


Monitor Identiteit 2021

Bezit, gebruik en misbruik van identiteitsmiddelen



Guido Brummelkamp
Ruud Hoevenagel
Auke Witkamp
Marierose Heineken-van Dooren
Maart 2022

Monitor Identiteit 2021

Bezit, gebruik en misbruik van identiteitsmiddelen



Inhoud

1. Inleiding	4	3. Identiteitsfraude	35
1.1 Een bijzonder jaar	5	3.1 Omvang van het probleem	36
1.2 Monitor identiteit: doel en ontwikkeling	6	3.2 Ervaren kwetsbaarheid voor identiteitsfraude	38
1.3 Onderzoeksmethode	8	3.3 Modus operandi van identiteitsfraude	39
1.4 Definities: identificatie, authenticatie en legitimatie	9	3.4 Identiteitsfraude: een indeling op basis van dader, middel en doel	42
2. Bezit en gebruik van identiteitsmiddelen	11	3.5 Acht typen van identiteitsfraude	47
2.1 Bezit van identiteitsmiddelen	12	3.6 Schade en hinder	50
2.2 Gebruik van identiteitsmiddelen	17	3.7 Ontvangen hulp	52
2.3 Kopiëren van identiteitsbewijzen	24	4. Kengetallen uit het stelsel	54
2.4 Risicovol gebruik	28	4.1 Rijksdienst voor Identiteitsgegevens (RvIG)	55
2.5 Verlies en diefstal	30	4.2 RDW	59
2.6 Fouten in registraties	32	4.3 Logius	61
2.7 Identificatie met behulp van biometrie	33	4.4 Fraudehelpdesk	65
		4.5 Centraal Bureau voor de Statistiek	67
		4.6 Koninklijke Marechaussee, ECID	70
		Bijlage 1: Onderzoeksverantwoording	72
		Bijlage 2: In welke situaties identificeren mensen zich op welke manier?	74
		Colofon	75



1. Inleiding

Sinds 2013 bestaat de monitor identiteit. Hiermee wordt tweejaarlijks bijgehouden hoe vaak, in welke situaties en op welke manier mensen zich identificeren met een wettig identiteitsmiddel. Tevens wordt in beeld gebracht hoe vaak dat misgaat en mensen slachtoffer worden van misbruik van hun identiteitsgegevens.

1.1 Een bijzonder jaar

Sinds 2013 bestaat de monitor identiteit, hiermee wordt bijgehouden welke identiteitsmiddelen Nederlandse burgers bezitten en hoe vaak zij zich daarmee identificeren. Het beeld daarover was vrij constant. Tot afgelopen jaar (2021). Wij identificeerden ons toen beduidend vaker dan daarvoor, wat geheel is toe te schrijven aan de maatregelen die werden genomen om de verspreiding van het coronavirus in te dammen. We maakten weliswaar minder vliegreizen, maar er kwamen drie nieuwe situaties bij waarvoor we onze identiteitsmiddelen juist vaker nodig hadden. Het betreffen de vaccinatie- en testcampagne en het gebruik van het coronatoegangsbewijs. Daarnaast bestelden we meer online waardoor we iets vaker een pakje moesten afhalen bij een afhaalpunt. Ten slotte waren er, los van corona, ook nog Tweede Kamerverkiezingen, waarvoor we ons moesten identificeren. Het afgelopen jaar identificeerden wij ons daardoor gemiddeld 10,6 keer met een wettig fysiek identiteitsmiddel. Dat is 30% meer dan in 2019, toen dat aantal ook al bovengemiddeld hoog was vanwege twee verkiezingen: die voor de Provinciale Staten en waterschappen (in maart 2019) en die voor het Europees parlement (in mei 2019).

Ook identificeerden we ons afgelopen jaar vaker online met DigiD. Op basis van cijfers die Logius hierover bijhoudt, schatten wij dat het gebruik van DigiD vorig jaar met ruim een kwart toenam. Ook dat is voor een belangrijk deel het gevolg van de coronamaatregelen. Alleen al ten behoeve van het laten testen op het coronavirus bij de GGD gebruikten wij 92 miljoen keer onze DigiD. Alleen al het testen zorgde daarmee voor een stijging van het gebruik van DigiD met 15% ten opzichte van 2020. Het zal eraan hebben bijgedragen dat DigiD nog weer verder is ingeburgerd. Op basis van de enquête onder de bevolking van 16 jaar en ouder, stellen wij vast dat het bezit de 100% nadert. Van de mensen die deelnamen aan de enquête bezit inmiddels 98% DigiD.

1.2 Monitor identiteit: doel en ontwikkeling

Voor burgers, bedrijven en overheden is het belangrijk om te kunnen vaststellen of degenen met wie zij contact aangaan werkelijk zijn wie zij zeggen te zijn. Burgers, bedrijven en overheden moeten kunnen terugvallen op een identiteitsstelsel met betrouwbare registraties en identiteitsmiddelen. De behoeften ten aanzien van dit stelsel zijn de afgelopen 25 jaar fundamenteel veranderd. Daar waar burgers, bedrijven en overheden voorheen voornamelijk face-to-face contact met elkaar hadden en voor identificatie gebruik maakten van paspoort, identiteitskaart en rijbewijs, verhouden zij zich nu vaak online tot elkaar en is men aangewezen op digitale identiteitsmiddelen. Het is belangrijk dat het identiteitsstelsel steeds aangesloten blijft bij deze ontwikkeling. De monitor identiteit helpt daarbij door inzicht te verschaffen in bezit, gebruik en misbruik van identiteitsmiddelen.

Met de monitor identiteit wordt tweejaarlijks in beeld gebracht hoe onder andere de digitalisering van het maatschappelijk verkeer doorwerkt in de behoefte en ervaringen van burgers met identiteitsverificatie. De monitor houdt bij hoe vaak, in welke situaties en op welke manieren mensen zich identificeren en hoe vaak en in welke omstandigheden het niet goed gaat en mensen bijvoorbeeld slachtoffer worden van identiteitsfraude. De monitor is opgezet om antwoord te geven op de volgende drie centrale vragen:

- Welke identiteitsmiddelen bezitten mensen?
- Hoe vaak, in welke situaties en op welke manier identificeren zij zich?
- Hoe vaak en op welke manier wordt misbruik gemaakt van identiteitsmiddelen?

Voorliggend rapport doet verslag van de zesde editie van de monitor identiteit. In de loop der jaren heeft de monitor zich ontwikkeld mede op basis van de kennisbehoefte van het Ministerie van Binnenlandse Zaken.

- In december 2013 verscheen de eerste editie. Op basis van bestaande bronnen werd het Nederlandse identiteitsstelsel cijfermatig in beeld gebracht. De monitor bevatte onder andere gegevens van RvIG, RDW, Marechaussee, Belastingdienst en Logius.
- In 2014 werd opnieuw aan de hand van bestaande gegevens het stelsel in beeld gebracht. Om meer inzicht te krijgen in het gebruik van identiteitsmiddelen werd de monitor aangevuld met een beknopte enquête onder burgers.
- In de editie van 2015 werd de enquête over het gebruik van identiteitsmiddelen uitgebreid. Belangrijke toevoegingen waren vragen over hoe mensen zich in specifieke situaties identificeren en waar zich eventuele risicovolle situaties voordoen. Ook is in deze editie begonnen met het in beeld brengen van identiteitsfraude, aan de hand van een aparte enquête.

- In 2017 is het onderwerp ‘identiteitsfraude’ verder verdiept. Deze editie gaf onder andere een omvattend beeld van wat identiteitsfraude concreet inhoudt, welke schade (materieel en immaterieel) slachtoffers lijden, tot wie zij zich wenden voor hulp en welke moeite het kost om de schade te herstellen.
- In 2019 is het begrip identiteitsfraude verder ontleed. Dit is gedaan aan de hand van drie vragen: Kent het slachtoffer de dader? Welk identiteitsmiddel is gebruikt (een fysiek identiteitsmiddel of een online account)? En: Welk doel had de dader (financieel gewin of pesten/zwartmaken)? Aan de hand van deze vragen zijn dat jaar zeven vormen van identiteitsfraude onderscheiden.

Met voorliggende editie is een volgende stap gezet in de ontwikkeling van de monitor. Naast een actualisatie van cijfermatige overzichten van voorgaande jaren, wordt dieper ingegaan op de voortschrijdende digitalisering van identificatie, de impact van de coronamaatregelen op de frequentie en manier waarop wij ons identificeren, en de ontwikkeling van de zeven vormen van identiteitsfraude die in de voorgaande editie van 2019 zijn onderscheiden. Tevens is een slag gemaakt in de kwaliteit van de controle op de betrouwbaarheid van het veldwerk. Bij de uitvoering van deze editie is samenwerking gezocht met marktonderzoeksbureau Ipsos.

1.3 Onderzoeksmethode

De kern van de monitor identiteit is een bevolkingsonderzoek dat bestaat uit twee enquêtes. Aanvullend worden gegevens verzameld over bezit, gebruik en misbruik van identiteitsmiddelen bij partijen binnen en buiten het identiteitsstelsel, zoals RvIG, Logius en CBS.

De eerste van de twee enquêtes is een vragenlijst die wordt voorgelegd aan een representatieve groep Nederlanders in de leeftijd van 16 jaar en ouder. Met deze vragenlijst wordt nagegaan welke identiteitsmiddelen men bezit, hoe vaak men die bij zich heeft en in welke situaties en met welke frequentie die gebruikt worden. De tweede enquête is een vragenlijst die alleen wordt voorgelegd aan mensen die te maken hebben gehad met identiteitsfraude. Deze mensen wordt gevraagd naar de aard van de fraude, schade, hinder en ook naar de instanties waartoe men zich wendde en de hulp die vervolgens eventueel geboden werd. De enquêtes worden na elkaar uitgevoerd. Dit jaar deden 2.473 mensen mee aan de eerste enquête, en 459 mensen mee aan de tweede enquête.

Representativiteit

Beide enquêtes worden afgenomen onder een groep mensen die deelnemen aan het panel van markonderzoeksbureau Ipsos. Deze mensen ontvingen voor hun deelname een vergoeding. Ipsos onderhoudt het panel actief wat inhoudt dat de samenstelling wordt

gecontroleerd op representativiteit. In bijlage 1 is de samenstelling van de groep mensen die in 2021 is geënquêteerd afgezet tegen de samenstelling van de Nederlandse bevolking. Ten aanzien van de representativiteit van onderzoek via online panels gelden desondanks beperkingen. In de eerste plaats zijn mensen die beperkt digivaardig zijn of om andere redenen niet of nauwelijks online zijn, er niet in vertegenwoordigd. In de tweede plaats is er een ondervertegenwoordiging van mensen die de (geschreven) Nederlandse taal niet of beperkt machtig zijn.

Betrouwbaarheid

Ook ten aanzien van betrouwbaarheid kent de online enquête onder een panel beperkingen. Het is althans beperkt mogelijk om na te gaan met welke zorgvuldigheid respondenten de vragen beantwoorden. Om deze reden zijn de data extra gecontroleerd op betrouwbaarheid. In de eerste plaats zijn respondenten met een buitengewoon lage responstijd buiten de analyse gehouden. Daarnaast is ten behoeve van de betrouwbaarheid van de enquête over slachtofferschap van identiteitsfraude aan het begin van de vragenlijst de respondenten gevraagd de fraude te beschrijven. In de analyse zijn alleen die respondenten betrokken die in hun antwoord daadwerkelijk refereerden aan identiteitsfraude.

1.4 Definities: identificatie, authenticatie en legitimatie

Burgers, bedrijven en overheden kunnen om verschillende redenen iemand vragen om een identiteitsbewijs te tonen. Vaak doet men dat om er zeker van te zijn dat iemand daadwerkelijk degene is die hij zegt te zijn. Men doet dat – met andere woorden - om iemand te identificeren. Identificatie vindt bijvoorbeeld veel plaats bij afhaalpunten in supermarkten waar klanten hun online bestelling afhalen. In sommige situaties is identiteitsverificatie wettelijk voorgeschreven zoals bijvoorbeeld in het geval dat iemand iets wil laten vastleggen in een notariële akte, of wanneer iemand aan boord gaat van een vliegtuig.

Vaak ook wordt mensen gevraagd om een identiteitsbewijs te tonen met als doel om na te gaan of iemand gemachtigd is om iets te doen. Er wordt dan gesproken van authenticatie. Authenticatie gebeurt vaak met een afgeleid identiteitsmiddel, zoals een toegangspas, username of token. Door een toegangspas te tonen, laat je niet zozeer zien wie je bent maar vooral dat je gemachtigd bent je ergens te begeven. Authenticatie gaat vaak gepaard met identificatie. Het meest bekende voorbeeld van dit moment is het gebruik van de Corona Check App. Met deze app kan je aantonen dat je gevaccineerd, hersteld, dan wel negatief getest bent en toegelaten kan worden tot bijvoorbeeld een restaurant. Daarbij is voorgeschreven dat de uitbater wel moet nagaan of degene die de app toont werkelijk degene is die hij zegt te zijn, aan de hand van een geldig wettig identiteitsbewijs.

Tenslotte wordt burgers regelmatig om een identiteitsbewijs gevraagd om te bepalen of zij bevoegd zijn om iets te doen. In deze situaties wordt gesproken van legitimatie. Legitimatie vindt veelvuldig plaats in supermarkten om te bepalen of iemand ouder is dan achttien jaar (en daarmee bevoegd is om alcohol dan wel tabak te kopen). Ook ten aanzien van legitimatie geldt dat het onderscheid met identificatie en authenticatie in de praktijk niet altijd duidelijk is. Denk bijvoorbeeld aan het huren van een auto waarbij het tonen van het rijbewijs zowel tot doel heeft om iemands identiteit te bewijzen als iemands rijvaardigheid.

Kijkend naar het onderscheid tussen identificatie, authenticatie en legitimatie, dan wordt duidelijk dat we onze wettige identiteitsmiddelen in veruit de meeste gevallen gebruiken voor identificatie. Ook het rijbewijs dat formeel in de eerste plaats een legitimatiebewijs is, wordt in de praktijk voornamelijk gebruikt als identiteitsbewijs. Dat we onze identiteitsmiddelen vooral gebruiken voor identificatie komt vooral voort uit wetgeving. De meeste situaties waarin het gebruik van een ID-middel wettelijk is voorgeschreven, hebben betrekking op identificatie. Een belangrijke bijdrage hieraan levert de Tijdelijke regeling maatregelen covid 19 (welke identificatie verplicht bij deelname aan de vaccinatie- en testcampagne), de Kieswet (welke het verplicht om je te identificeren bij verkiezingen) en de Vreemdelingenwet (welke het verplicht om je te identificeren bij het passeren van een Schengengrens en het aan

boord gaan van een vliegtuig). Waarin de uitkomsten van voorliggende editie van de monitor zich onderscheiden van de voorgaande edities is dat wettige identiteitsmiddelen vaker zijn ingezet ten behoeve van authenticatie. Dit komt door het gebruik van de Corona check app en het

papieren bewijs, dat formeel altijd moet worden gebruikt in combinatie met een identiteitsbewijs. In onderstaande tabel is het verschil tussen identificatie en authenticatie en legitimatie uitgelegd, waarbij enkele voorbeelden zijn gegeven van wetten waarin het wordt voorgeschreven.

