehelpdesk, aanvulling beroepsschrift tegen het besluit met kenmerk z2021-14398, 22 mei 2022, p. 9.

praktijk verleent, lijkt overeen te komen met het oorspronkelijke idee zoals dat ook was vastgelegd in de subsidievoorwaarden die bij de oprichting waren opgesteld. De kwaliteit van de dienstverlening wordt bovendien over het algemeen positief beoordeeld door ketenpartners en melders.

Ketenpartners zien meerwaarde in de Fraudehelpdesk, met name op het gebied van preventie. Uit interviews met de Fraudehelpdesk en deskresearch blijkt dat de Fraudehelpdesk jaarlijks (in samenwerking met ketenpartners) campagnes opzet, waarschuwingsberichten over actuele fraudevormen plaatst en een maandmonitor met actuele informatie over trends en ontwikkelingen uitbrengt. Hoewel ketenpartners meerwaarde inzien van de Fraudehelpdesk op het gebied van preventie worden in de literatuur kritische kanttekeningen geplaatst bij de effectiviteit van het verstrekken van algemene informatie via bijvoorbeeld campagnes.¹⁸⁴ Of campagnes en waarschuwingsberichten tot een gedragsverandering bij burgers en ondernemers leiden is zeer de vraag. Uit verschillende onderzoeken blijkt dat er bij interventies om gedrag te veranderen sprake moet zijn van een goede timing, interactie en een op een specifieke doelgroep gerichte informatie.¹⁸⁵ Experts van onderzoek naar cybergedrag geven bijvoorbeeld aan dat advies over veilig cybergedrag leerzamer is en sneller wordt overgenomen, wanneer dat gegeven wordt op het moment dat de onveilige gedraging (bijna) plaatsvindt.¹⁸⁶ Campagnes en de waarschuwingsberichten op de website en sociale media lijken niet aan (al) deze voorwaarden te voldoen.

De Fraudehelpdesk heeft volgens ketenpartners ook meerwaarde omdat de helpdesk beschikt over relevante en waardevolle informatie. De trends en ontwikkelingen die de Fraudehelpdesk signaleert worden over het algemeen herkend en kunnen ketenpartners helpen tijdig signalen op te pakken. Wel komt uit de interviews naar voren dat het, om meer zicht te krijgen en daardoor fraude beter te kunnen voorkomen, van belang is informatie op het gebied van trends, fraudevormen en modus operandi die bij ketenpartners ligt bij elkaar te brengen. Daarbij hoeven niet direct persoonsgegevens van strafrechtelijke aard te worden gedeeld, omdat het kan gaan om gegevens op geabstraheerd niveau die niet tot personen herleidbaar is. Mogelijk ligt hier een rol voor de Fraudehelpdesk. Hierbij wordt opgemerkt dat het beter zicht krijgen op verschillende verschijningsvormen en trends ook een van de actiepunten is in het actieplan van de integrale aanpak online fraude. Vanuit het ministerie, dat regie voert op de integrale aanpak, wordt hier al op ingezet.¹⁸⁷

Uit de beleidsreconstructie blijkt dat het doel was om slachtoffers te *ondersteunen*. De uitkomsten van het vragenlijstonderzoek ondersteunen gedeeltelijk de veronderstelling dat slachtoffers ondersteund worden, aangezien de helft van de respondenten tevreden is over de wijze waarop ze door de Fraudehelpdesk zijn geholpen en 61% van de respondenten het gevoel heeft naar de juiste organisatie te zijn doorverwezen. Wel lijkt de Fraudehelpdesk op dit moment meer op een melddesk dan een helpdesk, terwijl de naam wel suggereert dat een melder daadwerkelijk wordt geholpen. Warm doorverwijzen zou vanuit het perspectief van het slachtoffer meerwaarde hebben. Slachtoffers hoeven dan niet meerdere keren hun verhaal te vertellen. Bovendien haken bij koud doorverwijzen veel melders af. Een deel van de informatie gaat op dit moment dus verloren. Maar warm doorverwijzen stuit op juridische

¹⁸⁴ Bada e.a. 2015; Van 't Hoff- de Goede e.a. 2020, p. 124; Jansen e.a. 2019, p.103.

¹⁸⁵ Bullée en Junger 2020, p. 102; Van 't Hoff- de Goede e.a. 2020, p.123.

¹⁸⁶ Van 't Hoff- de Goede e.a. 2020, p.123.

¹⁸⁷ Actieplan integrale aanpak online fraude, p.7.

bezwaren vanwege de persoonsgegevens die dan moeten worden doorgegeven. Andere mogelijkheden om slachtoffers beter te ondersteunen zijn het bieden van hulp bij het doen van aangifte, het invullen van formulieren of het verhalen van schade.

Uit de beleidsreconstructie blijkt dat het idee destijds was om één helpdesk op te richten waar burgers én bedrijven terechtkonden voor advies en antwoorden op vragen op het gebied van financieel-economische criminaliteit.¹⁸⁸ Tegenwoordig zijn er tal van meld- en hulppunten voor horizontale fraude, waarvan de Fraudehelpdesk er één is. Uit het onderzoek naar het landschap van fraudemeldpunten blijkt dat de Fraudehelpdesk geen diensten verleent die uniek zijn, maar de combinatie van diensten en de brede oriëntatie op alle vormen van fraude zijn in het landschap van fraudemeldpunten wel uniek. De Fraudehelpdesk is de enige organisatie die speciaal in het leven is geroepen om zich specifiek bezig te houden met alle vormen van fraude.

Het ministerie wil deze evaluatie afwachten voor nadere besluitvorming voor de herijking van zowel de beleids- als de financieringsrelatie met de Fraudehelpdesk. Voor wat betreft de toekomst van de Fraudehelpdesk zijn verschillende ontwikkelrichtingen denkbaar. Op basis van dit onderzoek is het niet mogelijk eenduidige uitspraken te doen over de bijdrage die de Fraudehelpdesk, wanneer de Fraudehelpdesk de werkzaamheden op de huidige wijze voortzet, zal leveren aan het ondersteunen van slachtoffers en het weerbaarder maken van burgers en bedrijven tegen (pogingen) tot fraude. Wel lijkt de huidige dienstverlening van de Fraudehelpdesk gelet op de bevindingen van dit onderzoek een zekere meerwaarde te hebben op het gebied van preventie en het ondersteunen van slachtoffers.

Een andere mogelijkheid is dat de Fraudehelpdesk in de toekomst verdwijnt. In dat geval kan er op termijn een lacune op het gebied van fraudepreventie ontstaan. Zoals uit het onderzoek naar het landschap van fraudemeldpunten blijkt is de Fraudehelpdesk de enige organisatie die is toegespitst op alle vormen van fraude. Bij het verdwijnen van de Fraudehelpdesk, verdwijnt een organisatie die een overkoepelend beeld heeft en trends en ontwikkelingen signaleert over alle vormen van fraude. Uit de gesprekken met ketenpartners komt naar voren dat ketenpartners deze informatie, onder meer met het oog op preventie, nuttig achten. Op basis van dit onderzoek is het niet mogelijk uitspraken te doen of andere organisaties (een deel van) de diensten van de Fraudehelpdesk (kunnen) overnemen wanneer de Fraudehelpdesk verdwijnt.

Een laatste ontwikkelrichting is dat de Fraudehelpdesk de huidige dienstverlening doorontwikkelt. Daarbij kan gedacht worden aan het (praktisch) ondersteunen van slachtoffers en het bij elkaar brengen van informatie van ketenpartners op het gebied van trends en ontwikkelingen. Het doorontwikkelen van de huidige dienstverlening kan de meerwaarde van de Fraudehelpdesk (verder) vergroten. Het doorontwikkelen van diensten vraagt naar verwachting wel om meer tijd en capaciteit en dus om meer middelen.

¹⁸⁸ *Kamerstukken II 2008/09 29 911, nr. 32, p.2.*

Bijlage 1: Deelvragen

In hoeverre kunnen de doelen die de Fraudehelpdesk nastreeft in theorie via de geldende subsidievoorwaarden en het inrichtingsplan van de Fraudehelpdesk worden bereikt?

1. Wat is er beoogd met het oprichten van de Fraudehelpdesk? Welke doelen worden er met de Fraudehelpdesk nagestreefd?
2. Kunnen de beoogde doelen worden bereikt via het inrichtingsplan van de Fraudehelpdesk?
 - a. Via welke diensten dienen de doelen van de Fraudehelpdesk te worden bereikt?
 - b. Wat is de beleidstheorie achter deze doelen en diensten? Welke elementen/middelen en bedrijfsprocessen zijn voorzien voor het bereiken van deze doelen?
 - c. Wat zijn de veronderstelde werkzame mechanismen waarmee de doelen bereikt moeten worden?

In welke mate volstaat de praktische invulling van het inrichtingsplan van de Fraudehelpdesk in het bereikbaar maken van deze doelen?