TABEL 1: **Identificatie, authenticatie en legitimatie**

	Wat is het?	Voorbeelden van wetgeving waarin het tonen van een identiteitsmiddel wettelijk is voorgeschreven
Identificatie	Vaststellen van iemands identiteit: is iemand daadwerkelijk degene die hij zegt te zijn?	<ul style="list-style-type: none"> • Wet op de identificatieplicht, art.2 • Wet Basisregistratie Personen • Wet op de loonbelasting, art. 6a • Paspoortwet • Tijdelijke regeling maatregelen covid-19 • Kieswet, art. K11
Authenticatie	Vaststellen of iemand op basis van een identiteitsmiddel of afgeleid identiteitsmiddel (zoals een toegangspas, account of token) toegang kan worden verleend.	
Legitimatie	Vaststellen of degene die een ID-middel toont bevoegd is om iets te doen.	

Digitale authenticatie: DigiD

Deze monitor brengt vooral het bezit en gebruik van fysieke identiteitsmiddelen in beeld. Dit neemt niet weg dat ook wordt ingegaan op digitale middelen, met name DigiD. We doen dat in de eerste plaats op basis van registraties die de overheid daarvan zelf bijhoudt, zoals over het aantal jaarlijkse DigiD-authenticaties, het aantal aangesloten partijen, en het aandeel dat de verschillende sectoren hebben in het

gebruik ervan. Deze gegevens hebben we aangevuld met eigen gegevens uit onze enquête om een beeld te geven van het ervaren gebruiksgemak en redenen om geen DigiD te hebben.

2. Bezit en gebruik van identiteitsmiddelen

Vrijwel iedere Nederlander van 16 jaar of ouder heeft een paspoort of identiteitskaart. De meeste mensen (71%) hebben daarnaast ook nog een rijbewijs. Het afgelopen jaar gebruikten zij deze fysieke identiteitsmiddelen gemiddeld 10,6 keer. Dat is beduidend vaker dan voorgaande jaren, wat geheel is toe te schrijven aan de maatregelen die zijn genomen om de verspreiding van het coronavirus in te dammen. Er zijn het afgelopen jaar drie situaties bijgekomen waarin mensen verplicht zijn om zich te identificeren, namelijk bij het laten vaccineren tegen corona, bij het laten testen daarop en bij het gebruik van het coronatoegangsbewijs.

2.1 Bezit van identiteitsmiddelen

Vrijwel iedere Nederlander van 16 jaar of ouder heeft een paspoort of identiteitskaart. 63% heeft een paspoort, 44% een identiteitskaart. Daarnaast heeft 71% ook nog een rijbewijs. Hoewel dit in de eerste plaats een middel is om de rijvaardigheid mee aan te tonen - het is in beginsel een legitimatiebewijs - wordt het rijbewijs toch vooral gebruikt als identiteitsbewijs (zie ook tabel 78 bijlage 2). Twee derde van de Nederlanders heeft daarmee voor de meeste praktijksituaties¹ waarin op een identiteitsbewijs wordt gevraagd de beschikking over twee wettige identiteitsmiddelen.

TABEL 2: Welk identiteitsbewijs bezit men?
(meerdere antwoorden)

	2015 (n=4.854)	2017 (n=4.789)	2019 (n=4.994)	2021 (n=2.473)
Nederlands paspoort	60%	59%	62%	63%
Nederlands identiteitskaart	47%	51%	49%	44%
Nederlands rijbewijs	66%	71%	71%	71%
Nederlands verblijfsdocument	1%	1%	2%	1%
Buitenlands verblijfsdocument	1%	1%	2%	2%
Geen	0%	0%	0%	0%

Bron: enquête onder bevolking

¹ In de Vreemdelingenwet zijn situaties beschreven waarin expliciet is gesteld dat identiteitsverificatie moet plaats vinden aan de hand van een reisdocument. Bijvoorbeeld bij het passeren van een Schengengrens of bij het aan boord gaan van een vliegtuig. Een rijbewijs kan in deze situaties niet gebruikt worden als identiteitsmiddel.

TABEL 3: Hoeveel identiteitsbewijzen bezit men?

	2015 (n = 4.854)	2017 (n = 4.790)	2019 (n=4.994)	2021 (n=2.473)
1 identiteitsmiddel	33%	28%	27%	27%
2 identiteitsmiddelen	59%	63%	62%	64%
3 of meer identiteitsmiddelen	8%	9%	11%	9%
Geen	0%	0%	0%	0%
Totaal	100%	100%	100%	100%

Bron: enquête onder bevolking

Van alle deelnemers aan de enquête gaven er vier aan géén identiteitsmiddel te bezitten, wat neer komt op een promille. Op de

vraag waarom zij geen fysiek middel hebben, gaven drie aan daar geen behoefte aan te hebben.

TABEL 4: Welke combinatie van identiteitsmiddelen heeft men?

	2015 (n = 4.853)	2017 (n = 4.789)	2019 (n=4.994)	2021 (n=2.473)
Nederlands Paspoort en Nederlands Rijbewijs	33%	35%	35%	38%
Nederlandse ID-kaart en Nederlands Rijbewijs	23%	25%	23%	22%
Alleen Nederlands Paspoort	17%	12%	13%	14%
Alleen Nederlandse ID-kaart	14%	14%	12%	11%
Alleen Nederlands Rijbewijs	2%	1%	1%	1%
Nederlands Paspoort, Nederlands ID-kaart en Nederlands Rijbewijs	7%	8%	9%	8%
Nederlands Paspoort en Nederlandse ID-kaart	3%	2%	3%	2%

Bron: enquête onder bevolking

Het bezit van de verschillende identiteitsmiddelen is niet gelijk verdeeld over de bevolking. Het bezit van een paspoort ligt iets hoger onder mannen en hoger opgeleiden. Hetzelfde beeld geldt voor het bezit van

een rijbewijs. Onder jongeren, vrouwen en lager opgeleiden ligt het bezit van de identiteitskaart wat hoger. Ook dit beeld is over de jaren heen constant.

TABEL 5: **Bezit van fysieke identiteitsmiddelen: verschillen tussen mannen en vrouwen; ouderen en jongeren; lager en hoger opgeleiden**

	Geslacht	Leeftijd	Opleiding
Nederlands paspoort	Het bezit van een paspoort is hoger onder mannen	*	Het bezit van een paspoort ligt onder hoger opgeleiden hoger
Nederlandse identiteitskaart	Het bezit van een NIK is hoger onder vrouwen	Het bezit van een NIK ligt onder jongeren (30-) hoger	Het bezit van een NIK ligt onder lager opgeleiden hoger
Nederlands rijbewijs	Het bezit van een rijbewijs is hoger onder mannen	Het bezit van een rijbewijs ligt onder ouderen (30+) hoger	Het bezit van een rijbewijs ligt onder hoger opgeleiden hoger
Nederlands verblijfsdocument	*	Het bezit van een Nederlands verblijfsdocument ligt onder jongeren (20-) hoger	*
Buitenlands identiteitskaart	Het bezit van een buitenlandse identiteitskaart is hoger onder vrouwen	Het bezit van een buitenlandse identiteitskaart ligt in de groep 20-50 hoger	Het bezit van een buitenlandse identiteitskaart ligt onder hoger opgeleiden hoger

**) geen significante verschillen
Bron: enquête onder bevolking*

Het aantal DigiD-accounts is in de periode 2013 – 2020 ieder jaar toegenomen². Slechts 2% van de mensen die deelnamen aan de enquête gaf aan geen DigiD te bezitten. 71% heeft inmiddels de DigiD app

geïnstalleerd. Van hen heeft een derde (33%) de app wel eens gebruikt in combinatie met een paspoort, identiteitskaart of rijbewijs.

² Monitor Generieke Digitale Infrastructuur, 2018 & Monitor Digitale Overheid, 2021

TABEL 6: Aantal actieve DigiD-accounts (in miljoenen)

	2013	2014	2015	2016	2017	2018	2019	2020
Aantal actieve DigiD-accounts	11,0	11,8	12,7	13,5	13,5	13,8	15,0	18,3

Bron: Monitor Generieke Digitale Infrastructuur, 2018 & Monitor Digitale Overheid, 2021

Aan de mensen zonder DigiD is gevraagd waarom zij geen DigiD hebben. Ongeveer een kwart gaf aan dat het hen niet lukte om DigiD te krijgen. Ongeveer een zelfde deel gaf aan niet te weten wat DigiD is. Dit betreft dus een kleine groep namelijk een kwart van 2% van alle zestien-plussers.

TABEL 7: Waarom heeft u geen DigiD?

	2021 (n=34)
Ik weet niet wat een DigiD is	27%
Ik heb DigiD niet nodig	35%
Het lukt mij niet om DigiD te krijgen	24%
Ik wil geen DigiD	12%
Weet niet	15%

Bron: enquête onder bevolking

Van de mensen die wél DigiD hebben, vindt 11% het lastig om dat te gebruiken. Op de open vraag waarom men het lastig vindt, antwoorden veel mensen dat ze hun wachtwoord steeds/snel vergeten. Een ander veel genoemd euvel is dat het systeem niet altijd werkt en dat het soms lang duurt om in te loggen. Een derde hindernis die vaak genoemd wordt, is dat er veel handelingen moeten worden verricht voordat je met DigiD ergens bent ingelogd.

TABEL 8: Heeft u moeite om DigiD te gebruiken?

	2021 (n=2.426)		
	Eens	Oneens	w.n.z.
Ik vind het lastig om DigiD te gebruiken	11%	88%	2%
Ik heb hulp nodig om DigiD te gebruiken	5%	93%	2%

Bron: enquête onder bevolking

Ook dit jaar is het bezit van DigiD vergeleken met het bezit van andere private digitale middelen waar mensen zich online mee kunnen identificeren. Hierbij moet worden opgemerkt dat identificatie via DigiD van een andere orde is dan identificatie met de meeste private middelen. Bij DigiD is de identiteit van een natuurlijk persoon immers altijd gecontroleerd en is ieder account voorbehouden aan één uniek persoon. Bij de meeste private identiteitsmiddelen daarentegen, staat het de gebruiker vrij om zelf een naam of identiteit te kiezen (de meeste platforms staan het gebruik van aliassen toe). Meestal kan één en dezelfde persoon bovendien met verschillende identiteiten naar buiten treden. Het bezit van private accounts geeft vooral een beeld van hoe digitale identificatie zich door de tijd heen ontwikkelt. Kijkend naar de afgelopen zes jaar dan is het beeld redelijke constant met uitzondering van enkele platforms die de afgelopen twee jaar zijn gegroeid zoals Instagram en LinkedIn. Een nadere beschouwing leert dat het bezit van de meeste private middelen leeftijdgebonden is. Voor de meeste private identiteitsmiddelen die in tabel 9 zijn opgenomen, geldt dat 30-minners er minder vaak gebruik van maken dan 30-plussers. Alleen voor LinkedIn en Facebook geldt dit niet.

TABEL 9: Welke online identiteitsmiddelen/accounts bezit men?

	2015 (n = 4.853)	2019 (n=4.994)	2021 (n=2.473)
DigiD	87%	91%	98%
Facebook	64%	64%	67%
Google	48%	59%	61%
Instagram	-	34%	44%
Microsoft	44%	40%	44%
LinkedIn	23%	26%	36%
Apple	23%	29%	31%
Pinterest	-	21%	25%
Twitter	19%	17%	22%
Snapchat	-	15%	15%
eHerkenning	1%	3%	5%
Itsme	-	0,3%	0,1%
Irma	-	0,2%	0,3%
Anders	1%	1%	1%
Geen online identiteiten ^a	5%	2%	3%

Bron: enquête onder bevolking

2.2 Gebruik van identiteitsmiddelen

De coronamaatregelen hebben een duidelijke invloed gehad op het gebruik van identiteitsmiddelen. Het afgelopen jaar zijn er drie situaties bijgekomen waarin mensen verplicht zijn om zich te identificeren, namelijk bij het laten vaccineren tegen corona, bij het laten testen daarop en bij het gebruik van het coronatoegangsbewijs. Op basis van de enquête die medio oktober (2021) is gehouden, zou het aantal keren dat mensen zich het afgelopen jaar hebben geïdentificeerd op acht uitkomen. Over heel 2021 zal dat aantal hoger liggen omdat juist in november en december mensen zich weer vaker lieten testen en het toezicht op identificatie bij het gebruik van het coronatoegangsbewijs werd aangescherpt. Wanneer we de uitkomsten van de enquête van medio oktober op deze twee onderdelen (identificatie bij testen en het gebruik van het coronatoegangsbewijs) extrapoleren naar het einde van dit jaar komen we uit op 10,6. Het gebruik van identiteitsmiddelen is daarmee een stuk hoger dan in 2019, terwijl er toen aanzienlijk meer werd gevlogen en terwijl er dat jaar ook twee verkiezingen werden gehouden: in maart 2019 voor de Provinciale Staten en in mei 2019 voor het Europees parlement.

TABEL 10: Aantal keer dat men zich in een jaar identificeert

2015 (n = 4.853)	2017 (n = 4.789)	2019 (n=4.994)	2021 (n = 2.473)
5,7	7,7	8,2	10,6 (a)

a) schatting op basis van cijfers medio oktober 2021

Bron: enquête onder bevolking

Driekwart van de mensen die wij enquêeerden, heeft altijd een identiteitsbewijs op zak. Dit beeld is constant over de jaren. In tabel 11 is een overzicht gegeven. Voor zover daar tussen jaren verschillen zijn gemeten, zijn deze niet significant. Over het algemeen geldt dat men vaker een identiteitsbewijs bij zich heeft naarmate men ouder is. Mogelijk komt dat door het rijbewijs dat men vaker op zak heeft en waarvan het bezit hoger is, naarmate men ouder is.

TABEL 11: Wanneer heeft u een identiteitsbewijs bij u?