3. Welke ontwikkelingen waren er sinds de evaluatie in 2012 met betrekking tot de financiering van de Fraudehelpdesk en de geleverde diensten door de Fraudehelpdesk?
 - a. Wat was de aanleiding voor de eventueel doorgevoerde aanpassingen?
4. Welke rol spelen de 23 formele subsidievoorwaarden die in de subsidieaankondiging uit 2010 zijn opgenomen in de uitvoering van de diensten van de Fraudehelpdesk?
 - a. In welke mate komt de Fraudehelpdesk in de praktijk tegemoet aan de subsidievoorwaarden?
 - b. Zijn er voorwaarden die in de praktijk overbodig blijken te zijn?
5. In welke mate kunnen via de praktische inrichting van de Fraudehelpdesk de gestelde doelen ook worden bereikt?
 - a. Welke middelen en bedrijfsprocessen worden hiertoe ingezet en in welke mate volstaan deze in de praktijk?

Welke bijdrage heeft de Fraudehelpdesk geleverd aan de preventie en bestrijding van horizontale fraude?

6. In welke mate voorziet de Fraudehelpdesk in een behoefte van burgers en bedrijven?
 - a. Wat is de naamsbekendheid van de Fraudehelpdesk?
 - b. In hoeverre is de website van de Fraudehelpdesk eenvoudig te vinden? Is de website van de Fraudehelpdesk ook te vinden via de website van haar partners (zoals politie en OM)?

- c. Hoeveel unieke bezoekers komen er op de website van de Fraudehelpdesk? Welke ontwikkeling was er sinds de evaluatie uit 2012? Hoe kan deze ontwikkeling worden verklaard?
 - d. Hoeveel meldingen en doorverwijzingen zijn er geregistreerd, om welke soorten ging het en hoe zijn deze afgehandeld? Welke ontwikkeling was er sinds de evaluatie uit 2012? Hoe kan deze ontwikkeling worden verklaard?
7. Wat kan er worden gezegd over de bijdrage van de Fraudehelpdesk aan het functioneren van de fraudebestrijdingsketen?
- a. Welke nieuwe fraudevormen heeft de Fraudehelpdesk gesignaleerd sinds de laatste evaluatie uit 2012? Op welke wijze heeft de Fraudehelpdesk aandacht besteed aan het waarschuwen van burgers en bedrijven tegen deze nieuwe fraudevormen?
 - b. In welke mate worden doorverwezen zaken ook opgepakt door de ketenpartners van de Fraudehelpdesk? Indien doorverwezen zaken niet worden opgepakt, wat zijn daarvoor de belangrijkste redenen?
8. Hoe beoordelen burgers en bedrijven die contact hebben gehad met de Fraudehelpdesk:
- a. de dienstverlening en
 - b. de verstrekte informatie en/of het advies?
9. Hoe oordelen de ketenpartners van de Fraudehelpdesk over de dienstverlening van de helpdesk? Hoe kan de dienstverlening van de Fraudehelpdesk volgens de ketenpartners (verder) worden verbeterd?

Hoe zou de toekomstige doelbereiking van de Fraudehelpdesk (verder) kunnen worden verbeterd? Zijn er structurele of procesmatige aanpassingen nodig om de toekomstige bijdrage van de Fraudehelpdesk aan fraudepreventie en bestrijding in Nederland te verbeteren?

10. Zijn er momenteel knelpunten die de bijdrage van de Fraudehelpdesk aan de preventie en bestrijding van fraude hinderen of in de weg staan? Welke zijn dat?
11. Zijn er neveneffecten verbonden aan de dienstverlening door de Fraudehelpdesk? Welke zijn dat en hoe kunnen deze worden geëlimineerd?

Welke positie bekleedt de Fraudehelpdesk in het veld van de Nederlandse fraudepreventie en -bestrijding?

12. Welke loketten zijn er naast de Fraudehelpdesk in Nederland voor het melden van slachtofferschap en informatie over horizontale fraude en oplichting (onder burgers en bedrijven)? Wat is de specifieke rol van de meldpunten?
- a. Welke overlap is er in de diensten die de diverse meldpunten aanbieden?
 - b. Welke diensten van de Fraudehelpdesk zijn uniek?

Bijlage 2: Geraadpleegde documenten

Akkermans e.a. 2022

M. Akkermans, J. Arends, E. Derksen, C. Reep, *Online Veiligheid en Criminaliteit 2022*, CBS, mei 2023.

Bada e.a. 2015

M. Bada, A. Sasse, en J. Nurse, *Cyber security awareness campaigns: Why do they fail to change behaviour?* International Conference on Cyber Security for Sustainable Society, 2015.

Beerthuizen e.a. 2020

M.G.C.J. Beerthuizen, T. Sipma en A.M. van der Laan, *Aard en omvang van dader- en slachtofferschap van cyber- en gedigitaliseerde criminaliteit in Nederland*, WODC 2020.

Bullée en Junger 2020

J.W.H. Bullée & M. Junger, Social engineering: digitale fraude en misleiding, *Justitiële Verkenningen*, 46, 2020.

Bullée en Junger 2020

J.W.H. Bullée & M. Junger, How effective are social engineering interventions? A meta-analysis, *Information and Computer Security*, 28/5, 2020.

Button e.a. 2009

M. Button, C. Lewis & J. A. Tapley, *A better deal for victims*. London: National Fraud Authority 2009.

Conradie en Doms 2022

M. Conradie en B. Doms, *Cybersecurity onderzoek. Alert Online 2022*, I&O Research 2022.

Cross e.a. 2016

C. Cross, K. Richards & R. Smith, *Improving responses to online fraud victims: An examination of reporting and support*, Criminology Research Advisory Council 2016.

Cross 2018

C. Cross, Expectations vs reality: Responding to online fraud across the fraud justice network, *Elsevier*, 55, 2018.

Jansen e.a. 2019

J. Jansen, S. Westers, S. Twickler & W. Stol, Aankoopfraude vanuit het buitenland, alternatieven voor opsporing, *Politiekunde 99*, Den Haag: Sdu.

Leukfeldt e.a. 2018

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

Tromp e.a. 2010

N. Tromp, J. Snippe, B. Bieleman en E. de Bie, *Preventieve maatregelen horizontale fraude*, Intraval 2010.

Van 't Hoff-de Goede e.a. 2019

S. van 't Hoff-de Goede, R. van der Kleij, S. van de Weijer & R. Leukfeldt, *Hoe veilig gedragen wij ons online? Een studie naar de samenhang tussen kennis, gelegenheid, motivatie en online gedrag van Nederlanders*, WODC: 2019.

Van de Weijer en Leukfeldt 2023

S. van de Weijer en R. Leukfeldt, *Cybercriminaliteit tijdens de coronacrisis. Aard, omvang en impact van cyberrisico's voor burgers en het mkb*, NCSR en De Haagse Hogeschool, Amsterdam: 2023.

Van der Kleij e.a. 2020

R. Van der Kleij, S. van 't Hoff-de Goede, S. van de Weijer, R. Leukfeldt, Ons cybergedrag is veel onveilig dan we zelf denken. Implicaties voor effectief beïnvloedingsbeleid door overheid. *Justitiële verkenningen*. Nieuwe vormen van oplichting en fraude, jrg. 46, nr. 2, 2020.

Kamerstukken

Kamerstukken II 2007/2008 (handelingen), 28-2191.
Kamerstukken II 2007/2008, 28684, nr. 116, bijlage 1.
Kamerstukken II 2007/2008, 28684, nr. 119.
Kamerstukken II 2007/2008, 29 911, nr. 10.
Kamerstukken II 2007/2008, 31200 VI, nr. 48.
Kamerstukken II 2008/2009 (handelingen), 29911, nr. 22.
Kamerstukken II 2008/2009, 29911, nr. 32.
Kamerstukken II 2009/2010, 29911, nr. 35.
Kamerstukken II 2009/2010, 29911, nr. 37.
Kamerstukken II 2009/2010 (handelingen), 29911, nr. 39.
Kamerstukken II 2009/2010 (handelingen), 29911, nr. 41.
Kamerstukken II 2012/2013, 33400 VI, nr. 149.
Kamerstukken II 2019/2020 (handelingen), 26 643, nr. 679.

Documenten ontvangen van de Fraudehelpdesk

- Maandmonitoren augustus 2022 tot en met januari 2023
- Naamsbekendheidonderzoeken 2014, 2016, 2018, 2020, 2022
- Aantallen van het aantal websitebezoekers
- Jaarverslagen 2011, 2012 en 2013
- Communicatieplan 2023

- Functieboek
- Ontwikkelagenda
- Organogram
- Statuten 2007 en 2014
- Kennisgeving subsidie Helpdesk Finec, 20 september 2010
- Subsidietoekenningen 2014, 2015, 2017 – 2020 EZK
- Eindafrekening subsidie 2013, 2014, 2016, 2017, 2018 EZK
- Eindafrekening subsidie 2016, EZK
- Subsidietoekenningen 2012, 2013 2019 - 2023, JenV
- Eenmalige subsidie t.b.v. NPC project acquisitiefraude
- Wijziging subsidiebesluit 2020, JenV
- Wijziging subsidiebesluit 2022, JenV
- Restbedrag exploitatiesubsidie Fraudehelpdesk 2021
- Beslissing op bezwaren tegen de subsidiebesluiten van 13 februari en 2 september 2020
- DPIA helpdeskfunctie, 6 november 2020
- Protocol helpdesk, 6 november 2020
- Beslissing op bezwaar van de Autoriteit Persoonsgegevens, 3 februari 2022 (z2021-14398)
- Beroepsschrift tegen het besluit op bezwaar van de Autoriteit Persoonsgegevens, 22 mei 2022
- Besluit van de Autoriteit Persoonsgegevens, 12 juli 2021 (z2020-18959)

Overige documenten met betrekking tot de vergunningaanvraag bij de AP

Besluit z2018-12010, Autoriteit Persoonsgegevens 19 juni 2019 (Besluit inzake de vergunningaanvraag voor de verwerking van gegevens van strafrechtelijke aard ten behoeve van derden van de verwerking 'Fraudehelpdesk' van Safecin).

Bijlage 3: Lijst met gesprekspartners

Planevaluatie

- Beleidsmedewerker Rechtshandhaving en Criminaliteitsbestrijding, ministerie van JenV
- Senior beleidsmedewerker, Directie Veiligheid en Bestuur, ministerie van JenV
- Directeur Fraudehelpdesk
- Prof. em. dr. of Cyber Security and Business at University of Twente
- Lector Cybercrime & Cybersecurity bij de Haagse Hogeschool en senior onderzoeker cybercrime en coördinator van het cybercrime cluster van het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR)

Procesevaluatie: Fraudehelpdesk

- Directeur Fraudehelpdesk
- Voorzitter van de RvT van stichting SafeCin
- Lid van de RvT van stichting SafeCin
- Frontofficecoördinator
- Medewerker kwaliteit
- Medewerker frontoffice
- Woordvoerder
- Adviseur Marketing

Procesevaluatie: ketenpartners

- Beleidsmedewerker Rechtshandhaving en Criminaliteitsbestrijding, ministerie van JenV
- Senior beleidsmedewerker, Directie Veiligheid en Bestuur, ministerie van JenV
- CISO & Teamlead Veiligheid bij de Nederlandse Vereniging van Banken
- Teamleider Landelijk Meldpunt Internet Oplichting
- Beleidsmedewerker Slachtofferhulp Nederland
- Voorzitter RvT Stichting Slachtofferhulp Nederland
- Accountmanager Cybercrime, Politie Noord Nederland
- Landelijk coördinator bestrijding horizontale fraude bij het Openbaar Ministerie, Functioneel Parket
- Beleidssecretaris Criminaliteit, VNO-NCW en MKB-Nederland
- Senior toezichthouder, marktintegriteit en handhaving, AFM
- Senior medewerker, meldpunt financiële markten, AFM
- Communicatieadviseur en campagneleider, ACM
- Directeur ECC Nederland
- Manager Platform Veilig Ondernemen
- Hoofd communicatie en PR, ESET Nederland

Procesevaluatie: experts

- Prof. em. dr. of Cyber Security and Business at University of Twente
- Lector Cybercrime & Cybersecurity bij de Haagse Hogeschool en senior onderzoeker cybercrime en coördinator van het cybercrime cluster van het Nederlands Studiecentrum Criminaliteit en Rechtshandhaving (NSCR)

Deelnemers expertmeeting

- Beleidsmedewerker, ministerie van JenV
- Projectleider, Landelijk Meldpunt Internetoplichting Politie
- Landelijk coördinator bestrijding horizontale fraude bij het Openbaar Ministerie, Functioneel Parket
- Adviseur, Ouderenbond Anbo
- Manager Media, Ouderenbond Seniorweb
- Prof. em. dr. of Cyber Security and Business at University of Twente
- Twee adviseurs informatie & expertise, Centraal Meldpunt Identiteitsfraude

Bijlage 4: Vragenlijst melders FHD

Introductie

Heeft u als particulier of namens uw bedrijf een melding gedaan?

- Particulier
- Namens mijn bedrijf
- Weet ik niet

Op welke manier heeft u een melding gedaan?

- Telefonisch
- Via het formulier op de website van de Fraudehelpdesk
- Telefonisch en via het formulier op de website van de Fraudehelpdesk
- Anders
- Weet ik niet

Waarom heeft u contact gezocht met de Fraudehelpdesk?

- Ik had een algemene vraag
- Ik was opgelicht
- Ik was misschien opgelicht
- Ik wilde een melding doen van een poging tot oplichting
- Weet ik niet
- Anders: ...

Waardering dienstverlening

Binnen welke termijn werd uw melding beantwoord?

- Binnen twee werkdagen
- Binnen een week
- Langer dan een week
- Weet ik niet

Stelling: ik ben tevreden over de wijze waarop ik door de Fraudehelpdesk ben geholpen

- Helemaal mee oneens
- Mee oneens
- Neutraal
- Mee eens
- Helemaal mee eens
- Weet ik niet

Bij de antwoorden (helemaal) oneens: waarom bent u het (helemaal) oneens met deze stelling?

Hieronder ziet u vijf stellingen. Per stelling kunt u aangeven in hoeverre u het met de stelling eens bent of niet.

1. De medewerker die mij adviseerde was vriendelijk
2. De medewerker die mij adviseerde was deskundig
3. De medewerker die mij adviseerde was hulpvaardig

4. Het advies dat ik kreeg was duidelijk
5. Het contact met de Fraudehelpdesk voldeed aan mijn verwachtingen

- Helemaal mee oneens
- Mee oneens
- Neutraal
- Mee eens
- Helemaal mee eens
- Weet ik niet

Heeft de Fraudehelpdesk u doorverwezen naar een andere organisatie (bijvoorbeeld naar de politie of Slachtofferhulp)?

- Ja
- Nee
- Weet ik niet

Bij 'ja' op de vorige vraag verscheen de volgende stelling:

Ik heb het gevoel dat ik naar de juiste organisatie ben doorverwezen.

- Helemaal mee oneens
- Mee oneens
- Neutraal
- Mee eens
- Helemaal mee eens
- Weet ik niet

Heeft u ideeën over hoe de Fraudehelpdesk in de toekomst melders beter kan helpen?

- Ja
- Nee
- Weet ik niet

Bij 'ja' op de vorige vraag verscheen een tekstblok om idee(ën) in te vullen.

Afsluiting

We willen in aanvulling op deze vragenlijst ook graag een paar korte telefoongesprekken voeren. Het doel van dat gesprek is om een nog scherper beeld te krijgen van hoe het met de Fraudehelpdesk gaat. Wilt u daaraan meewerken?

- Ja
- Nee

Bij 'ja': U kunt hieronder uw e-mailadres en/of telefoonnummer achterlaten. We gebruiken uw gegevens enkel om contact met u op te nemen en vernietigen de informatie nadat we telefonisch contact met u hebben gehad.