	2015 (n = 4.853)	2017 (n = 4.789)	2019 (n=4.994)	2021 (n=2.473)
Altijd	77%	76%	76%	75%
Vaak	15%	16%	16%	16%
Soms	6%	6%	6%	7%
Nooit	2%	2%	2%	2%
Totaal	100%	100%	100%	100%

Bron: enquête onder bevolking

De coronamaatregelen hebben ook de top-10 van meest voorkomende activiteiten waarbij een identificatieplicht geldt, sterk gewijzigd. De drie eerder genoemde coronamaatregelen (vaccinatie, testen en coronatoegangsbewijs) vormen samen met de Tweede Kamerverkiezingen de belangrijkste situaties waarin mensen een wettig identiteitsbewijs hebben laten zien.

TABEL 12: Top-10 van meest voorkomende activiteiten die mensen de afgelopen 12 maanden hebben ondernomen en waarbij men zich heeft moeten identificeren (*)

	2019 (n=4.994)	2021 (n=2.468)
Laten vaccineren tegen corona (a)	-	77%
Corona check app of papieren bewijs gebruikt (waarbij tenminste één keer een identiteitsmiddel moest worden getoond)	-	57% (b) / 77% (c)
Gestemd bij de laatste Tweede Kamer verkiezingen (15-17 maart 2021) (d)		68%
Laten testen op corona (e)	-	50%
Gestemd bij Provinciale Staten verkiezingen (20 maart 2019)	48%	-
Gestemd bij verkiezingen voor het Europees parlement (23 mei 2019)	45%	-
Pakje in ontvangst genomen bij een afhaalpunt/postkantoor	42%	47%
In een hotel, pension, camping of particuliere huurwoning overnacht	39%	35%
Geregistreerd bij een ziekenhuis/ zorginstelling/ dokter/ therapeut	30%	25%
Alcohol of sigaretten gekocht (waarbij tenminste één keer een identiteitsmiddel moest worden getoond)	4% (f)	22% (g)
Vliegreis gemaakt	39%	16%
Nieuw ID-bewijs aangevraagd bij de gemeente	12%	11%

(a) Op basis van Rijksoverheid.nl heeft medio november 2021 (week 45), 84,7% van de bevolking van 18 jaar en ouder zich laten vaccineren.

(b) Stand van zaken medio oktober 2021

(c) Schatting voor heel 2021 op basis van stand van zaken medio oktober

(d) Opkomst bij de Tweede Kamerverkiezingen wast 78,7%.

(e) Stand van zaken medio oktober 2021

(f) Percentage heeft betrekking op de gehele groep ondervraagden.

(g) Percentage heeft betrekking op de groep mensen in de leeftijd van 16 tot 25 jaar.

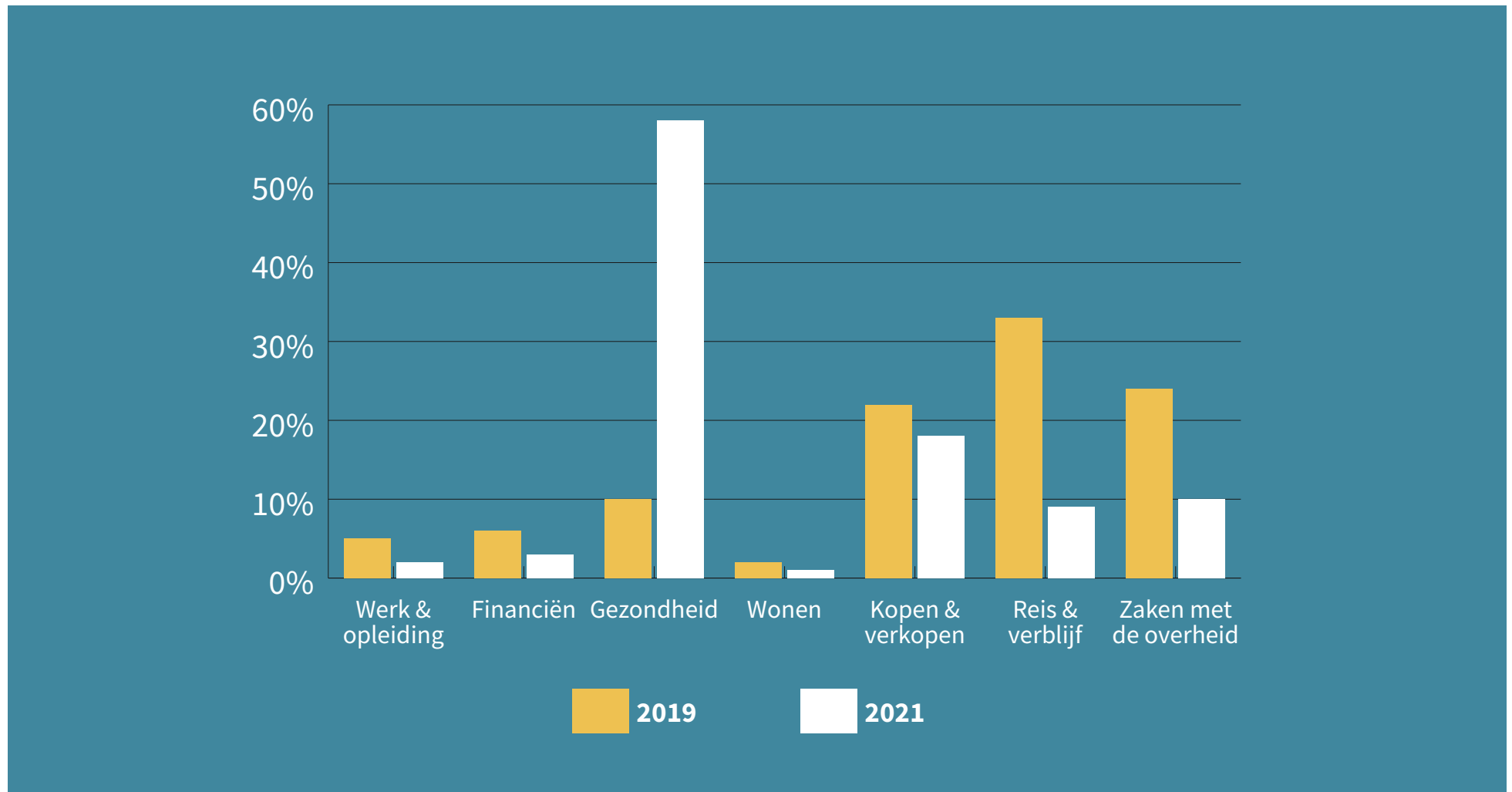
Bron: enquête onder bevolking

In het kader van dit onderzoek zijn 39 veel voorkomende situaties onderscheiden waarin mensen kan worden gevraagd om zich te identificeren met een wettig fysiek identiteitsmiddel. In sommige situaties is identificatie aan de hand van een wettig identiteitsmiddel bij wet voorgeschreven. In tabel 78 in bijlage 2 is per activiteit aangegeven hoe vaak in 2021 werd gevraagd naar een identiteitsmiddel; hoe vaak identificatie face to face plaatsvond dan wel op afstand; hoe vaak wordt gevraagd om een kopie; en welk middel men het vaakst gebruikt om zich te identificeren. In tabel 13 zijn de gegevens samengevat in zeven domeinen: 'reis en verblijf', 'gezondheid', 'kopen en verkopen', 'financiën', 'werk en opleiding', 'wonen' en 'zaken met de overheid'

TABEL 13: **Identificatie met een wettig fysiek identiteitsmiddel in zeven domeinen**

Kenmerken van identificatie	
Reis en verblijf (o.a. vliegreizen, verblijf in hotel, camping)	<ul style="list-style-type: none"> • 9% van alle identificaties (was 33% in 2019) • Vooral vanwege Vreemdelingenwet bij het maken van vliegreizen • Voornamelijk face to face • Paspoort wordt meest gebruikt • Soms moet kopie overhandigd worden (bij huur auto, camping, hotel)
Gezondheid (o.a. vaccinatie, testen, bezoek aan zorginstelling)	<ul style="list-style-type: none"> • 58% van alle identificaties (was 10% in 2019) • Vooral door coronamaatregelen / Tijdelijke regeling maatregelen covid-19 • Sterke toename gebruik van DigiD • Van fysieke middelen wordt rijbewijs het meest gebruikt • Vrijwel geen gebruik van kopieën
Kopen en verkopen (o.a. pakketje afhalen, telefoonabonnement)	<ul style="list-style-type: none"> • 18% van alle identificaties • Vooral voor ophalen online aankopen bij afhaalpunt • Veel identificatie vanwege Alcoholwet en Tabakswet (identificatieplicht bij aanschaf alcohol en tabak) • Rijbewijs en NIK worden het meest gebruikt • Weinig gebruik van kopieën (behalve bij aangaan telefoonabonnement)
Financiën (o.a. bankrekening openen, notarisbezoek)	<ul style="list-style-type: none"> • 3% van alle identificaties • Vooral voor zaken met banken, wettelijk voorgeschreven met Wet ter voorkoming van witwassen en financieren terrorisme • Toename van identificatie op afstand • Paspoort meest gebruikt • Veel gebruik van kopieën en scans
Werk en opleiding (o.a. nieuwe baan, inschrijven bij uitzendbureau)	<ul style="list-style-type: none"> • 2% van alle identificaties • Vooral vanwege Wet arbeid vreemdelingen • Voornamelijk face to face • Paspoort en Identiteitskaart het meest gebruikt • Veel gebruik van kopieën en scans
Wonen (o.a. huren woning, zaken doen met makelaar)	<ul style="list-style-type: none"> • 1% van alle identificaties • Geen wettelijke grondslag • Voornamelijk face to face • Paspoort en identiteitskaart meest gebruikt • Veel gebruik van kopieën en scans
Zaken met de overheid (o.a. verkiezingen, subsidie aanvragen, aangifte)	<ul style="list-style-type: none"> • 10 % van alle identificaties • Vooral door Tweede Kamerverkiezingen van maart 2021. • Voornamelijk face to face, • Wisselend gebruik van paspoort, identiteitskaart en rijbewijs. • Op onderdelen sterke stijging DigiD (aanvragen subsidies, en aangifte bij politie) • Weinig gebruik van kopieën of scans

Figuur 1: Welk domein heeft welk aandeel in het totaal aantal keer dat Nederlandse burgers zich identificeren met een wettig identiteitsmiddel?



Paspoorten en identiteitskaarten hebben een chip waarop de gegevens van het document zijn opgeslagen. Op de documenten is dat aangegeven met een logo. 66% van de geënquêteerden is bekend met deze chip. Het is een lichte stijging ten opzichte van 2019

TABEL 14: **Paspoorten en identiteitskaarten hebben een chip waarop de gegevens van het document zijn opgeslagen. Wist u dat?**

	2019 (n=4.994)	2021 (n=2.473)
Ja	59%	66%
Nee	41%	34%
Totaal	100%	100%

Bron: enquête onder bevolking

Er zijn verschillende instanties en apps die de gegevens die digitaal zijn opgeslagen in het paspoort en de identiteitskaart kunnen uitlezen. Dit jaar gaf 12% aan gegevens wel eens te hebben uitgelezen of te hebben laten uitlezen. Veruit de meeste van hen deden dat met hun eigen telefoon. Meestal deden ze dat door gebruik te maken van de DigiD-app. Enkele andere situaties waarin de chip werd uitgelezen, waren het bezoek aan een ziekenhuis en reizen via Schiphol.

TABEL 15: **Heeft u de gegevens die op deze chip zijn opgeslagen zelf wel eens uitgelezen met een app of apparaat?**

	2019 (n=2.936)	2021 (n=1.633)
Ja	8%	12%
Nee	92%	88%
Totaal	100%	100%

Bron: enquête onder bevolking

2.3 Kopiëren van identiteitsbewijzen

Het afgelopen jaar heeft ruim een derde van de geënquêteerde een kopie gemaakt van zijn identiteitsbewijs om deze vervolgens op te sturen, te mailen of te overhandigen. Dit beeld komt overeen met dat van 2019. Ongeveer twintig procent liet (daarnaast) een kopie van zijn

identiteitsbewijs maken waar men zelf bij aanwezig was. Dat laatste komt bijvoorbeeld regelmatig voor bij het inchecken bij een camping of hotel, bij de aanvang van een nieuw dienstverband of wanneer men iets huurt. Dit jaar kwam dat aanzienlijk minder vaak voor dan in 2019.

TABEL 16: Heeft u in de afgelopen 12 maanden wel eens een kopie van uw identiteitsbewijs gemaakt of laten maken?

	Paspoort		Identiteitskaart		Rijbewijs		Nederlands verblijfsdoc.	
	2019 (n = 3.110)	2021 (n=1.567)	2019 (n = 2.431)	2021 (n=1.093)	2019 (n = 3.520)	2021 (n=1.763)	2019 (n = 83)	2021 (n=30)
Een kopie of scan opgestuurd, gemaaild of overhandigd	41%	36%	36%	35%	17%	18%	31%	40%
Een kopie of scan laten maken bij een identiteitscontrole (waar uzelf fysiek bij aanwezig was)	30%	18%	23%	18%	14%	11%	29%	23%

Bron: enquête onder bevolking

Een situatie waarin het gangbaar is om bij identificatie ook een kopie of scan te geven, is wanneer iemand een nieuwe werkgever krijgt. Vrijwel alle werkgevers vragen om een kopie. Tevens wordt meestal om een kopie of scan gevraagd bij bepaalde financiële diensten zoals het aangaan van een (hypothecaire) lening, het openen van een (beleggings) rekening of het openen van een account voor cryptovaluta.

TABEL 17: **Top-10 van situaties waarin mensen het vaakst een kopie van hun identiteitsmiddel moeten overhandigen of opsturen**

% dat aangeeft een kopie te hebben overhandigd of opgestuurd	2019 (n=4.994)	2021 (n=2.473)
Een nieuwe werkgever gekregen	87%	91%
Een hypotheek, lening, krediet of credit card afgesloten	85%	82%
Beleggingsrekening geopend	80%	82%
Cryptovaluta aangeschaft	-	81%
Ingeschreven bij een uitzendbureau	74%	81%
Een bankrekening geopend	77%	69%
Ingeschreven voor een opleiding	60%	65%
Verhuisd naar een andere huurwoning	76%	61%
Zaken geregeld bij de notaris	75%	60%

Bron: enquête onder bevolking

Vanuit de rijksoverheid wordt mensen geadviseerd voorzichtig om te gaan met kopietjes van hun identiteitsbewijs. Een advies is bijvoorbeeld om gegevens die niet relevant zijn voor identificatie onleesbaar te maken en om op de kopie aan te geven waar deze specifiek voor is bedoeld. Iets minder dan de helft van de geënquêteerden die het afgelopen jaar wel eens een kopie heeft gemaakt van zijn identiteitsbewijs, heeft daarop één of meerdere gegevens onleesbaar gemaakt. 36% heeft wel eens op een kopie aangegeven voor welk doel het gebruikt mag worden. Het beeld is vergelijkbaar met dat van twee jaar geleden.

TABEL 18: Heeft u de kopie bewerkt om misbruik te voorkomen?

	2019 (n=2.779)	2021 (n=1.169)	2019 (n=2.779)	2021 (n=1.169)	2019 (n=2.779)	2021 (n=1.169)
	Nooit gedaan		Wel eens gedaan		Weet niet meer	
Ik heb op de kopie of scan vermeld voor welk doel en op welke datum die precies gebruikt mag worden	56%	56%	38%	36%	6%	8%
Ik heb het Burgerservicenummer doorgestreept	55%	49%	42%	45%	3%	6%
Ik heb de pasfoto onherkenbaar gemaakt	78%	74%	18%	22%	4%	4%
Ik heb andere gegevens die de vragende partij niet nodig had doorgestreept	58%	57%	37%	38%	5%	5%

Bron: enquête onder bevolking

Wanneer we verder terugkijken, dan lijkt het bewustzijn ten aanzien van het bewerken van kopietjes zich te stabiliseren. Over de perioden 2015-

2019 was er een stijging van het aantal mensen dat kopietjes bewerkte. De afgelopen twee jaar heeft die stijging niet doorgezet.

TABEL 19: Heeft u de kopie bewerkt om misbruik te voorkomen? (% dat aangeeft dit nooit gedaan te hebben)

	2015 (n=2.717)	2017 (n= 2.681)	2019 (n=2.779)	2021
Ik heb op de kopie of scan vermeld voor welk doel die precies gebruikt mag worden	66 %	59 %	56 %	56%
Ik heb het Burgerservicenummer doorgestreept	73 %	61 %	55 %	49%
Ik heb de pasfoto onherkenbaar gemaakt	85 %	80 %	78 %	74%
Ik heb andere gegevens die de vragende partij niet nodig had doorgestreept	72 %	64 %	58 %	57%

Bron: enquête onder bevolking

Om het makkelijker te maken gegevens op een kopie van een identiteitsbewijs onleesbaar te maken, bestaat al enkele jaren de KopieID app. Deze is uitgegeven door het ministerie van BZK. Sinds 2017 is de bekendheid van de app steeds iets toegenomen. Dit jaar geeft 24% van de geënquêteerden aan de app te kennen.

TABEL 20: Kent u de KopieID app?

	2017 (n = 4.789)	2019 (n=4.994)	2021 (n=2.473)
Ja	14%	17%	24%
Nee	86%	83%	76%
Totaal	100%	100%	100%

Bron: enquête onder bevolking

In lijn met de kennis over de KopieID app is ook het gebruik dit jaar opnieuw (iets) toegenomen. Dit jaar geeft 14% van de geënquêteerden aan de app wel eens gebruikt te hebben.

TABEL 21: Heeft u de KopieID app wel eens gebruikt?

	2017 (n = 4.789)	2019 (n=4.994)	2021 (n=2.473)
Ja	7%	10%	14%
Nee	93%	90%	86%
Totaal	100%	100%	100%

Bron: enquête onder bevolking

2.4 Risicovol gebruik

Het afgelopen jaar heeft 5% van de geënquêteerden zijn identiteitsbewijs wel eens ergens achtergelaten. Dit percentage is een stuk lager dan in 2019, toen 9% aangaf dat wel eens gedaan te hebben. Een duidelijke verklaring voor het lagere percentage is er niet, het is wel aannemelijk dat de reisbeperkingen vanwege de coronamaatregelen een rol hebben gespeeld. Ten opzichte van 2019 lieten minder mensen hun bewijs achter bij een camping of hotel, wat niet weg neemt dat dat nog steeds de situatie is waarin mensen het vaakst hun identiteitsbewijs (moeten) achterlaten.

TABEL 22: Heeft u uw identiteitsbewijs wel eens ergens achtergelaten?

	2015 (n = 4.853)	2017 (n = 4.789)	2019 (n = 4.994)	2021 (n=2.445)
Ja	5%	10%	9%	5%
Nee	95%	90%	91%	95%
Totaal	100%	100%	100%	100%

Bron: enquête onder bevolking

TABEL 23: Waar heeft u uw identiteitsbewijs achtergelaten?

	2021 (n=118)
Hotel/camping	60%
Benzinestation	19%
Winkel	15%
Verhuurbedrijf	6%
Ergens anders	14%
Totaal	114%

Bron: enquête onder bevolking

In 2021 heeft 9% van de geënquêteerden zijn identiteitsbewijs wel eens uitgeleend aan iemand anders. Vaak was dat aan een gezins- of familielid, in de meeste gevallen was dat om een stem te kunnen uitbrengen bij de Tweede Kamerverkiezingen.

TABEL 24: **Heeft u uw identiteitsbewijs wel eens uitgeleend aan iemand?**

	2021 (n=2.468)
Ja	9%
Nee	91%
Totaal	100%

Bron: enquête onder bevolking

TABEL 25: **Aan wie heeft u uw identiteitsbewijs uitgeleend?**
(meerdere antwoorden mogelijk)

	2021 (n=203)
Gezins- of familielid	77%
Vriend/kennis	13%
Buur of buurtgenoot	7%
Collega	5%
Klas- /studiegenoot	1%
Iemand anders	5%
Totaal	108%

Bron: enquête onder bevolking

TABEL 26: **Waarom leende u uw identiteitsbewijs uit?**
(meerdere antwoorden mogelijk)

	2021 (n=222)
Om namens mij te stemmen	49%
Om diensten af te nemen namens mij	23%
Om sigaretten of alcohol te kopen	9%
Om toegang te krijgen tot een gebouw of terrein	14%
Anders, namelijk	11%

Bron: enquête onder bevolking

2.5 Verlies en diefstal

In 2020 werden er ruim 33 duizend paspoorten en ruim 96 duizend identiteitskaarten als vermist opgegeven³. Deze aantallen zijn beduidend lager dan de jaren daarvoor. Dit laat mogelijk zien dat mensen een vermissing van een reisdocument pas opgegeven als ze die nodig hebben. Wellicht bleef opgave van vermissing afgelopen tijd bij meer mensen uit omdat zij minder reisden (althans een reis ondernemen waarvoor een reisdocument vereist is). Uit de enquête komt het beeld naar voren dat het aantal mensen dat zijn paspoort of rijbewijs kwijtraakte (al dan niet door diefstal) min of meer gelijk is gebleven. Het aantal mensen dat zijn identiteitskaart kwijtraakte nam – afgaande op de enquête - wel iets af.

³ Op basis van RvIG, zie ook tabel 53

TABEL 27: Bent u in de afgelopen 12 maanden wel eens een identiteitsdocument kwijtgeraakt of is zo'n document van u gestolen?

		2017 (n=4.789)	2019 (n=4.994)	2021 (n=2.445)
Paspoort	Kwijtgeraakt	1,9%	1,7%	1,5%
	Gestolen	1,4%	0,7%	0,4%
Identiteitskaart	Kwijtgeraakt	3,8%	3,2%	1,9%
	Gestolen	2,2%	1,1%	0,3%
Rijbewijs	Kwijtgeraakt	1,4%	1,4%	1,3%
	Gestolen	0,9%	0,7%	0,5%

Bron: enquête onder bevolking

De meeste mensen geven de vermissing van hun identiteitsmiddel binnen een week aan. De meesten gaan daarvoor naar de gemeente, wat formeel gezien ook het geëigende loket is. 15% deed aangifte bij de politie.

TABEL 28: Wanneer heeft u de diefstal of het verlies doorgegeven?

	2021 (n=86)
Binnen 24 uur	28%
Binnen 48 uur	17%
Binnen een week	24%
Binnen een maand	10%
Pas toen ik een nieuw id-bewijs nodig had (na meer dan een maand)	14%
Nog niet	6%
Totaal	100%

Bron: enquête onder bevolking

TABEL 29: Waar heeft u de diefstal of het verlies doorgegeven?

	2021 (n=86)
Ik heb de vermissing niet doorgegeven	27%
Gemeente	50%
Politie	15%
Ergens anders	8%
Totaal	100%

Bron: enquête onder bevolking

2.6 Fouten in registraties

Bij 6% van de geënquêteerden is het wel eens voorgekomen dat gegevens niet goed waren geregistreerd bij de gemeente. Ten opzichte van 2017 en 2019 is dit beeld constant. Op de vraag wat er dan niet goed geregistreerd stond, geven veel mensen aan dat het om hun adresgegevens ging. Situaties waarbij fouten ontstaan, zijn verhuizingen en wijzigingen in gezinssamenstelling waaronder echtscheidingen. Verder hebben fouten betrekking op de spelling van namen. Voor zover de fouten in de registratie ten tijde van de enquête al waren hersteld, gaven mensen aan dat het hen zo'n drie weken had gekost.

TABEL 30: Is het bij u wel eens voorgekomen dat uw gegevens niet goed geregistreerd stonden bij de gemeente?

	2017 (n=4.790)	2019 (n=4.994)	2021 (n=2.298)
Ja	8%	6%	6%
Nee	92%	94%	94%
Totaal	100%	100%	100%

Bron: enquête onder bevolking

TABEL 31: Was het mogelijk om de fout(en) te corrigeren, en hoeveel tijd kostte dat?

	2019 (n=316)	2021 (n=145)
Ja	77%	77%
Nee	17%	13%
Ik ben er nog mee bezig	6%	10%
Totaal	100%	100%
	(n=242)	(n=111)
Aantal weken (5% trimmed)	4	3

Bron: enquête onder bevolking

2.7 Identificatie met behulp van biometrie

Het gebruik van biometrie bij identificatie is opnieuw iets toegenomen. De situatie in 2021 is op dit punt sterk veranderd ten opzichte van het jaar waarop we dit voor eerst hebben gemeten (2015). Daar waar gezichtsherkenning in 2015 nog amper voorkwam (destijds

gaf 2% aan zich wel eens met automatische gezichtsherkenning te hebben geïdentificeerd), maakt nu bijna 20% er (wel eens) gebruik van. Biometrische identificatie wordt voornamelijk gebruikt voor het ontgrendelen van telefoons.

TABEL 32: Heeft u zich in de afgelopen 12 maanden wel eens geïdentificeerd m.b.v. biometrische kenmerken?

	2015 (n=4.853)	2017 (n=4.789)	2019 (n=4.994)	2021 (n=2.473)
Vingerdruk-herkenning	11%	20%	33%	35%
Iris-/oogherkenning	2%	3%	5%	4%
Stemherkenning	1%	2%	2%	2%
Automatische gezichtsherkenning	2%	3%	10%	19%
Andere vormen van biometrische herkenning	0%	0%	0%	1%
Geen van bovenstaande	81%	72%	56%	51%

Bron: Enquête onder bevolking

TABEL 33: Waarvoor identificeerde u zich met behulp van biometrie?

	2021 (n=1.492)
Ontgrendelen computer	14%
Ontgrendelen telefoon of tablet	89%
Voor het maken van een vliegreis	4%
Om toegang te krijgen tot een site of app	20%
Om toegang te krijgen tot een kantoor of bedrijventerrein	2%
Anders	2%

Bron: Enquête onder bevolking

3. Identiteitsfraude

Het afgelopen jaar gaf 3% van de geënquêteerden aan te maken te hebben gehad met een ongewenste dubbelganger. De drie meest voorkomende typen van identiteitsfraude zijn misbruik van een account van een webwinkel, misbruik van een sociaal media-account of berichtenservice, en misbruik van persoonsgegevens om toegang te krijgen tot een bankrekening.

Voor zover er achter identiteitsfraude een financieel motief zit, slaagt de dader lang niet altijd in zijn opzet. In 18% van alle gevallen heeft het slachtoffer daadwerkelijk financiële schade geleden. Ruim een derde van de geënquêteerden geeft aan naast eventuele financiële schade ook nog andere hinder te hebben ondervonden. De meesten geven aan dat het hen (redelijk) wat moeite heeft gekost het probleem op te lossen.

Je bericht

Hi Scott,

Zou je een foto kunnen sturen van je rijbewijs zodat ik kan checken dat ik het geld aan de juiste persoon overmaak?

Met vriendelijke groet,

JP

3.1 Omvang van het probleem

Het afgelopen jaar gaf 3% van de mensen die wij enquêteerden aan te maken te hebben gehad met een ongewenste dubbelganger. Zij gaven aan in de afgelopen twee jaar (24 maanden) te maken te hebben gehad met een persoon of organisatie die zich buiten hun wil om voor hen had uitgegeven. Wanneer we dit percentage vergelijken met die van voorgaande jaren, is er geen duidelijke trend waarneembaar. De slachtofferpercentages waarover wij sinds 2014 rapporteren, schommelen tussen de 2,1% (2014) en 5,7% (2017).

TABEL 34: Omvang identiteitsfraude 'Heeft iemand, voor zover u weet, zich in de afgelopen 2 jaar (24 maanden) wel eens zonder uw toestemming voor u voorgedaan?'

2014 (n=1.987)	2015 (n=4.853)	2017 (n=4.789)	2019 (n=4.994)	2021 (n=2.473)
2,1%	3,4%	5,7%	4,1%	3,0%

Bron: enquête onder bevolking

Kijkend naar de omvang en trends op basis van andere onderzoeken en registraties ontstaat een wisselend beeld. Dat komt vooral door de verschillende manieren waarop het begrip identiteitsfraude wordt gedefinieerd. In sommige publicaties wordt fraude strikt gedefinieerd

als een misdrijf waaraan een financieel motief ten grondslag ligt, andere studies (waaronder voorliggende) hebben een bredere definitie en scharen er ook niet-financieel gemotiveerde misdrijven onder zoals identiteitsmisbruik om iemand zwart te maken. We geven hier een overzicht van de meest actuele publicaties; de manier waarop daarin identiteitsfraude is afgebakend; en de eventuele trends die daarin zijn gevonden.

Identiteitsfraude als financieel delict: het CBS houdt sinds 2012 met een grootschalige enquête bij hoeveel mensen er slachtoffer zijn geweest van identiteitsfraude⁴. Het CBS gebruikt het begrip identiteitsfraude als label, dat zij plakt op drie specifieke vormen van financiële criminaliteit: skimming (kopiëren en vervolgens misbruiken van bankpassen), pharming (door middel van malware inbreken op een computer om toegang te krijgen tot een bankrekening) en phishing (ontfutselen van inloggegevens van een bankrekening). Veel vormen van identiteitsfraude vallen buiten deze afbakening. Het verklaart waarom CBS sinds 2012 lagere slachtofferpercentages publiceert en laat vooral ook zien dat financiële instellingen er tot nu toe in slagen het probleem te beheersen. Het slachtofferpercentage ligt al geruime tijd rond de 0,5% (zie tabel 69).

⁴ Sinds 2017 wordt het onderzoek in de oneven jaren uitgevoerd, daarvoor was het een jaarlijks terugkerend onderzoek.