Bijlage 5: Externe communicatie en projecten¹⁸⁹

Jaar	Activiteit
2012	Campagne over halfvijf fraude tijdens de Week van de Veiligheid Project Acquisitiefraude/Mass Marketingfraude i.s.m. NPC
2013	Project Acquisitiefraude/Mass Marketingfraude in samenwerking met het NPC
2014	Fraudebus. Doel van het experiment was om de plaatselijke bevolking voor te lichten over fraudeverschijningsvormen op het gebied van dating, vacatures en identiteit met aansprekend voorlichtingsmateriaal. Een reclamemast over datingfraude, een televisiespotje gericht op ondernemers over het voorkomen van identiteitsfraude op vijf regionale zenders en een radiospot over datingfraude via vijf regionale zenders.
2015	Vijf reclamemasten voor vakantiefraude, een tv-spot over de risico's van online bestellen van het ene bedrijf bij het andere bedrijf bij vier regionale omroepen.
2016	Een tv-spot op Uitzending Gemist om naar de website van de Fraudehelpdesk te gaan, drie reclamemasten voor de gevaren van identiteitsfraude. Fraudelnfodesk. In het project werd ingezet op de samenwerking met het systeem van het Engelse Cifas, een anti-fraude organisatie die een cross-sectoraal fraudedata matching systeem heeft ingericht.
2017	Organisatie van het Fraudecongres.
2018	Zes betaalde reclame acties over identiteitsfraude in het bedrijfsleven en bij non-profitorganisaties, over zaken doen per e-mail, over CEO-fraude en datingfraude.
2019	Lanceren van een campagne over nephelpdesks in samenwerking met het ECP, lanceren van een campagne over nep-sms'sjes, inrichten van een campagne over CEO-fraude en een social media campagne over datingfraude. Participeren in een project samen met VNO-NCW, MKB Nederland, banken en andere private partijen. Dit project was gericht op de aanpak van ondermijning.
2020	Campagne ontwikkeld en uitgevoerd over beleggingsadvertenties in samenwerking met facebook en de AFM, campagne opgezet over BEC-fraude op verzoek van en in samenwerking met The Hague Security Delta, het OM, de Politie en andere betrokken organisaties. Naast deze campagnes heeft de Fraudehelpdesk ook andere campagnes uitgevoerd in 2020. Dit waren in totaal elf campagnes. Op initiatief van de Fraudehelpdesk in samenwerking met het ministerie van JenV, het CCV, de Politie en Slachtofferhulp Nederland is een minidocumentaire ontwikkeld als campagnemateriaal over datingfraude.
2021	Campagne ontwikkeld en uitgevoerd over hulpvraagfraude in samenwerking met Meta (grotendeels bekostigd door Facebook), een campagne over beleggingsfraude met de AFM, een campagne over kamer/woningverhuurfraude in samenwerking met OM en verschillende verhuurplatforms, en een campagne over vakantiefraude met ECC. In 2021 is gestart met het ontwikkelen van een online portaal, de zogenoemde FraudeHub. Via dit portaal kunnen ketenpartners centraal cijfers en campagnemateriaal op het gebied van fraude delen. De Fraudehelpdesk is hiervan de hostende partij.
2022	Campagne ontwikkeld en uitgevoerd over hulpvraagfraude in samenwerking met Meta, campagne over vakantie-gerelateerde fraude in samenwerking met het ECC, een campagne over schaamte in samenwerking met Slachtofferhulp Nederland, en een campagne over veilig aankopen via webshops samen met ACM, ECC, LMIO, JenV en de Consumentenbond, en een campagne over datingfraude. Ontwikkeling van Fraudehelpdesk zakelijk. Diensten die een meerwaarde voor de ondernemers (MKB en ZZP'ers) moeten realiseren.

¹⁸⁹ De informatie over opgezette en uitgevoerde campagnes, reclame-uitingen en projecten is afkomstig uit de jaarverslagen van 2012 tot en met 2022.

Bijlage 6: Websiteonderzoek

Hoofdcategorie	Zoekterm	Gemiddelde zoekvolume per maand	Positie Google	Zichtbaarheid
Acquisitiefraude	acquisitie fraude	20	1	Zichtbaar op de eerste resultatenpagina in Google
	advertentiefraude	20	3	Zichtbaar op de eerste resultatenpagina in Google
	acquisitiefraude betekenis	20	9	Zichtbaar op de eerste resultatenpagina in Google
	wat is advertentiefraude	10	4	Zichtbaar op de eerste resultatenpagina in Google
	opgelicht advertentiefraude	10	5	Zichtbaar op de eerste resultatenpagina in Google
	spookfacturen herkennen	10	1	Zichtbaar op de eerste resultatenpagina in Google
	spookfactuur melden	30	1	Zichtbaar op de eerste resultatenpagina in Google
	factuurfraude	50	22	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	fraude ceo	10	1	Zichtbaar op de eerste resultatenpagina in Google
	ceo fraude voorkomen	20	4	Zichtbaar op de eerste resultatenpagina in Google
	ceo-fraude	320	1	Zichtbaar op de eerste resultatenpagina in Google
	telefoonnummer fraude melden	10	1	Zichtbaar op de eerste resultatenpagina in Google
	telefoon fraude melden	40	1	Zichtbaar op de eerste resultatenpagina in Google
	telefoon fraudeurs	50	1	Zichtbaar op de eerste resultatenpagina in Google
	telefoonnummer fraudehelpdesk	20	1	Zichtbaar op de eerste resultatenpagina in Google
	fraude telefoonnummer	140	1	Zichtbaar op de eerste resultatenpagina in Google
	fraude telefoonnummer melden	50	2	Zichtbaar op de eerste resultatenpagina in Google
	fraude telefoontjes	30	1	Zichtbaar op de eerste resultatenpagina in Google
	fraude telefoon	20	1	Zichtbaar op de eerste resultatenpagina in Google
	fraude telefoon melden	10	1	Zichtbaar op de eerste resultatenpagina in Google
	fraude telefoonnummer zoeken	10	6	Zichtbaar op de eerste resultatenpagina in Google
	fraude via telefoon	20	3	Zichtbaar op de eerste resultatenpagina in Google
	fraude met telefoonnummer	10	1	Zichtbaar op de eerste resultatenpagina in Google
	fraude met telefoon	10	1	Zichtbaar op de eerste resultatenpagina in Google
	bsn fraude telefoon	10	1	Zichtbaar op de eerste resultatenpagina in Google
	bsn nummer fraude telefoon	10	1	Zichtbaar op de eerste resultatenpagina in Google
	verdacht telefoontje melden	40	1	Zichtbaar op de eerste resultatenpagina in Google
	verdacht telefoontje	10	1	Zichtbaar op de eerste resultatenpagina in Google
	verdachte telefoontjes melden	10	3	Zichtbaar op de eerste resultatenpagina in Google

Algemeen	fraude melden	1300	1	Zichtbaar op de eerste resultatenpagina in Google
	cybercrime	1000	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	cyber crimes	720	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	cybercrime melden	50	6	Zichtbaar op de eerste resultatenpagina in Google
	ik ben misleid	10	96	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	ik ben opgelicht	170	11	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	ik ben opgelicht door een bedrijf	10	6	Zichtbaar op de eerste resultatenpagina in Google
	ik ben opgelicht via internet	30	13	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	ik ben opgelicht wat kan ik doen	20	13	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	oplichting melden	320	1	Zichtbaar op de eerste resultatenpagina in Google
	fraude bedrijf melden	10	1	Zichtbaar op de eerste resultatenpagina in Google
	fraude bedrijf	20	3	Zichtbaar op de eerste resultatenpagina in Google
Beleggingsfraude	boilerroomfraude	590	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	wat is boilerroomfraude	50	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	ponzifraude	2400	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	piramidespel opgelicht	40	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	piramidefraude	20	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
Faillissementsfraude	faillissementsfraude melden	10	5	Zichtbaar op de eerste resultatenpagina in Google
	faillissementsfraude	170	12	Zichtbaar in Google, maar niet op de eerste resultatenpagina
Fraude met betaalmiddelen	afpersmail melden	10	1	Zichtbaar op de eerste resultatenpagina in Google
	hacking	14800	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	hacking melden	10	6	Zichtbaar op de eerste resultatenpagina in Google
	hack melden	10	5	Zichtbaar op de eerste resultatenpagina in Google
	hackers melden	10	5	Zichtbaar op de eerste resultatenpagina in Google
	telenet hacking melden	10	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	ransomware melden	10	20	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	malware melden	10	1	Zichtbaar op de eerste resultatenpagina in Google
	malware mail melden	10	1	Zichtbaar op de eerste resultatenpagina in Google
	malware herkennen	30	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	ransomware herkennen	10	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	Malware	3600	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	malware betekenis	720	74	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	ransomware	3600	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	ransomware betekenis	880	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	smishing	720	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
smishing betekenis	260	101	Niet zichtbaar binnen de eerste 10 pagina's van Google	

smishing herkennen	10	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
smishing melden	10	2	Zichtbaar op de eerste resultatenpagina in Google
smishing attack	20	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
smishing wat is dat	10	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
bankfraude	210	16	Zichtbaar in Google, maar niet op de eerste resultatenpagina
bankfraude melden	50	1	Zichtbaar op de eerste resultatenpagina in Google
bankfraude geld terug	40	50	Zichtbaar in Google, maar niet op de eerste resultatenpagina
fraude bankrekening	50	5	Zichtbaar op de eerste resultatenpagina in Google
fraude bank	40	7	Zichtbaar op de eerste resultatenpagina in Google
fraude bankpas	20	35	Zichtbaar in Google, maar niet op de eerste resultatenpagina
fraude bank melden	10	1	Zichtbaar op de eerste resultatenpagina in Google
fraude bankrekeningnummer	40	5	Zichtbaar op de eerste resultatenpagina in Google
ik ben opgelicht via tikkie	10	35	Zichtbaar in Google, maar niet op de eerste resultatenpagina
valse e-mail melden	30	1	Zichtbaar op de eerste resultatenpagina in Google
verdachte e-mail melden	10	1	Zichtbaar op de eerste resultatenpagina in Google
phishing e-mail melden	10	1	Zichtbaar op de eerste resultatenpagina in Google
ongewenste e-mail melden	10	3	Zichtbaar op de eerste resultatenpagina in Google
e mail melden	10	1	Zichtbaar op de eerste resultatenpagina in Google
afpersmail	30	1	Zichtbaar op de eerste resultatenpagina in Google
afpersmail ontvangen	20	1	Zichtbaar op de eerste resultatenpagina in Google
afpersmails	10	1	Zichtbaar op de eerste resultatenpagina in Google
phishing	8100	15	Zichtbaar in Google, maar niet op de eerste resultatenpagina
phishing mail	3600	1	Zichtbaar op de eerste resultatenpagina in Google
phishing betekenis	880	38	Zichtbaar in Google, maar niet op de eerste resultatenpagina
phishing melden	480	1	Zichtbaar op de eerste resultatenpagina in Google
phishing mail melden	390	1	Zichtbaar op de eerste resultatenpagina in Google
phishing telefoonnummers	140	4	Zichtbaar op de eerste resultatenpagina in Google
phishing sms melden	170	5	Zichtbaar op de eerste resultatenpagina in Google
skimmen	1900	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
skimmen betekenis	260	58	Zichtbaar in Google, maar niet op de eerste resultatenpagina
tikkie fraude herkennen	50	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
fraude creditcard	50	23	Zichtbaar in Google, maar niet op de eerste resultatenpagina
fraude met betaalproducten	50	8	Zichtbaar op de eerste resultatenpagina in Google
skimming voorkomen	10	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
skimmen voorkomen	10	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
phishing melden whatsapp	10	1	Zichtbaar op de eerste resultatenpagina in Google