Identiteitsfraude als een verzamelbegrip: in 2019 is onderzoek gedaan naar de aard en verschijningsvormen van digitale criminaliteit op basis van politieregistraties. Van identiteitsfraude is in dit onderzoek sprake zodra politiemensen een voorval in hun registratiesysteem als zodanig beschrijven. Het is een delict dat met name samenhangt met inbraak op een mailaccount, verdachte links die worden verstuurd via mail of berichtendiensten, en misbruik van webshopaccounts (het doen van bestellingen op naam van een ander). Op basis hiervan wordt het totaal aantal registraties van identiteitsfraude op ruim 34.210 geschat, wat neerkomt op 0,9% van het totale aantal politieregistraties⁵.

Een vergelijkbare manier om de aard en omvang van het probleem in beeld te krijgen wordt gehanteerd door Fraudehelpdesk. Deze organisatie waar burgers en bedrijven zich kunnen melden met uiteenlopende meldingen en vragen over fraude, spreekt van identiteitsfraude wanneer iemands identiteit wordt misbruikt. Dat hoeft niet altijd de identiteit te zijn van degene die schade leidt. Zo rapporteerde Fraudehelpdesks afgelopen jaar een zeer sterke stijging van identiteitsfraude, welke hoofdzakelijk het gevolg van een explosieve toename van Whatsapp hulpvragen. Het betreffen berichten waarmee criminelen met een valse hulpvraag, ontvangers geld proberen afhandig te maken. Vaak zijn het de mensen die zo'n hulpvraag ontvangen die de melding doen, en niet zozeer de mensen voor wie de fraudeur zich voordeed. Zie ook tabel 66 & 67.

Identiteitsfraude als reisdocumentfraude: in het kader van haar verantwoordelijkheid voor grenscontroles, controleert de Koninklijke Marechaussee identiteit van reizigers bij hun grenspassage. Met de kennis die zij daarmee heeft over fraude met reisdocumenten ondersteunt zij ook andere partijen zoals de IND, politie en gemeenten. Jaarlijks rapporteert zij over het aantal fraudes met reisdocumenten dat bij haar in beeld kwam⁶. In 2020 betroffen het in totaal 1.817 zaken. Hiermee is het aantal ten opzichte van eerdere jaren gedaald, wat door ECID toegeschreven wordt aan de reisbeperkingen als gevolg van corona. Zie ook tabel 72.

Identiteitsfraude als misbruik van iemands identiteit: een afbakening van het begrip identiteitsfraude die vergelijkbaar is met die in voorliggende monitor, is een Amerikaans onderzoek uit 2019⁷. In dit onderzoek verstaat men onder identiteitsfraude uiteenlopende delicten al dan niet ingegeven door financieel gewin. De meest voorkomende vormen betreffen: uitgaven doen op creditcardnummer van een ander, het openen van een bankrekening op naam van een ander, het afnemen van nutsvoorzieningen op naam van een ander, het aangaan van een dienstverband op naam van een ander (door illegale arbeidsmigranten) en het afnemen van medische zorg op naam van een ander. Volgens de studie is 12,7 % van de Amerikaanse bevolking van 16 jaar en ouder, over een periode van vijf jaar slachtoffer geweest van identiteitsmisbruik.

5 Beerthuizen, M., Sipma, T., & Van der Laan, A. (2020). Aard en omvang van dader- en slachtofferschap van cyber- en gedigitaliseerde criminaliteit in Nederland. Den Haag: WODC.

6 Identiteitsfraudekamer ECID. (2021). Statistisch jaaroverzicht van identiteits- en documentfraude in 2020. Den Haag: Expertisecentrum Identiteitsfraude en Documenten (ECID).

7 Center for Victim research. (2019). What we know about identity theft and fraud victims from research and practice based evidence. U.S. Department of Justice.

3.2 Ervaren kwetsbaarheid voor identiteitsfraude

De kern van identiteitsfraude is dat persoonsgegevens in handen zijn gekomen van mensen die daar misbruik van maken, al dan niet met een financieel motief. Om een beeld te krijgen van de mate waarin mensen zich er kwetsbaar voor voelen, is gevraagd of men wel eens het vermoeden heeft gehad dat persoonsgegevens zonder toestemming zijn doorverkocht, gelekt of gestolen. 9% van de geënquêteerden geeft aan dat dat in het afgelopen jaar (waarschijnlijk) gebeurd is. Het blijft echter een kwetsbaarheid die voor veel mensen onzichtbaar is en moeilijk te schatten. Een derde geeft aan geen inschatting te kunnen maken.

TABEL 35: **Zijn er in het afgelopen jaar persoonsgegevens van u zonder uw toestemming doorverkocht, gelekt of gestolen?**

	2021 (n=2.473)
Ja, zeker wel	2%
Waarschijnlijk wel	7%
Waarschijnlijk niet	21%
Nee, zeker niet	36%
Weet niet	33%
Wil niet zeggen	1%
Totaal	100%

Bron: enquête onder bevolking

Op de vraag of men wel eens bang is dat misbruik wordt gemaakt van één van hun online accounts antwoordt ruim een kwart 'ja'. Het beeld is voor verschillende typen van accounts (social media, e-mail en webwinkelaccounts) ongeveer hetzelfde.

TABEL 36: **Bent u wel eens bang dat iemand misbruik maakt van uw social media-, e-mail- en/of webwinkel account door zich voor u uit te geven?**

	social media (n=2.186)	e-mail (n=2.473)	webwinkel (n=2.307)
Ja	30%	26%	26%
Nee	68%	72%	72%
Wil niet zeggen	3%	3%	2%
Totaal	100%	100%	100%

Bron: enquête onder bevolking

3.3 Modus operandi van identiteitsfraude

Aan de deelnemers van de enquête die hebben aangegeven te maken te hebben gehad met iemand die zich voor hen had uitgegeven, is gevraagd te beschrijven wat er is voorgevallen. Op basis van de antwoorden kunnen, ongeacht de prevalentie, enkele typische modus operandi van identiteitsfraude worden onderscheiden. Wij illustreren de voorvallen aan de hand van quotes die zijn samengesteld uit antwoorden van één of enkele respondenten. Met onderstaande inventarisatie is geprobeerd een uitputtend overzicht te geven. Alle voorvallen die de 459 slachtoffers van

identiteitsfraude hebben beschreven, zijn er in principe mee afgedekt. Dit betekent niet dat de lijst uitputtend is voor alle mogelijke vormen van identiteitsfraude. Identiteitsfraude die bijvoorbeeld niet uit de enquête naar voren kwam is misbruik van een identiteitsbewijs om illegaal arbeid te verrichten of misbruik om een medische behandeling te ondergaan op naam van een ander.

TABEL 37: **Modus operandi van identiteitsfraude**

Wat is er gebeurd?

Webwinkelen op andermans rekening	‘Er zijn spullen op mijn naam gekocht bij een webwinkel. Deze spullen zijn op een ander adres afgeleverd dan de mijne. De rekening werd wél naar mij gestuurd’
Opgedrongen koopwaar	‘Ik kreeg het Sms-bericht dat ik ‘mijn aankoop’ kon afhalen bij het afhaalpunt van de supermarkt. Toen ik daar kwam moest ik voor het pakje betalen. Ik had echter niets besteld terwijl het wel op mijn naam en adres stond’
Overname van een account	‘Ik kreeg een e-mail met daarin een melding dat iemand was ingelogt op mijn social media-account. Ik was dat echter zelf niet. Ik heb toen uit voorzorg mijn wachtwoord gewijzigd’ ‘Mijn Netflix account wordt ook gebruikt door iemand anders’
Whatsapp hulpvraagfraude	‘Iemand heeft zich voorgedaan als mij in een whatsapp bericht aan met mijn moeder. Daarin werd om geld gevraagd. Omdat mijn moeder echt dacht dat ze met mij aan het chatten was, ging ze in op dit verzoek’
Aquisitiefraude	Ik kreeg een Sms-bericht waarin stond dat ik geld moest overmaken om een pakketje in ontvangst te kunnen nemen.
Creditcardfraude	‘Ik kreeg een Sms van mijn creditcardmaatschappij met het bericht dat er een goedkeuring was gegeven voor een redelijk hoog bedrag. Ze wilden weten of dat werkelijk van mij kwam. Ze merkten het aan als een verdachte transactie omdat ik nooit grote uitgaven doe met mijn creditcard. Het is dus vrijdeld.’
Datingsitefraude	‘Er is op mijn naam en met mijn foto een profiel aangemaakt op verschillende datingsites’
Phishing	‘Ik kreeg van de bank een mail waarin mij werd gevraagd om verschillende gegevens. Ik heb deze mail direct verwijderd’
Marktplaatsfraude	‘Op Marktplaats heeft iemand op mijn naam een advertentie geplaatst waarin gevraagd werd naar een bepaald type meubel. Ik heb dit gemeld bij Marktplaats’
Stalking	Ik wordt gestalked door mijn ex. Hij heeft mij opgegeven voor een woningbouwproject, heeft een profiel aangemaakt op een datingsite en een reservering gemaakt bij een sauna.
Ongewenst collegiaal gedrag	‘Tijdens mijn vakantie heeft een collega vanaf mijn adres mails gestuurd naar verschillende klanten.’
Bankfraude	‘Er is een lening afgesloten op mijn naam’
Reizen op andermans kosten	‘Iemand heeft met mijn OV-kaart op mijn kosten gereisd’
Misbruik van DigiD	‘Mijn ex-partner heeft met mijn DigiD ingelogd om het gezag over de kinderen te krijgen’

Bron: Slachtofferenquête

Identiteitsfraude is min of meer gelijk verdeeld over de verschillende leeftijdsklassen. In de voorgaande edities van de monitor kwam het als een delict naar voren waar jongere mensen sneller last van hadden. Een verklaring voor deze verandering is dat de aard van identiteitsfraude is veranderd. Er is een afname van fraude via social media met als doel om iemand te pesten en een toename van fraude met een financieel motief. Dit laatste type van fraude is minder leeftijdsgevoelig.

TABEL 38: **Identiteitsfraude: slachtofferpercentage per leeftijdscategorie**

	2019 (n=109)	2021 (459)
16 - 30 jaar	7,2 %	3,7%
31 - 45 jaar	4,9 %	3,9%
46 - 54 jaar	4,2 %	3,4%
55 - 69 jaar	2,4 %	1,8%
70 plus	1,1 %	2,8%

Bron: Slachtofferenquête

3.4 Identiteitsfraude: een indeling op basis van dader, middel en doel

Wat de beschrijvingen in tabel 37 duidelijk maken, is dat identiteitsfraude volgens de door ons gehanteerde definitie een veelvormig delict is.

Ondanks die ene overeenkomst dat iemands identiteitsgegevens zijn misbruikt, zijn de situaties niet altijd goed met elkaar te vergelijken. Zo is het misbruik van identiteitsgegevens door een gekrenkte ex-partner van een andere orde dan de diefstal van inloggegevens door een anonieme hacker om in te kunnen breken op een bankrekening van een willekeurig slachtoffer. Het overall slachtofferpercentage van 3%, krijgt daarom pas zeggingskracht wanneer het begrip identiteitsfraude nader wordt ontleed. Aan de hand van de volgende drie vragen zijn er drie betekenisvolle indelingen te maken:

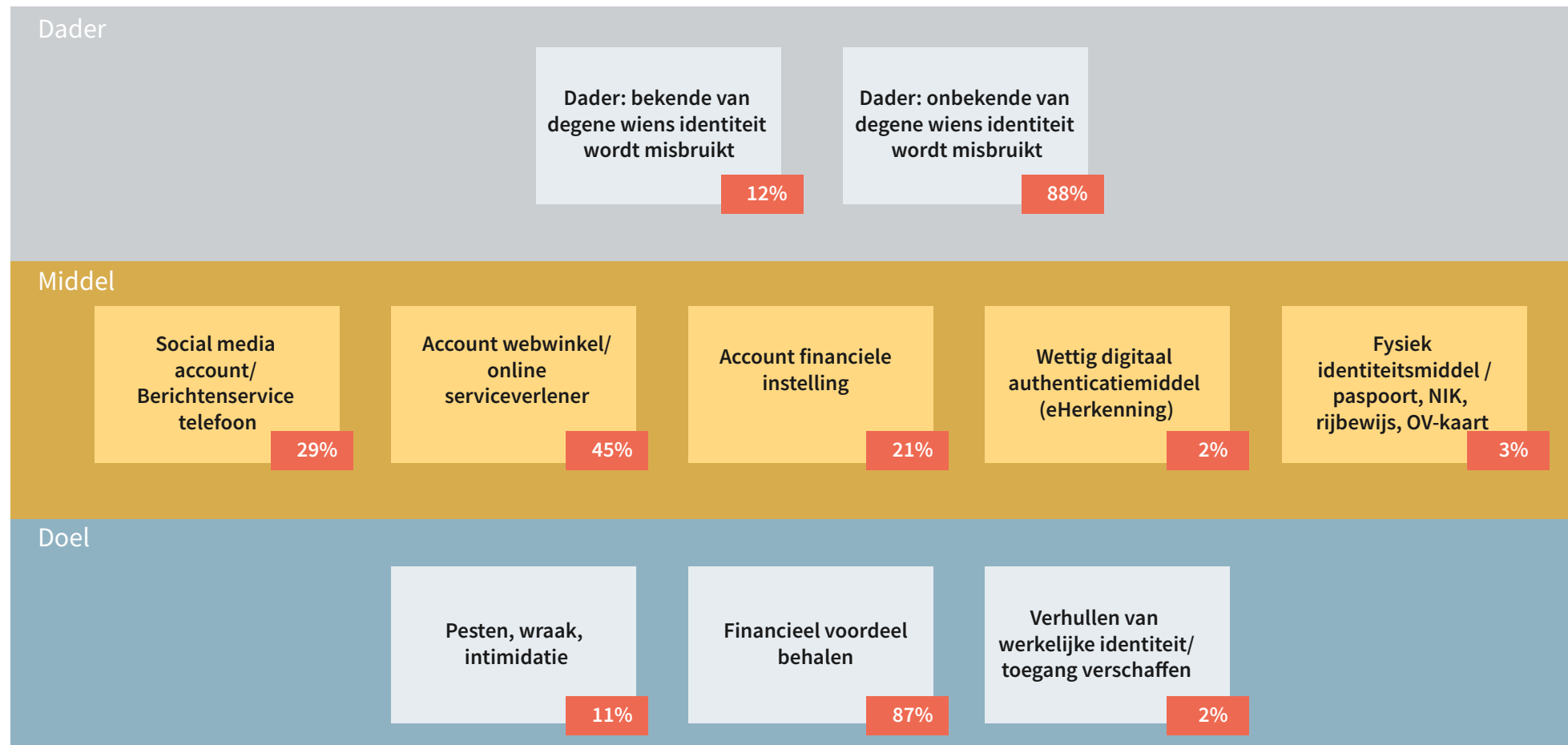
a) Kennen dader en slachtoffer elkaar? Er zijn op basis van deze vraag twee typen delicten te onderscheiden: ten eerste het delict waarbij een dader het specifiek gemunt heeft op de persoon van het slachtoffer; ten tweede het delict waarbij het de dader niet zozeer te doen om een specifiek persoon te benadelen maar vooral een gelegenheid ziet om voordeel te behalen.

b) Welk identiteitsmiddel of type platform is misbruikt? Er zijn op basis van deze vraag vijf typen van fraude te onderscheiden. Misbruik van een social media account (bijvoorbeeld een berichtendienst, netwerkkapp of datingsite), een account van een webwinkel of online serviceprovider (bijvoorbeeld een account van een telefoonaanbieder of zorgverzekeraar), een account van een financiële dienstverlener (bijvoorbeeld een bank of handelsplatform voor cryptovaluta), een authenticatiemiddel (bijvoorbeeld DigiD) of misbruik van een fysiek identiteitsmiddel (bijvoorbeeld rijbewijs, paspoort, identiteitskaart, OV-chipkaart).

c) Wat is het motief van de dader? Zoals eerder aangegeven wordt soms onderscheid gemaakt tussen misbruik en fraude. Fraude zou zich van misbruik onderscheiden vanwege het financiële motief. Kijkend naar de casuïstiek kan ook hier dat onderscheid gemaakt worden. Er zijn delicten die primair zijn ingegeven door financieel gewin, er zijn er ook die tot doel hebben een slachtoffer te frustreren. Er is daarnaast ook nog een delict dat niet goed in deze tweedeling past, namelijk het misbruik van iemand anders zijn identiteit om de eigen identiteit te verhullen bijvoorbeeld om een straf te ontlopen.