	phishing melden sms	10	7	Zichtbaar op de eerste resultatenpagina in Google
	vishing	590	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	fraude met creditcard	20	23	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	phishing herkennen	70	27	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	creditcard fraude melden	20	6	Zichtbaar op de eerste resultatenpagina in Google
	e-skimming	10	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	slachtoffer van phishing	10	66	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	slachtoffer phishing mail	10	31	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	ik ben slachtoffer van phishing	10	19	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	tikkie fraude melden	30	14	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	phishing voorkomen	30	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	pinpasfraude	210	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	telefoonnummer melden phishing	10	3	Zichtbaar op de eerste resultatenpagina in Google
Fraude met online handel	domeinnaam oplichting	10	1	Zichtbaar op de eerste resultatenpagina in Google
	domeinnaamfraude	10	1	Zichtbaar op de eerste resultatenpagina in Google
	opgelicht domeinnaam	10	3	Zichtbaar op de eerste resultatenpagina in Google
	spoofing melden	50	1	Zichtbaar op de eerste resultatenpagina in Google
	spoof melden	50	1	Zichtbaar op de eerste resultatenpagina in Google
	spoofing telefoonnummer melden	20	1	Zichtbaar op de eerste resultatenpagina in Google
	spoofing	5400	16	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	spoofing betekenis	1000	19	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	spoofing voorkomen	110	26	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	spoofing email	390	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	spoofing bank	40	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	internetfraude melden	210	2	Zichtbaar op de eerste resultatenpagina in Google
	internetfraude helpdesk	10	1	Zichtbaar op de eerste resultatenpagina in Google
	fraude via internet	10	3	Zichtbaar op de eerste resultatenpagina in Google
	internetoplichting	260	7	Zichtbaar op de eerste resultatenpagina in Google
	internetoplichting bankrekeningnummers	10	11	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	valse webshops	10	5	Zichtbaar op de eerste resultatenpagina in Google
	valse website melden	20	1	Zichtbaar op de eerste resultatenpagina in Google
	valse websites	20	1	Zichtbaar op de eerste resultatenpagina in Google
	valse websites melden	20	1	Zichtbaar op de eerste resultatenpagina in Google
	internetoplichting melden	30	5	Zichtbaar op de eerste resultatenpagina in Google
Hypotheekfraude	hypotheekfraude melden	20	2	Zichtbaar op de eerste resultatenpagina in Google
	hypotheekfraude	170	101	Niet zichtbaar binnen de eerste 10 pagina's van Google

Identiteitsfraude	identiteitsfraude melden	140	11	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	identiteitsfraude voorkomen	70	41	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	ceo-fraude betekenis	20	2	Zichtbaar op de eerste resultatenpagina in Google
Telecomfraude	vriend-in-noodfraude	50	93	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	whatsappfraude	880	7	Zichtbaar op de eerste resultatenpagina in Google
	belfraude	30	6	Zichtbaar op de eerste resultatenpagina in Google
	telecomfraude	10	7	Zichtbaar op de eerste resultatenpagina in Google
	telefoonnummer melden	70	3	Zichtbaar op de eerste resultatenpagina in Google
Verzekeringsfraude	internetplichting verzekering	10	50	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	verzekeringsfraude melden	90	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
Voorschotfraude	kredietfraude	10	44	Zichtbaar in Google, maar niet op de eerste resultatenpagina
	fraude valsheid in geschrifte	10	101	Niet zichtbaar binnen de eerste 10 pagina's van Google
	erfenisfraude	30	3	Zichtbaar op de eerste resultatenpagina in Google
	fraude lening aanvraag	10	2	Zichtbaar op de eerste resultatenpagina in Google
	fraude lening	10	2	Zichtbaar op de eerste resultatenpagina in Google
	fraude met leningen	10	1	Zichtbaar op de eerste resultatenpagina in Google

Bijlage 7: Fraudemeldpunten horizontale fraude

Naam meldpunt	Beheerder	Type fraude	Registreren	Monitoren	Signaleren	Analyseren en onderzoeken	Voorlichting met het oog op preventie	Begeleiding/ondersteuning van slachtoffers	Doorverwijzen van slachtoffers naar andere org.	Aanpakken van fraudezaken
Autoriteit Consument en Markt	ACM	overig	1	1	1	1	1	0	1	1
Autoscout24	Autoscout24	meerdere vormen	1	0	0	0	1	0	0	0
Centraal Meldpunt Identiteitsfraude	Rijksdienst voor Identiteitsgegevens (BZK)	identiteitsfraude	1	0	1	0	1	1	0	0
Incidentenregisters van verschillende financiële instellingen en brancheverenigingen	Stichting CIS	meerdere vormen	1	0	0	0	0	0	0	0
Consumentenbond	Consumentenbond	meerdere vormen	1	0	0	0	1	1	1	0
Consuwijzer	ACM	meerdere vormen	1	1	0	1	1	0	1	0
Diverse bedrijven: Marktplaats	Marktplaats	meerdere vormen	1	0	0	0	1	0	1	0
Diverse bedrijven: Microsoft	Microsoft	overig	1	0	0	0	1	0	0	0
Financial Intelligence Unit	FIU	meerdere vormen	1	1	1	1	1	0	0	0
Fraudehelpdesk	Fraudehelpdesk	meerdere vormen	1	1	1	0	1	1	1	0
Fraudeloket Verzekeringsbedrijf	Onderdeel van het VVZ	verzekeringsfraude	1	1	1	1	0	0	0	1
Fraudeloket Zorg	PVV	verzekeringsfraude	1	0	1	0	0	0	0	0
Fraudemeldpunt Accountants KLPD	Politie	meerdere vormen	1	0	0	1	0	0	0	1

Fraudespreekuur Den Haag	Team Insolventies rechtbank Den Haag	faillissementsfraude	1	1	0	1	1	0	0	0
Informatiedesk FIOD	FIOD/Belastingdienst	meerdere vormen	1	1	1	1	0	0	0	1
Kansspelautoriteit	ZBO	overig	1	1	0	1	1	0	1	1
Kenniscentrum Fraudebeheersing in de Zorg	Zorgverzekeraars Nederland	verzekeringsfraude	1	0	0	1	0	0	0	0
Klokkenluiders VG	Klokkenluiders VG	verzekeringsfraude	1	1	1	1	0	1	0	0
Koninklijke vereniging Bloemist Winkeliers	Branchevereniging bloemisten	acquisitiefraude	1	1	0	0	1	0	1	0
Landelijk Meldpunt Internetoplichting	Politie	fraude met online handel	1	0	0	1	1	0	1	1
Maxmeldpunt.nl	Omroep MAX	meerdere vormen	1	0	0	0	1	1	1	0
Meld misdaad anoniem	Stichting M.	meerdere vormen	1	0	0	0	0	0	0	0
Meldpunt Financiële Markten Consumenten	AFM	meerdere vormen	1	1	0	1	0	0	0	1
Meldpunt Fraude in de Dentale Branche	Branchevereniging Tandtechniek	verzekeringsfraude	1	1	1	1	0	0	0	0
Meldpunt Integriteit Woningcorporaties	ILenT	overig	1	0	1	1	0	0	0	1
Meldpunt International Card services (ICS)	ICS	fraude met betaalmiddelen	1	0	0	0	1	0	0	1
Meldpunt wetenschappelijke Integriteit	NWO	overig	1	0	0	0	0	0	0	1
Meldpunten van banken: ING	ING	meerdere vormen	1	0	0	0	1	0	0	1
Meldpunten van banken: KNAB	KNAB	fraude met betaalmiddelen	1	0	0	0	1	0	1	1
Meldpunten van banken: Regiobank	Regiobank	fraude met betaalmiddelen	1	0	0	0	1	1	1	1
Meldpunten van woningcorporaties: Lefier	Lefier	overig	1	0	0	0	0	0	0	0
Meldpunten van woningcorporaties: Woonzorg Nederland	Woonzorg Nederland	overig	1	0	0	1	0	0	0	1
Meldpunten van zorgverzekeraars: ASR	ASR	verzekeringsfraude	1	0	1	1	0	0	0	1