In figuur 3 zijn op basis van de drie indelingen die aan de hand van bovenstaande vragen te maken zijn verschillende elementen van identiteitsfraude van elkaar onderscheiden en gekwantificeerd.

Figuur 3: Drie manieren om identiteitsfraude en -misbruik in te delen: dader, middel, doel



Een vierde kenmerk van identiteitsfraude aan de hand waarvan een betekenisvolle indeling kan worden gemaakt, maar die voorlopig buiten het schema is gehouden (om deze niet te ingewikkeld te maken), is impact. Er bestaan grote verschillen in de impact die identiteitsfraude op mensen kan hebben. Voor 34% van de geënquêteerden was het incident ernstig

genoeg om contact te leggen met een instantie: om het op te lossen, om advies te vragen, of om het aan te geven (zie ook tabel 48). 18% heeft financiële schade geleden, en 36% zegt er ook op een andere manier last van te hebben gehad. Regelmatig rapporteren mensen uit deze groep dat hun vertrouwen in anderen of henzelf is aangetast (zie ook tabel 37 en 40).

In het vervolg van deze paragraaf ontleden wij het begrip en de prevalentie van identiteitsfraude op de drie manieren die in figuur 3 zijn onderscheiden.

a.) Dader

12% van de mensen die aangaven te maken te hebben gehad met identiteitsfraude of -misbruik geeft aan de persoon te kennen die zich voor hem/haar heeft voorgedaan. Het zijn vaak mensen in de directe sociale omgeving. Regelmatig is het een ex partner of gezins-/familielid.

Een groep respondenten die zich op dit punt onderscheidt, betreffen de mensen die die dader uiteindelijk ook hebben aangesproken. Het gaat dan voornamelijk om het gebruik van andermans account of creditcard voor het doen van een aankoop. Een voorbeeld hiervan is de moeder wiens zoon op haar telefoon een game had geactiveerd, waarmee hij uitgaven heeft gedaan. Naast de bekenden die in tabel 39 zijn onderscheiden, benoemen de geënquêteerden onder andere een pakketbezorger, een ex schoonzus, de nieuwe vriendin van de ex-partner en een clubgenoot als degene die hun persoonsgegevens heeft misbruikt.

TABEL 39: Kent u de persoon die zich voor u heeft voorgedaan?

	2019 (n=438)	2021 (n=459)
Ja	23%	12%
Nee	77%	88%
Totaal	100%	100%

Bron: Slachtofferenquête

TABEL 40: Wie was deze persoon?

	(n=53)
(ex) Partner	38%
Gezins- of familielid (niet zijnde een (ex) partner)	15%
Vriend of kennis	8%
Buur of buurtgenoot	8%
Collega	6%
Klas- of studiegenoot	2%
Iemand anders	25%
Totaal	100%

Bron: Slachtofferenquête

b.) Middel

Identiteitsfraude- en misbruik waarover de geënquêteerden rapporteren, is bij uitstek een delict dat plaatsvindt in het digitale domein. Gevallen waarbij de dader zich in het fysieke domein identificeerde aan de hand van een fysiek identiteitsmiddel dat niet van hem was maar van iemand anders, komen in dit onderzoek weinig naar voren. Een voorbeeld van een casus waarin dit wel het geval was, betrof een man die er na enige tijd achter kwam dat iemand op zijn Ov-kaart reisde. Er zijn wel meerdere gevallen waarbij sprake was van een ‘hybride domein’, waarbij een dader weliswaar gebruik maakte van een fysieke (kopie) van een identiteitsmiddel, maar zich digitaal (op afstand) tot het slachtoffer of een instantie verhiel. Een voorbeeld hiervan is de vrouw op wiens naam een lening werd afgesloten waarbij onder andere een kopie van haar identiteitsbewijs is gebruikt.

Wat net als voorgaande jaren duidelijk naar voren komt, is dat voor zover er kwetsbaarheden zijn, die vooral zitten bij de private platforms en accounts. Misbruik van publieke authenticatie- of identiteitsmiddelen – digitaal dan wel fysiek – komt weinig voor. Hierbij moet worden opgemerkt dat misbruik van publieke middelen waarschijnlijk ook een vorm van identiteitsfraude is die met een slachtofferenquête niet altijd naar voren komt, omdat burgers er niet altijd direct zelf slachtoffer van zijn. Te denken valt bijvoorbeeld aan de fraude waarnaar de Koninklijke Marechaussee onderzoek doet: fraude met reisdocumenten

in het kader van illegale immigratie. Met betrekking tot het publieke authenticatiemiddel DigiD zijn er wel enkele mensen die aangeven te maken te hebben gehad met misbruik. Het ging in deze gevallen meestal om misbruik door een ex-partner. Een voorbeeld daarvan is de man die aangeeft dat zijn ex-partner, net voor het beëindigen van de relatie met zijn DigiD het gezag over de kinderen heeft gewijzigd.

TABEL 41: Welke middelen zijn misbruikt?⁸

	(n=459)
Account van een webwinkel of serviceprovider	45%
Social media account / berichtenservice gebaseerd op telefoonnummer	29%
Account financiële instelling / creditcard	21%
Wettig digitaal authenticatiemiddel (DigiD, eHerkening)	2%
Fysiek identiteitsmiddel (paspoort, identiteitskaart, rijbewijs, ov-kaart)	3%
Totaal	100%

Bron: Slachtofferenquête

⁸ Met betrekking tot ID-middelen is de vraagstelling in 2021 iets gewijzigd ten opzichte van 2019, waardoor niet kan worden vergeleken tussen deze twee jaren.

c.) Doel

Op basis van de vraag hoe men merkte dat er iemand anders was die zich voor hen uitgaf, hebben wij een inschatting gemaakt van het doel achter de fraude. In veruit de meeste gevallen is dat een financieel doel. Het is de dader meestal te doen om financieel voordeel te behalen door een aankoop te doen zonder daarvoor te betalen (45%), of door met een valse vraag geld via een berichtenservice te vragen (12%), of door inbraak op iemands bankrekening (21%). In 11% van de gevallen was er geen financieel motief maar vooral een persoonlijk motief. Het was de dader dan te doen om het slachtoffer te frustreren, te pesten of zwart te maken. In 3% van de gevallen tenslotte, probeerde de dader ergens toegang toe te krijgen. Een voorbeeld hiervan is de man wiens rijbewijs werd misbruikt door iemand die werd aangehouden als zwartrijder in het openbaar vervoer, of de man die de DigiD van zijn ex gebruikte om gezag over de kinderen te krijgen.

TABEL 42: Doel achter identiteitsfraude

Doel		2019 (n=438)	2021 (n=459)
Financieel voordeel behalen	Misbruik webwinkelaccount, berichtenservice, account financiële instelling	70%	87%
Pesten, wraak, intimidatie	Misbruik accounts sociale media om iemand zwart te maken/pesten	27%	11%
Eigen identiteit verhullen	o.a misbruik van iemand ID kaart om straf te ontlopen, misbruik van DigiD	3%	2%
Totaal		100%	100%

Bron: Slachtofferenquête

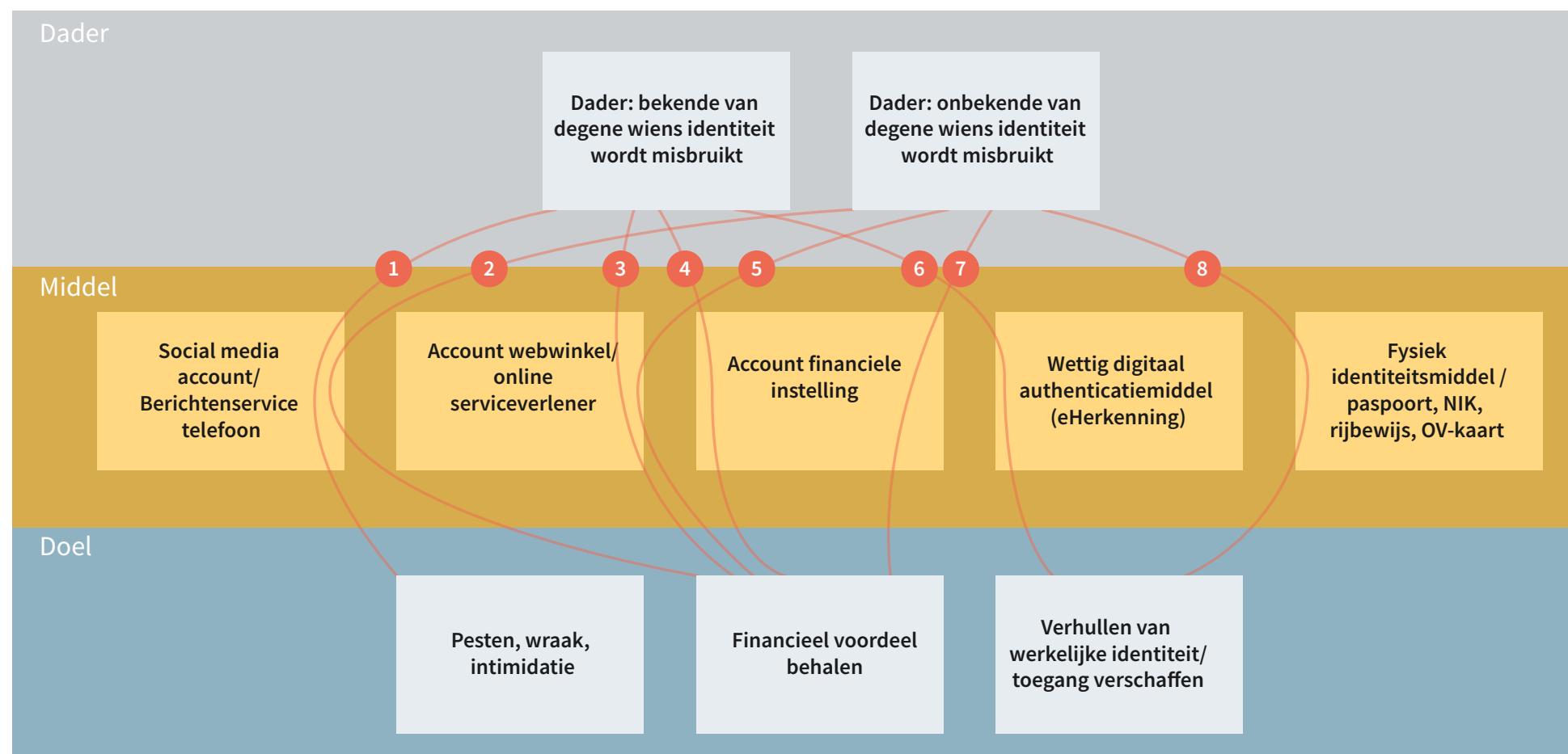
Bij het onderscheid dat hier gemaakt wordt tussen typen van identiteitsfraude op basis van doel moet worden opgemerkt dat de dader lang niet altijd in zijn opzet slaagt. Vaak is het bij een poging gebleven. Slechts in 18% van alle gevallen leidt het slachtoffer ook daadwerkelijk schade (zie tabel 44). Een voorbeeld daarvan is de man die via zijn telefoon een melding kreeg dat iemand probeerde in te loggen op zijn account. Deze man heeft daarop zijn wachtwoord aangepast. Een ander voorbeeld is de man die door zijn creditcardmaatschappij wordt benaderd met de vraag over een ongebruikelijke transactie, en daardoor kon voorkomen dat de transactie daadwerkelijk plaatsvond.

3.5 Acht typen van identiteitsfraude

In praktisch elke casus van identiteitsfraude lopen de eerder genoemde indelingen door elkaar heen. Misbruik van een webwinkelaccount kan gepleegd worden door een onbekende of bekende van het slachtoffer, en

iemand kan inbreken op een sociale media-account om te pesten of om financieel voordeel te behalen. In onderstaande figuur zijn de combinaties weergegeven die uit de slachtofferenquête kunnen worden afgeleid.

Figuur 4: Acht typen van Identiteitsfraude



Op basis van de enquête zijn de acht onderscheiden vormen gekwantificeerd. Onderstaande tabel geeft een overzicht. De nummers in onderstaande tabel corresponderen met die in figuur 4. De percentages in de linker kolom tellen niet op tot 100% omdat een deel van de casussen (18%) buiten deze indeling valt.