Meldpunten van zorgverzekeraars: DSW	DSW	verzekeringsfraude	1	0	1	1	0	0	0	1
Meldpunten van zorgverzekeraars: Zilveren Kruis	Achmea - Zilveren Kruis	verzekeringsfraude	1	0	0	1	0	0	0	1
Meldpunten verzekeringsmaatschappijen: Allianz Direct	Allianz	verzekeringsfraude	1	0	1	1	0	0	0	1
Meldpunten verzekeringsmaatschappijen: Klaverblad	Klaverblad	verzekeringsfraude	1	0	1	1	0	0	0	1
Meldpunten verzekeringsmaatschappijen: Nationale Nederlanden	Nationale Nederlanden	verzekeringsfraude	1	1	0	1	0	0	0	1
Netbeheerder: Coteq	Coteq	overig	1	0	0	1	1	0	0	1
Netbeheerder: Liander	Liander	overig	1	0	0	1	0	0	0	1
Netbeheerder: Stedin	Stedin	overig	1	0	0	1	0	0	0	1
NZA	NZA	verzekeringsfraude	1	0	0	1	0	0	0	1
Publeaks	Stichting Publeaks	meerdere vormen	1	0	0	0	0	0	0	0
Slachtofferhulp Nederland	SHN	meerdere vormen	1	0	1	0	1	1	1	0
So-da.nl	So-da	meerdere vormen	1	0	0	0	0	1	1	1
Stiba	Stiba	overig	1	0	0	0	0	0	0	0
Stichting BREIN	Stichting BREIN	overig	1	0	0	1	0	0	0	1
Telecomprovider: Tele-2	Tele2	meerdere vormen	1	1	1	1	1	0	1	0
Telecomprovider: T-Mobile	T-mobile	meerdere vormen	1	0	0	0	1	0	1	0
Telecomprovider: Vodafone	Codafone	fraude met betaalmiddelen	1	0	1	0	1	0	1	0

Naam informatiepunt/doorverwijspunt	Beheerder	Type fraude	Meldingen regi-	Monitoren	Signaleren	Analyseren en	Voorlichting met	Begeleiding/on-	Doorverwijzen	Aanpakken van
			streten			onderzoeken	het oog op pre-ventie	dersteuning van slachtoffers	van slachtoffers naar andere org.	fraudezaken
CBM	Branchevereniging	overig	0	0	0	0	1	0	0	0
Diverse bedrijven: Ideal	Ideal	fraude met betaalmiddelen	0	0	0	0	0	0	1	0
Hackhelpdesk	PVO en CCV	meerdere vormen	0	0	0	0	1	1	1	0
Helpwanted	Offlimits	meerdere vormen	0	0	0	0	1	0	1	0
Hetccv.nl	CCV	meerdere vormen	0	0	0	0	1	0	1	0
Kamer van Koophandel	KvK	meerdere vormen	0	0	0	0	1	0	1	0
Maakhetzenietmakkelijk.nl	Ministerie J&V	fraude met betaalmiddelen	0	0	0	0	1	0	1	0
Nederlandse Vereniging van Banken	NVB	fraude met betaalmiddelen	0	0	0	0	1	0	1	0
Opgelicht	Avrotros	meerdere vormen	0	0	0	0	1	1	0	0
Seniorweb.nl	Vereniging seniorweb	meerdere vormen	0	0	0	0	1	0	1	0
Slachtofferwijzer.nl	Fonds slachtofferhulp	meerdere vormen	0	0	0	0	1	1	1	0
Veiligbankieren.nl	Nederlandse Vereniging van Banken	fraude met betaalmiddelen	0	0	0	0	1	0	1	0
Veiliginternetten.nl	Publiek initiatief (EZK, NCSC en ECP)	meerdere vormen	0	0	0	0	1	0	1	0
Voorkomstsmartphonefraude.nl	Samenwerking tussen Nederlandse telecomproviders	telecomfraude	0	0	0	0	1	1	1	0
Zowerktfraude.nl	Initiatief van NVB	fraude met betaalmiddelen	0	0	0	0	1	0	1	0

Bijlage 8: Subsidievoorwaarden

Voorwaarde	Methodiek	Beoordeling
<i>Ervaring en expertise</i>		
Het personeel van de helpdesk moet over voldoende en aantoonbare kennis beschikken op het terrein van fraude (specifiek oplichting, corruptie en witwassen) om eenvoudige algemene vragen te kunnen beantwoorden over veel voorkomende fraudezaken;	Interviews Fraudehelpdesk en vragenlijstonderzoek	Voldaan. Uit het vragenlijst onderzoek blijkt dat 40% van de respondenten het helemaal eens was met de stelling dat de medewerker deskundig was.
Het personeel van de helpdesk dient te beschikken over ervaring en expertise met een helpdesктаak en specifieke aantoonbare kennis en ervaring te hebben met de verwerking van meldingen, gegevensopslag, analyse en monitoring;	Interviews Fraudehelpdesk	Voldaan.
Het personeel van de helpdesk moet over voldoende en aantoonbare kennis beschikken om te kunnen bepalen naar welke instanties welke vragen dienen te worden doorgeleid.	Interviews Fraudehelpdesk	Voldaan.
<i>Netwerk</i>		
Het personeel van de helpdesk moet aantoonbaar beschikken over een netwerk bij in ieder geval politie, OM, AFM en Consumentenautoriteit om specifieke vragen aan deze instanties door te kunnen geleiden en er moet over en weer voldoende vertrouwen zijn om tot vruchtbare samenwerking te komen;	Interviews Fraudehelpdesk Interviews ketenpartners en experts	Voldaan.
Het voorstel dient een plan te bevatten om de netwerkpartners in kaart te brengen en een plan van aanpak hoe de doorverwijzingsfunctie naar de netwerkpartners zal worden vormgegeven en hoe de netwerkpartners zullen worden betrokken bij de inrichting en werking van de helpdesk;	Deskresearch	Hierover hebben de onderzoekers geen informatie ontvangen. Uit de evaluatie van 2012 blijkt dat wel aan deze voorwaarde is voldaan met de offerte van SafeCin.
Er dient te worden voorzien in een tweemaandelijks netwerkoverleg waarvan de subsidieverstrekker verslag zal ontvangen	Interviews JenV en EZK	Uit de evaluatie van 2012 blijkt dat het ministerie afzag van deze voorwaarde. Ook tijdens dit onderzoek is niet gebleken dat dit wel bestaat.
<i>Inrichting en werking helpdesk</i>		

De helpdesk vormt een front office voor consumenten (en kleine ondernemers);	Interviews Fraudehelpdesk En vragenlijstonderzoek	Voldaan.
De front office zal belast worden met: het verstrekken van algemene kennis en informatie over bestaande vormen van fraude en oplichting.	Interviews Fraudehelpdesk	Voldaan.
De front office zal doorverwijzen naar de relevante netwerkpartner als het gaat om meldingen en vragen van consumenten die op het werkterrein van de netwerkpartner liggen.	Interviews ketenpartners en experts Dossierstudie	Voldaan.
De front office dient te voldoen aan de gestelde eisen en er dient verantwoording afgelegd te worden over de behaalde resultaten aangaande de subsidievoorwaarden;	Deskresearch Interviews Fraudehelpdesk	N.v.t. omdat de subsidievoorwaarden niet meer van toepassing zijn.
Er dient continuïteit en capaciteit te zijn gegarandeerd op werkdagen tussen 09.00 en 17.00 uur gedurende de looptijd van de subsidie;	Websiteonderzoek	Niet volledig voldaan. Digitale meldingen kunnen 24/7 worden gedaan. De Telefonische helpdesk is op ma, di, do en vr van 9.00 - 12.00 en van 13.00 - 15.00 open en op wo van 13.00 - 15.00.
Er dient een website ingericht te zijn en onderhouden te worden met de meest gestelde vragen en algemene inhoudelijke en verwijzingsinformatie met een digitaal meldpunt voor schriftelijke vragen met een 24/7 bereikbaarheid;	Websiteonderzoek	Voldaan.
Een reactietijd op schriftelijke vragen van twee werkdagen dient in acht te worden genomen;	Digitale vragenlijst gebruikers	43% van de respondenten van het vragenlijst onderzoek geeft aan dat zij binnen 2 dagen reactie hebben gehad en 31% van de respondenten heeft binnen een week reactie gehad.
Het voorstel dient een uitgewerkt communicatieplan te bevatten om naamsbekendheid aan de helpdesk te geven;	Deskresearch	Voldaan. We hebben een recent communicatieplan voor 2023 ontvangen.
Er dient ten behoeve van eenvormigheid, effectiviteit en efficiëntie te worden gewerkt met vraag-en-antwoord-scripts die zijn opgesteld en actueel worden gehouden met de relevante partners;	Interviews Fraudehelpdesk en observatie	Voldaan.
Er dient gebruik te worden gemaakt van een standaard meldingsformulier voor de registratie van binnengekomen vragen en meldingen;	Websiteonderzoek	Voldaan.

Bij de registratie en de rapportage over de resultaten dient onderscheid te worden gemaakt tussen de soorten meldingen en afhandelingswijze waarbij in ieder geval de categorie cybercrime (gevallen waarbij computers of netwerken essentieel zijn) apart dient te worden weergegeven	Deskresearch	Voldaan.
<i>Financiën en rapportage</i>		
Er dient te worden voldaan aan de algemene voorwaarden zoals beschreven in de Wet Justitie-subsidies; ¹⁹⁰	Deskresearch	N.v.t.
Een financiële paragraaf dient onderdeel uit te maken van het verzoek;	Deskresearch	De onderzoekers hebben hier geen document over ontvangen. Uit de evaluatie van 2012 blijkt dat wel aan deze voorwaarde is voldaan.
Na tien maanden proefperiode vanaf het moment van ontvangst van de beschikking, dient er gerapporteerd te zijn over de effectiviteit en de werking van de helpdesk t.b.v. een beslissing over de continuering. In ieder geval dient er gerapporteerd te worden over de tevredenheid van de netwerkpartners en de aantallen meldingen en doorverwijzingen naar soort en afhandelingswijze.	Deskresearch	Voldaan.
<i>Algemeen</i>		
Na ontvangst van de beschikking dient de helpdesk binnen drie maanden operationeel te zijn;	Deskresearch	Voldaan.
De medewerkers van de helpdesk hebben een geheimhoudingsplicht;	Interviews Fraudehelpdesk	Voldaan.
Het type werkzaamheden ten behoeve van de helpdesk dient reeds de hoofdtak te vormen van de uitvoerende instantie.	Interview directeur SafeCin	Voldaan.

¹⁹⁰ Deze wet is op 1 juli 2022 vervangen door de Kaderwet overige JenV subsidies.

Bijlage 9: Definities

1-centfraude

Een vorm van phishing (zie phishing) waarbij iemand zegt dat die zogenaamd controleren of het opgegeven rekeningnummer echt is en stuurt een linkje voor een betaling van een (paar) cent. In alle gevallen leidt de link naar een nep-website, bijvoorbeeld van de bank, die sprekend lijkt op een echte website. Wie hier 'inlogt', stuurt de gegevens naar de cybercriminelen achter de nep-website (www.fraudehelpdesk.nl/fraudevormen-en-termen).

Aan- en verkoopfraude

Bij aankoopfraude maakt iemand geld over naar een persoon of bedrijf zonder de dienst of het product te ontvangen waarvoor is betaald. Bij verkoopfraude worden goederen wel geleverd, maar betaalt de ontvanger daar niet voor (www.politie.nl/informatie).

Acquisitiefraude

Bij acquisitiefraude is sprake van misleidende handelspraktijken tussen organisaties. Ondernemers worden met aanbiedingen overgehaald om een contract te tekenen waaruit dan een aanzienlijke betalingsverplichting ontstaat, terwijl er geen of slechts een geringe prestatie tegenover staat (Nationaal Dreigingsbeeld 2017, p.132).

Beleggingsfraude

Er is sprake van beleggingsfraude wanneer burgers en bedrijven verleid worden te beleggen in producten die niet bestaan, waardeloos zijn of rendementen beloven die opgebracht moeten worden door nieuwe deelnemers, zogenoemde piramidespelen (Nationaal Dreigingsbeeld 2017, p. 138).

Boilerroomfraude

Boilerroomfraude ontleent zijn naam aan de boilerroom, meestal een (relatief) klein kantoor in het buitenland, van waaruit mensen telefonisch benaderd worden om geld te investeren. Doordat de potentiële klanten de telefoongesprekken van de andere medewerkers op de achtergrond kunnen horen, wordt de indruk gewekt dat er een succesvol en betrouwbaar bedrijf actief is. Om potentiële klanten over te halen geld in te leggen, worden hun hoge rendementen in het vooruitzicht gesteld. In werkelijkheid blijkt het vaak om waardeloze aandelen te gaan (Nationaal Dreigingsbeeld 2017, p. 138).

Cybercrime

Cybercrime staat voor alle vormen van criminaliteit waarbij ICT zowel het doel als het middel is. Het gebruik van computers/internet is dus een voorwaarde om de criminaliteit uit te voeren (www.fraudehelpdesk.nl/fraudevormen-en-termen).

Datingfraude

Bij datingfraude heeft iemand online romantisch contact met een man of vrouw, vrijwel altijd in het buitenland, die zich presenteert als iemand anders. Vroeg of laat komt van de

datingpartner de vraag om ‘even’ geld voor te schieten. Bijvoorbeeld voor een noodgeval, ziekte of voor de invoerrechten van dure goederen die naar het slachtoffer toegestuurd zouden worden. De schade loopt vaak in de vele duizenden euro’s per slachtoffer (www.fraudehulpdesk.nl/fraudevormen-en-termen).

Faillissementsfraude

Van faillissementsfraude is sprake als een faillissement opzettelijk wordt misbruikt om financieel gewin te behalen (Nationaal Dreigingsbeeld 2017, p. 142).

Fraude met betaalmiddelen

Er is sprake van fraude met betaalmiddelen als er financiële transacties worden gedaan met het betaalmiddel van een ander zonder dat die ander daarvan op de hoogte is (Nationaal Dreigingsbeeld 2017, p. 145).

Fraude met online handel

Fraude met online handel is het niet nakomen van leverings- of betalingsverplichtingen die voortkomen uit transacties die online tot stand zijn gekomen (Nationaal Dreigingsbeeld 2017, p. 149).

Hacking

Het zich ongeoorloofd toegang verschaffen tot een digitale omgeving. Hacking wordt vaak ingezet om toegang te krijgen tot online-accounts als e-mail en social media om uit naam van een ander berichten te kunnen versturen (www.fraudehulpdesk.nl/fraudevormen-en-termen). Uit het onderzoek naar de vindbaarheid van de website van de Fraudehulpdesk blijkt dat er ook wordt gezocht op de term ‘telenet hacking melden’. Telenet is een Vlaams telecombedrijf.

Helpdeskfraude

De oplichters doen zich voor als helpdesk en bieden allerlei oplossingen aan. Allereerst moet bepaalde software gedownload worden, een zogenaamde remote acces tool (RAT), software om op afstand toegang te krijgen tot de computer van een ander. Met die software zouden ze op afstand het ‘probleem’ op de computer kunnen oplossen. Deze software kan criminelen uiteindelijk ook toegang geven tot een online bankomgeving. Zo sluizen ze geld weg naar hun eigen rekening, zonder dat iemand dit in de gaten heeft. Ook is het mogelijk dat potentiële slachtoffers naar frauduleuze websites worden geleid (www.fraudehulpdesk.nl/fraudevormen-en-termen).

Hulpvraagfraude

Hulpvraagfraude doet zich voor wanneer iemand per app wordt benaderd met een hulpvraag door een ‘bekende’ (meestal een zoon/dochter of ander familielid), zogenaamd met een nieuw telefoonnummer. De ‘bekende’ of het familielid vraagt de ontvanger, na een kort gesprekje, om geld over te maken. Dat moet altijd snel en het gaat om forse bedragen (www.fraudehulpdesk.nl/fraudevormen-en-termen).

Hypotheekfraude

Hypotheekfraude bestaat uit het op oneigenlijke en/of valse gronden verkrijgen van een hypothecaire lening om onroerend goed aan te schaffen (Nationaal Dreigingsbeeld 2017, p. 136).

Identiteitsfraude

Van identiteitsfraude is sprake wanneer iemand zich bedient van andermans identiteit of een gecreëerde, fictieve identiteit om daarmee geld en/of goederen te verwerven (www.fraudehulpdesk.nl/fraudevormen-en-termen).

Malware

Malware is elke software die gebruikt wordt om computersystemen te verstoren, gevoelige informatie te verzamelen of toegang te krijgen tot private computersystemen (www.fraudehulpdesk.nl/fraudevormen-en-termen).

Phishing

Phishing is een vorm van cybercrime waarbij criminelen proberen persoonlijke gegevens zoals inloggegevens, creditcardinformatie, pincodes of andere gegevens te achterhalen. Phishing kan plaatsvinden via diverse kanalen: per e-mail, WhatsApp, sms maar ook telefonisch en persoonlijk (www.fraudehulpdesk.nl/fraudevormen-en-termen).