TABEL 43: Acht vormen van identiteitsfraude	
	2021
1. Online pesten/intimideren	10%
2. Geld vragen uit naam van iemand (buiten diens medeweten)	9%
3. Misbruik van webwinkelaccount/service provider door een bekende	7%
4. Hacken van account webwinkel/ service provider door een onbekende	38%
5. Misbruik van bankrekening door een bekende	2%
6. (Poging) Hacken van bankrekening door een onbekende	18%
7. Misbruik van een wettig digitaal authenticatiemiddel (DigiD) door een bekende	2%
8. Eigen identiteit verhullen door misbruik fysiek ID-middel (b.v. om boete te ontlopen)	1%

Bron: Slachtofferenquête

Het schema uit figuur 4 is gebaseerd op het schema uit de voorgaande editie van de monitor (2019). Het schema is dit jaar wel aangepast. Op basis van enkele casussen over misbruik van DigiD onderscheiden we nu vijf in plaats van vier middelen die kunnen worden misbruikt. Het is goed denkbaar dat het schema de komende jaren opnieuw moet worden aangepast. Er zullen nieuwe vormen van identiteitsfraude bijkomen, terwijl andere wellicht verdwijnen of minder belangrijk worden. In de gesprekken die wij voerden met de partijen uit het identiteitsstelsel kwamen twee vormen van identiteitsfraude naar voren die mogelijk in de komende jaren gaan opspelen:

- Fraude met DigiD door onbekenden: hoewel het gebruik van DigiD het afgelopen jaar een grote vlucht heeft genomen, werd door heel weinig geënquêteerden aangegeven dat er misbruik was gemaakt van zijn of haar DigiD. Geen van de geënquêteerde rapporteerde over een gehacked DigiD-account, door een onbekende. Het is denkbaar dat dat verandert naarmate er meer partijen zich aansluiten op DigiD, waarmee de DigiD-inloggegevens waardevoller worden.

- Fraude met biometrische gegevens: identificatie van biometrie is in opkomst (zie ook tabel 32). Tot nu toe is in de slachtofferenquête nooit melding gedaan van misbruik van biometrische gegevens. De afgelopen jaar is er bij de politie wel een enkele melding geweest van identiteitsfraude waarbij gebruik is gemaakt van deep fakes: een video of audio gesprek waarbij iemands beeld of stem is vervalst. Het betreffen echter incidenten die nog in geen enkele statistiek zichtbaar zijn.

3.6 Schade en hinder

Identiteitsfraude leidt in 18% van de gevallen tot financiële schade. Er zijn met name drie vormen van identiteitsfraude die leiden tot financiële schade: oplichting via webwinkels, misbruik maken van inloggegevens van een bank of creditcardgegevens, whatsapp hulpvraagfraude.

TABEL 44: Heeft u financiële schade geleden?

	2015 (n=552)	2017 (n=460)	2019 (n=438)	2021 (n=459)
Ja	19%	23%	21%	18%
Nee	79%	75%	78%	82%
Geen antwoord	2%	2%	1%	0%
Totaal	100%	100%	100%	100%

Bron: Slachtofferenquête

Net als voorgaande jaren lopen de schade bedragen sterk uiteen: van enkele euro's tot meer dan €10.000. Het gemiddelde ligt dit jaar op € 6.270. Dat is hoger dan in 2019, waarbij direct moet worden opgemerkt dat dit wordt bepaald door de enkele zaken in 2021 waarbij het fraudebedrag zeer hoog was. Net als voorgaande jaren heeft het gemiddelde schadebedrag weinig zeggingskracht omdat de bedragen sterk uiteenlopen. Ongeveer de helft van de slachtoffers met financiële schade, raamt deze op een bedrag tot 500 euro. In zo'n 60% van de gevallen is de schade uiteindelijk (gedeeltelijk) gecompenseerd (zie tabel 46).

TABEL 45: Hoe hoog was de schade?

	2019 (n=81)	2021 (n=76)
Gemiddeld schadebedrag	€ 5.047	€ 6.270
Minder dan € 25	4%	7%
€ 25 - € 50	5%	5%
€ 50 - € 100	14%	7%
€ 100 - € 250	19%	17%
€ 250 - € 500	19%	9%
€ 500 - € 1.000	19%	16%
€ 1.000 - € 1.500	5%	4%
€ 1.500 - € 2.500	5%	8%
€ 2.500 - € 10.000	6%	15%
meer dan € 10.000	5%	13%
Totaal	100%	100%

Bron: Slachtofferenquête

Tabel 46: Aard van de schade en compensatie

	2019 (n=92)	2021 (n=82)	Is de schade gecompenseerd?			
			ja	nee	gedeeltelijk	weet niet
Er is geld van mij gestolen	29%	35%	41%	38%	21%	0%
Ik heb moeten betalen voor producten of diensten die ik niet heb besteld of afgenomen	52%	45%	41%	49%	8%	3%
Kosten voor juridische bijstand	13%	6%	40%	60%	0%	0%
Aanschaf van een nieuw identiteitsbewijs	15%	10%	25%	75%	0%	0%
Telefoonkosten, postzegels, etc.	12%	11%	0%	100%	0%	0%
Anders	14%	17%	0%	93%	7%	0%

Bron: Slachtofferenquête

Ruim een derde van de geënquêteerden geeft aan naast eventuele financiële schade ook nog andere hinder te hebben ondervonden. In de enquête is aan de deelnemers gevraagd te beschrijven wat die hinder inhield. Uit de antwoorden leiden wij af dat de impact van identiteitsfraude groot kan zijn. Er wordt regelmatig gesproken over verlies van vertrouwen in zichzelf en in anderen. In veel gevallen komt de fraude over als een gebeurtenis waar mensen weinig of helemaal geen grip op hebben.

TABEL 47: Heeft u (naast eventuele financiële schade) nog op andere wijze hinder gehad van de fraude?

	2015 (n=552)	2017 (n=461)	2019 (n=438)	2021 (n=459)
Ja	32%	31%	40%	36%
Nee	65%	67%	58%	62%
Geen antwoord	3%	2%	2%	2%
Totaal	100%	100%	100%	100%

Bron: Slachtofferenquete

3.7 Ontvangen hulp

Niet altijd wordt hulp gezocht bij identiteitsmisbruik. Van de geënquêteerden wendde 34% zich tot één of meerde instanties voor hulp advies of om aangifte te doen. Wat opvalt is dat 53% contact heeft gezocht met de politie, maar dat 15% uiteindelijk aangifte doet. Op de vraag waarom men geen aangifte doet, wordt regelmatig geantwoord

dat er te weinig aanknopingspunten waren, dat aangifte weinig toegevoegde waarde heeft als er geen financiële schade is geleden, of dat de betrokkene zich volgens de politie beter tot de instantie kon wenden (bijvoorbeeld een webwinkel) om het probleem op te lossen.

Tabel 48: Met welke instantie(s) heeft u contact gezocht (meerdere antwoorden mogelijk)

	2015 (n=283)	2017 (n=215)	2019 (n=250)	2021 (n=158)
Politie	25%	34%	32%	53%
Bank	38%	32%	32%	44%
Fraudehelpdesk	9%	14%	10%	22%
Bedrijf waar men zich voor mij heeft uitgegeven	9%	7%	22%	17%
Centraal Meldpunt Identiteitsfouten en -fraude (CMI)	5%	12%	12%	16%
Provider van social media en/of e-mail	18%	33%	21%	15%
Internetprovider	10%	17%	10%	11%
Gemeente	5%	7%	5%	6%
Zorgaanbieder	4%	4%	3%	3%
UWV	1%	1%	0%	1%
Belastingdienst	1%	3%	2%	1%
Anders	25%	17%	11%	23%

Bron: Slachtofferenquête

Net als voorgaande edities van de monitor is de tevredenheid over de hulp die wordt geboden door banken het grootst. Al zijn de verschillen tussen de instanties afgelopen jaar minder groot. Het optreden van banken wordt gemiddeld beoordeeld met het rapportcijfer 7.3. Het positieve oordeel zal samenhangen met het gegeven dat mensen die geconfronteerd worden met identiteitsfraude via hun bank, meestal gecompenseerd worden. Regelmatig ontdekken banken onrechtmatigheden zelfs eerder dan de rekeninghouder zelf.

TABEL 42: Hoe beoordeelt u de wijze waarop u bent geholpen? (1 'zeer slecht'...10 'uitmuntend')

	2021
Bank	7,3 (n=69)
Centraal Meldpunt Fraude en Fouten (CMI)	7,2 (n=24)
Fraudehelpdesk	7,0 (n=32)
Politie	6,7 (n=84)
Provider (internet, social media)	6,2 (n=23)

Bron: Slachtofferenquête

Ruim de helft (52%) van de slachtoffers geeft aan dat het (redelijk wat) moeite heeft gekost om het probleem op te lossen. Voor zover het probleem inmiddels is opgelost, deed 70% daar langer dan een week over.

TABEL 43: Binnen welke termijn was het probleem opgelost?

	2015 (n=397)	2017 (n=331)	2019 (n=318)	2021 (n=285)
Binnen een dag	24%	20%	23%	30%
Binnen een week	30%	35%	33%	33%
Binnen een maand	30%	29%	30%	22%
Binnen een half jaar	12%	15%	11%	13%
Langer dan een half jaar	4%	1%	2%	1%
Totaal	100%	100%	100%	100%

Bron: Slachtofferenquête

3.7 Ontvangen hulp

Niet altijd wordt hulp gezocht bij identiteitsmisbruik. Van de geïnterviewden wendde 34% zich tot één of meerdere instanties voor hulp advies of om aangifte te doen. Wat opvalt is dat 53% contact heeft gezocht met de politie, maar dat 15% uiteindelijk aangifte doet. Op de vraag waarom men geen aangifte doet, wordt regelmatig geantwoord

dat er te weinig aanknopingspunten waren, dat aangifte weinig toevoegde waarde heeft als er geen financiële schade is geleden, of dat de betrokkene zich volgens de politie beter tot de instantie kon wenden (bijvoorbeeld een webwinkel) om het probleem op te lossen.

Tabel 4b: Met welke instantie(n) heeft u contact gezocht (meerdere antwoorden mogelijk)

	2015 (n=288)	2017 (n=215)	2019 (n=258)	2021 (n=258)
Politie	25%	34%	32%	53%
Bank	36%	32%	32%	44%
Fraudehulpdesk	9%	14%	10%	22%
Bedrijf waar men zich voor mij heeft uitgegeven	9%	7%	22%	17%
Centraal Meldpunt Identiteitsfouten en -fraude (CMI)	5%	12%	12%	10%
Provider van social media en/of e-mail	18%	33%	21%	15%
Internetprovider	10%	17%	10%	11%
Gemeente	5%	7%	5%	0%
Zorgaanbieder	4%	4%	3%	3%
UWV	1%	1%	0%	1%
Belastingdienst	1%	3%	2%	2%
Anders	25%	17%	11%	23%

4. Kengetallen uit het stelsel

4.1 Rijksdienst voor Identiteitsgegevens (RvIG)

De Rijksdienst voor Identiteitsgegevens (RvIG) is verantwoordelijk voor het beheer van de Basisregistratie Personen (BRP), het stelsel van reisdocumenten en het beheer en de uitgifte van Burgerservicenummers (BSN) aan gemeenten. Daarmee neemt RvIG een centrale plaats in,

in het Nederlandse identiteitsstelsel. Ook het Centraal Meldpunt Identiteitsfraude (CMI) is een onderdeel van RvIG, evenals het Meldpunt Fouten in Overheidsregistraties (MFO), dat op 1 januari 2021 is opgericht.

TABEL 51: Aantal paspoorten en identiteitskaarten in omloop (x 1.000.000)

	2012	2013	2014	2015	2016	2017	2018	2019	2020
Paspoorten	10,1	10,1	10,2	8,7	8,8	8,4	8,0	9,3	9,6
Identiteitskaarten	7,8	7,8	8,0	7,2	7,1	6,4	5,9	7,3	7,4

Bron: RvIG, 2021

TABEL 52: Uitgegeven paspoorten en identiteitskaarten

	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Aantal uitgegeven paspoorten	2.158.965	1.852.789	1.921.886	1.792.056	1.893.174	2.169.638	1.886.703	769.662	392.843	615.550
Aantal uitgegeven identiteitskaarten	1.497.960	1.215.549	1.348.180	1.610.532	1.805.762	1.725.632	1.333.337	694.062	543.714	777.566

Bron: RvIG, 2021

TABEL 53: Vermissingen (x 1.000)

	2012	2013	2014	2015	2016	2017	2018	2019	2020
Aantal paspoorten gestolen/vermist	49,2	48,6	54,6	54,9	58,8	62,7	59,4	52,6	33,2
Aantal identiteitskaarten gestolen/vermist	129,9	135,0	148,1	148,3	152,9	157,4	162,9	134,4	97,0
Aantal personen met 3 of meer vermissingen van paspoorten en/of identiteitskaarten		8,0	8,1	12,9	13,6	14,7	10,5		

Bron: RvIG, 2021

Centraal Meldpunt Identiteitsfraude

Burgers die mogelijk slachtoffer zijn geworden van identiteitsfraude kunnen dat melden bij het Centraal Meldpunt Identiteitsfraude (CMI). Het CMI registreert de meldingen en geeft advies en ondersteuning en schakelt eventueel met ketenpartners zoals bijvoorbeeld Belastingdienst of politie. Daarnaast levert het CMI een bijdrage aan bewustwording en preventie van identiteitsfraude. Het aantal meldingen dat het CMI

ontving, is in de periode 2010 tot 2020 jaarlijks gestegen van 152 tot 6.765. In 2021 nam het iets af, in dat jaar waren er 6.397 meldingen. Tabel 54 geeft een overzicht, in tabel 55 zijn de meldingen gespecificeerd. Tot eind 2020 konden burgers ook bij het CMI terecht voor het melden van fouten in identiteitsgegevens. Sinds 2021 is daar een apart meldpunt voor, namelijk het Meldpunt Fouten in Overheidsregistraties (MFO).