Piramidefraude

Een vorm van beleggingsfraude waarbij investeerders wordt voorgehouden dat hun geld lucratief wordt belegd. In werkelijkheid wordt niets of slechts een (klein) deel van de ingelegde gelden belegd. De deelnemers geacht worden zelf nieuwe deelnemers aan te brengen. De 'voet' van de piramide betaalt het rendement van de top (Nationaal Dreigingsbeeld 2017, p. 139).

Ponzifraude

Het is een vorm van klassieke beleggingsfraude waarbij investeerders wordt voorgehouden dat hun geld lucratief wordt belegd. In werkelijkheid wordt niets of slechts een (klein) deel van de ingelegde gelden belegd. De vooraf afgesproken (hoge) rendementen worden betaald met de inleggeden van latere investeerders. Ponzifraude en piramidefraude lijken op elkaar. Bij piramidefraude worden deelnemers geacht zelf nieuwe deelnemers aan te brengen top (Nationaal Dreigingsbeeld 2017, p. 139).

Ransomware

Ransomware, ook wel gijzelsoftware of gijzelvirus genoemd, is een vorm van Malware (zie aldaar). Bij ransomware maakt de kwaadaardige software apparaten en/of bestanden op een computer door versleuteling onbruikbaar voor de gebruiker. De fraudeur biedt vervolgens tegen betaling een code aan waarmee de bestanden weer ontsleuteld kunnen worden (www.fraudehulpdesk.nl/fraudevormen-en-termen).

Skimmen

Skimmen is het illegaal kopiëren van betaal(kaart)gegevens, bijvoorbeeld het kopiëren van de gegevens uit de magneetstrip van een bankpasje tijdens het pinnen. De pincode wordt daarbij afgekeken en met deze combinatie kan geld worden opgenomen van de betaalpas (www.fraudehulpdesk.nl/fraudevormen-en-termen).

Smishing

Phishing (zie phishing) via de sms.

Online oplichting (Social engineering)

Het gebruik van sociale vermommingsen, culturele en psychologische trucs om computergebruikers hackers te laten helpen bij het illegaal binnendringen of gebruiken van computersystemen en netwerken (Bullée en Junger 2020).

Spoofing

Spoofing is de techniek waarbij de afzender van een e-mail, sms of telefoontje zichzelf verhuult door het tonen van een andere afzender. Door spoofing te gebruiken probeert de afzender van een vals bericht betrouwbaar over te komen (www.fraudehelpdesk.nl/fraudevormen-en-termen).

Telecomfraude

Telecomfraude betreft elke vorm van misbruik van een telecommunicatievoorziening, waardoor de integriteit van de telecommunicatie-infrastructuur wordt of kan worden aangetast (Nationaal Dreigingsbeeld 2017, p. 154).

Vacaturefraude

Ieder vals, bedrieglijk of misleidend wervingsaanbod van werkgelegenheid (www.fraudehelpdesk.nl/fraudevormen-en-termen).

Verzekeringsfraude

Verzekeringsfraude is het met opzet misleiden van de verzekeraar bij het aanvragen van een verzekering of bij het beroep doen op een verzekering (Nationaal Dreigingsbeeld 2017, p. 156).

Voorschotfraude

Voorschotfraude omvat allerlei vormen van oplichting waarbij het slachtoffer onder valse voorwendselen wordt verzocht een voorschot te betalen, met de belofte een grotere beloning in het vooruitzicht (Nationaal Dreigingsbeeld 2017, p. 160).

Bijlage 10: Responsverantwoording

naamsbekendheidsonderzoeken

Steekproefsamenstelling naamsbekendheidsonderzoek onder burgers in 2014									
Respondenten	2014								
	N=1000								
Leeftijd		Man	Vrouw						
18 – 30 jaar	12%	29%	71%						
31 – 45 jaar	27%	52%	48%						
46 – 64 jaar	40%	43%	57%						
65+ jaar	21%	69%	31%						
Regio	18-30	31-45	46-64	65+		18-30	31-45	46-64	65+
Zuid-Holland	18%	21%	19%	22%	Utrecht	8%	5%	8%	5%
Noord-Holland	14%	14%	14%	17%	Drenthe	4%	6%	6%	2%
Noord-Brabant	17%	14%	16%	7%	Friesland	3%	3%	5%	5%
Gelderland	11%	10%	9%	12%	Zeeland	4%	3%	4%	5%
Limburg	9%	9%	10%	7%	Groningen	3%	4%	2%	6%
Overijssel	8%	7%	6%	8%	Flevoland	2%	3%	2%	4%
Opleidingsniveau	18-30	31-45	46-64	65+		18-30	31-45	46-64	65+
Basisschool	6%	8%	4%	13%	HAVO	4%	4%	7%	5%
MAVO	9%	11%	11%	18%	VWO	2%	1%	3%	3%
LBO	3%	41%	28%	30%	HBO	28%	10%	16%	12%
MBO	35%	21%	27%	16%	WO	13%	4%	5%	3%

In onderstaande tabellen is de steekproefrespons opgenomen zoals deze in de rapporten van de bureaus is verantwoord.¹⁹¹

Steekproefopstelling naamsbekendheidsonderzoek onder ondernemers in 2020 (N=440)

Geslacht		Opleiding	
Man	63%	Vrouw	37%
Leeftijd		Opleiding	
Jonger dan 34 jaar	12%	Laag	16%
35 tot 50 jaar	36%	Midden	21%
50 jaar of ouder	52%	Hoog	63%
Regio		Opleiding	
West-Nederland	47%	Oost-Nederland	18%
Zuid-Nederland	23%	Noord-Nederland	11%
Aantal medewerkers		Opleiding	
Eenmanszaak/zzp'er	29%	50 tot 100	5%
2 tot 20	60%	100 of meer	0%
20 tot 50	6%		
Sector		Opleiding	
Industrie- en nutsbedrijven	3%	Communicatie	3%
Bouwnijverheid	5%	Financiële dienstverlening	5%
Handel	18%	Zakelijke dienstverlening + overige dienstverlening	30%
Horeca	6%	onderwijs	3%
Transport en logistiek	3%	Gezondheids- en welzijnszorg	10%
Anders	14%		

¹⁹¹ Door afronding kan het voorkomen dat een percentage tot net boven of onder de honderd procent optelt.

Steekproefsamenstelling naamsbekendheidsonderzoek onder burgers in 2016, 2018, 2020 en 2022									
Respondenten	2016	2018	2020	2022					
	N=1000	N=1000	N=1111	N=1015					
Geslacht	2016	2018	2020	2022		2016	2018	2020	2022
Man	50%	49%	49%	49%	Vrouw	50%	51%	51%	51%
Leeftijd ¹⁹²	2016	2018	2020	2022	Opleiding ¹⁹³	2016	2018	2020	2022
Jonger dan 34 jaar		26%	27%	27%	Laag		24%	26%	18%
35 tot 50 jaar		27%	23%	23%	Midden		40%	44%	36%
50 jaar of ouder		47%	50%	50%	Hoog		36%	30%	47%
Regio	2016	2018	2020	2022		2016	2018	2020	2022
West-Nederland	41%	45%	47%	46%	Oost-Nederland	22%	21%	21%	20%
Zuid-Nederland	25%	24%	22%	24%	Noord-Nederland	12%	10%	10%	10%
Huishoudsituatie	2016	2018	2020	2022	Huishoudinkomen	2016	2018	2020	2022
Inwonend bij ouders/familie/voogd	Niet bekend	9%	14%	Niet bekend	Minimum	Niet bekend	Niet bekend	16%	9%
Alleenstaand zonder (thuiswonende) kinderen	Niet bekend	26%	24%	Niet bekend	Beneden modaal	Niet bekend	Niet bekend	19%	12%
Alleenstaand met thuiswonende kinderen	Niet bekend	4%	6%	Niet bekend	Modaal	Niet bekend	Niet bekend	14%	16%
Samenwonend en/of gehuwd zonder thuiswonende kinderen	Niet bekend	35%	33%	Niet bekend	Anderhalf keer modaal	Niet bekend	Niet bekend	15%	18%
Samenwonend en/of gehuwd met (thuiswonende) kinderen	Niet bekend	26%	22%	Niet bekend	Twee keer modaal	Niet bekend	Niet bekend	10%	16%
Anders	Niet bekend	1%	1%	Niet bekend	Meer dan twee keer modaal	Niet bekend	Niet bekend	2%	4%
					Wil ik niet zeggen	Niet bekend	Niet bekend	24%	26%

¹⁹² In 2016 werden iets andere leeftijdscategorieën gehanteerd dan in de jaren 2018, 2020 en 2022, namelijk 18-35 (26%), 36-49 (25%), 50-64 (30%) en 65+ (19%).

¹⁹³ In 2016 werden andere categorieën voor het opleidingsniveau aangehouden: basisschool (2%), MAVO (11%), HAVO (7%), VWO (4%), LBO (8%), MBO (31%), HBO (26%) en WO (11%).



pro facto