TABEL 54: Aantal meldingen bij het Centraal Meldpunt Identiteitsfraude (CMI)

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020	2021
Meldingen van ID-fraude	152	209	266	583	793	769	1.677	2.915	3.249	4.142	6.765	6.397
Meldingen van fouten	11	13	25	34	51	36	47	50	58	50	72	nvt

Bron: Centraal Meldpunt Identiteitsfraude, 2021

TABEL 55: Meldingen uitgesplitst naar middel

	2016	2017	2018	2019	2020	2021
BSN	4%	2%	1%	1%	1%	2%
DigiD	4%	2%	4%	2%	2%	4%
Gestolen gegevens	1%	0%	0%	0%	1%	1%
ID-bewijs gestolen en vermist	6%	4%	3%	3%	4%	4%
Kopie van identiteitsbewijs	40%	41%	45%	43%	30%	38%
Mailadres	7%	4%	3%	3%	3%	2%
Openbare gegevens ⁹	26%	23%	22%	23%	28%	32%
Overige	5%	5%	3%	3%	1%	1%
Bankpas	2%	3%	3%	2%	2%	2%
Creditcard	2%	2%	2%	1%	1%	0%
Onbekend	4%	2%	2%	2%	1%	1%
Foto (=nieuw)		4%	5%	7%	8%	5%
Account gehackt (=nieuw)		7%	7%	10%	17%	7%
Totaal	100%	100%	100%	100%	100%	100%

Bron: Centraal Meldpunt Identiteitsfraude, 2021

⁹ Gegevens die vrij beschikbaar zijn zoals naam, adres en telefoonnummer

Meldpunt Fouten in overheidsregistraties

Sinds januari 2021 bestaat het Meldpunt Fouten in Overheidsregistraties (MFO). Het meldpunt is opgericht naar aanleiding van een kritisch rapport van de Algemene rekenkamer, waaruit duidelijk werd dat in het huidige stelsel en het structurele hergebruik van persoonsgegevens ertoe kan leiden dat mensen hun grip op hun eigen gegevens kunnen verliezen. Het MFO helpt burgers, bedrijven en overheidsorganisaties bij het corrigeren van een fout in een overheidsregistratie. Het meldpunt wijst de weg naar de overheidsorganisatie die het onjuiste gegeven kan corrigeren. Als dat niet lukt, gaat het aan de slag om de fout en de problemen die daardoor zijn ontstaan te helpen oplossen. Het helpt waar mogelijk om aanmaningen en boetes te laten stoppen. Zolang er nog geen oplossing is, helpt het meldpunt betrokkenen niet verder in de problemen te komen¹⁰.

¹⁰ Digitale overheid, [Meldpunt Fouten in overheidsregistraties geopend](#), 5 januari 2021

TABEL 56: Meldingen fouten in overheidsregistraties

	Aantal meldingen 2021
Basisregistratie Personen (BRP)	343
Handelsregister (HR)	1
Basisregistratie Adressen en gebouwen (BAG)	10
Basisregistratie Topografie (BRT)	0
Basisregistratie Kadaster (BRK)	6
Basisregistratie Voertuigen (BRV)	7
Basisregistratie Inkomen (BRI)	5
Basisregistratie Waardering Onroerende Zaken (WOZ)	7
Basisregistratie Grootschalige Topografie (BGT)	0
Basisregistratie Ondergrond (BRO)	0
Meerdere registraties	31
Overige registraties	95
Totaal	505

Bron: MFO, 2021

4.2 RDW

RDW is een zelfstandig bestuursorgaan dat de registratie van gemotoriseerde voertuigen en rijbewijzen in Nederland verzorgt. In die

hoedanigheid heeft zij overzicht van het aantal in omloop zijnde en aantal uitgegeven rijbewijzen.

TABEL 57: Aantal rijbewijzen (x 1.000.000)

	2012	2013	2014	2015	2016	2017	2018	2019	2020
Aantal nieuwe rijbewijzen	1,2	1,0	1,2	1,2	1,5	1,9	1,9		
Aantal rijbewijzen in omloop	10,9	11,1	11,6	11,6	11,8	11,7	11,9	11,2	11,4

Bron: RDW 2021

TABEL 58: Omwisselingen en departementale uitgiften (x 1.000)

	2012	2013	2014	2015	2016	2017	2018
Aantal omwisselingen binnen de EU/EVA	10,6	11,6	15,0	15,1	16,3	17,3	17,8
Aantal omwisselingen buiten de EU/EVA	5,8	5,9	6,6	7,3	8,3	9,2	11,4
Aantal departementale uitgiften van rijbewijzen	4,5	4,0	4,1	4,1	5,1	7,4	8,2

Bron: RDW, 2019

TABEL 59: Verlies, diefstal, vervalsingen

	2012	2013	2014	2015	2016	2017	2018
Aantal verlies / diefstal (x 1.000)	10,2	10,1	10,2	10,7	11,0	11,3	11,7
Valse/vervalste rijbewijzen						54	57

Bron: RDW, 2019

4.3 Logius

Logius is onderdeel van het Ministerie van Binnenlandse Zaken en faciliteert rijksbreed de ontwikkeling van digitale diensten. Zelf omschrijft zij haar dienstverlening als ‘het verbinden van overheid, burgers en bedrijven’. Belangrijke diensten betreffen het beheer van DigiD, MijnOverheid en Digipoort. In het kader van de monitor identiteit zijn

vooral de activiteiten met betrekking tot DigiD relevant. Ontwikkelingen daarover worden al enige jaren gevolgd door ICTU (in opdracht van het Ministerie van Binnenlandse Zaken) met de Monitor Generieke Digitale Infrastructuur.

TABEL 60: DigiD accounts (x 1.000.000)

	2013	2014	2015	2016	2017	2018	2019	2021 ¹¹
Aantal actieve DigiD's	11,0	11,8	12,7	13,5	13,5	13,8	15,0	16,8

Bron: Monitor Generieke Digitale Infrastructuur, 2018 & Monitor Digitale Overheid, 2021

TABEL 61: Aantal op DigiD aangesloten organisaties

	2014	2015	2016	2017	2018	2019	2020
Totaal aantal aangesloten organisaties	526	551	570	623	647	663	701
Totaal aangesloten webdiensten		717	771	871	945	1023	1124

Bron: Monitor Generieke Digitale Infrastructuur, 2018 & Monitor Digitale Overheid, 2021

¹¹ Cijfers over 2020 zijn niet beschikbaar

TABEL 62: Gebruik DigiD (x 1.000.000)

	2013	2014	2015	2016	2017	2018	2019	2020	2021 ¹²
Totaal aantal authenticaties	117,0	158,3	206,0	258,5	280,2	308,0	340,8	402,5	557
Aantal authenticaties op beveiligingsniveau			184,8	231,3	251,5	260,1	223,9	161,2	121,5
Aantal authenticaties op midden			21,2	27,1	28,7	36,8	64,6	99,6	149,3
Aantal authenticaties op midden (app)					2,6	10,9	46,8	95,6	132
Aantal authenticaties op substantieel (app)					0,01	0,2	5,4	46,1	153,6

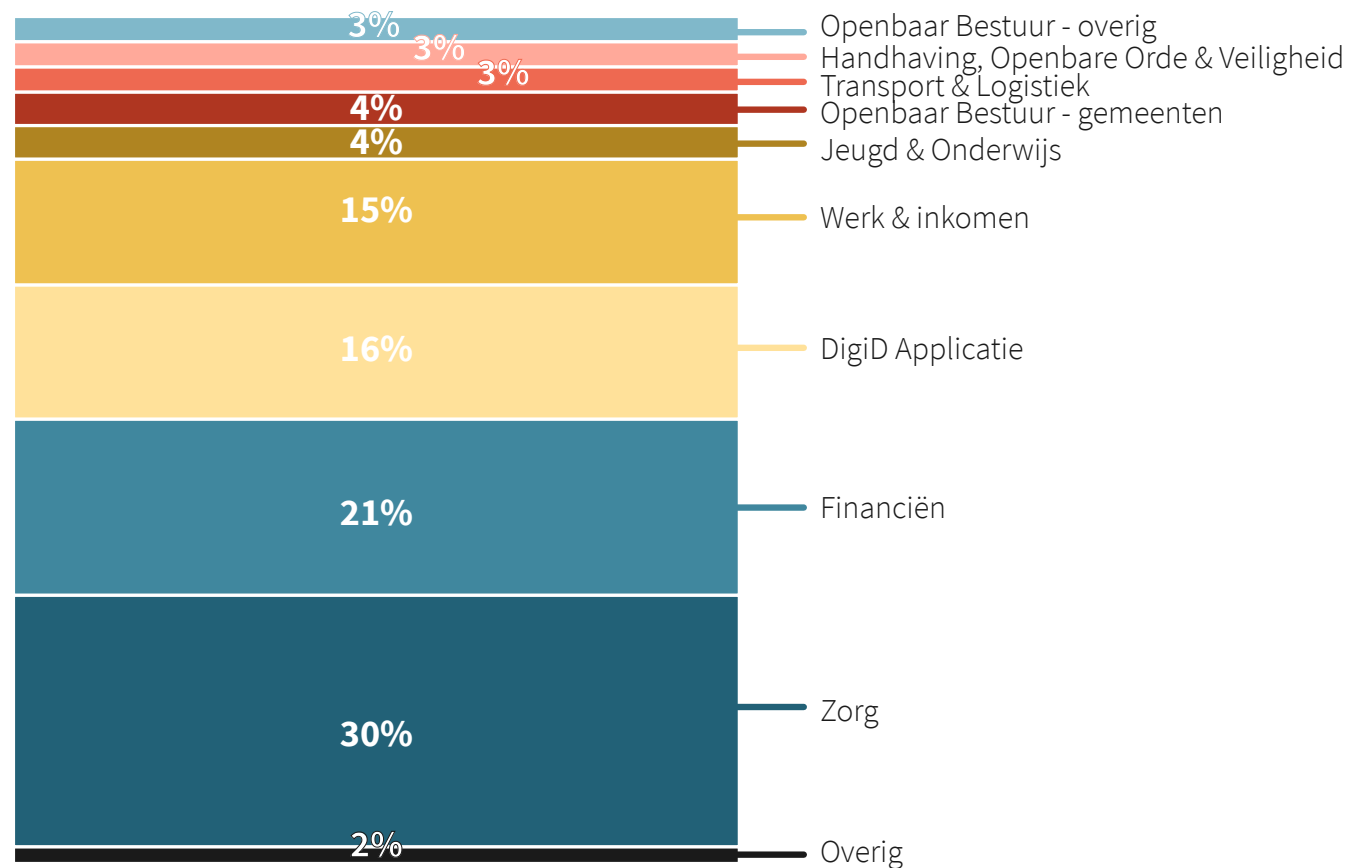
Bron: Monitor Generieke Digitale Infrastructuur, 2018 & Monitor Digitale Overheid, 2021

Het gebruik van DigiD neemt jaarlijks toe. Afgelopen jaar was er sprake van een sprong. Deze sprong komt vooral op het conto van GGD-GHOR.

In 2021 vonden er 92,5 miljoen authenticaties plaats ten behoeve van het laten testen op het coronavirus.

¹² Schatting op basis van cijfers van Logius over de periode januari-september 2021

Figuur 5: Aantal DigiD-authenticaties per branche



Bron: Logius, maandrapportage DigiD Burger 2021 (periode januari- september 2021)

Sinds 2018 is de Europese eIDAS-verordening van kracht. Sindsdien moeten publieke organisaties en private organisaties met een publieke taak Europees erkende inlogmiddelen accepteren binnen hun digitale dienstverlening. Het afgelopen jaar (2021) werd er naar schatting bijna

93.000 keer door andere dan Nederlandse EU-burgers ingelogd bij Nederlandse organisaties met zo'n Europees inlogmiddel. Het betroffen met name Belgische burgers. Het vaakst werd met eIDAS ingelogd bij de Belastingdienst.

TABEL 63: Gebruik eIDAS in Nederland door burgers uit diverse EU-lidstaten

Lidstaat	totaal periode jan - aug 2021	schatting heel 2021
Duitsland	4.983	7.475
Estland	1.375	2.063
Spanje	359	539
Kroatië	108	162
België	49.167	73.751
Luxemburg	1	2
Italië	2.793	4.190
Portugal	1.803	2.705
Litouwen	754	1.131
Slowakije	338	507
Letland	16	24
Tsjechië	67	101
Totaal	61.764	92.646

Bron: Logius

TABEL 64: Gebruik eIDAS door burgers uit andere EU-lidstaten

	periode jan – aug 2021	Schatting heel 2021 ¹³
Belastingdienst	19.709	29.564
Sociale Verzekeringsbank	10.918	16.377
UWV	6.523	9.785
Stichting Pensioenregister	5.674	8.511
Dienst Uitvoering Onderwijs	3.964	5.946
Onderlinge Waarborgmaatschappij CZ groep U.A.	2.481	3.722
Stichting Pensioenfonds ABP	1.806	2.709
CJIB	1.634	2.451
CZ Groep Zorgverzekeraar	1.110	1.665
Stichting Pensioenfonds van de Metalektro (PME)	848	1.272

Bron: Logius

¹³ Schatting op basis gegevens Logius over de periode januari – augustus 2021.

4.4 Fraudehelpdesk

Sinds 2011 bestaat de Fraudehelpdesk. Fraudehelpdesk is een privaat initiatief dat financieel wordt ondersteund door het ministerie van Justitie en Veiligheid. De organisatie is een loket voor particulieren en bedrijven die slachtoffer zijn geworden van fraude. Daarnaast houdt zij zich bezig met publieksvoorlichting en advisering aan onder meer het ministerie van Justitie. De vormen van fraude ten aanzien waarvan Fraudehelpdesk hulp biedt en adviseert, zijn divers en lopen uiteen van hacking, acquisitiefraude tot aan datingfraude. In totaal ontving zij in 2020 ongeveer 350.000 meldingen. Ten behoeve van voorliggende monitor heeft Fraudehelpdesk gegevens verstrekt over aantallen meldingen van identiteitsfraude.

TABEL 65: **Schade per fraudevorm (Euros)**

	2017	2018	2019	2020
Cybercrime	941.025	862.223	1.482.523	1.352.900
Identiteitsfraude natuurlijke personen	57.707	363.373	1.439.957	6.484.982
Marktplaats/webwinkel fraude	595.701	370.670	479.941	734.269

Bron: Fraudehelpdesk 2021

Fraudehelpdesk registreerde in 2020 heel veel meer gevallen van identiteitsfraude. Deze zeer sterke toename komt voornamelijk door de sterke opkomst van Whatsapp-hulpvraagfraude. Fraudehelpdesk kreeg hier ruim 12 duizend meldingen van binnen.

TABEL 66: **Vormen van aan identiteit gerelateerde fraude geregistreerd door Fraudehelpdesk (aantal meldingen)**

	2017	2018	2019	2020
Acquisitiefraude	3.587	3.245	1.886	1.514
Card fraude	27	37	31	52
Cyber crime	6.360	6.253	14.237	8.982
Flessentrekkerij	25	16	11	0
Identiteitsfraude natuurlijke personen¹⁴	443	1.024	2.672	12.602
Identiteitsfraude rechtspersonen	586	662	908	1.985
Marktplaats/webwinkel fraude	1.909	1.454	2.371	4.827

Bron: Fraudehelpdesk, 2021

¹⁴ Stijging in 2020 is voornamelijk het gevolg van een zeer sterke toename van valse Whatsapp hulpvragen (zie ook tabel...).

TABEL 67: Meldingen die specifiek betrekking hebben op
Whatsapp-hulpvraagfraude

	2020
Aantal meldingen	12.133
Slachtoffers	1.340
Totaal schadebedrag 2020	€ 3.863056

Bron: Fraudehelpdesk, 2021

TABEL 68: Vormen van aan identiteit gerelateerde fraude
geregistreerd door Fraudehelpdesk (aantal slachtoffers)

	2017	2018	2019	2020
Acquisitiefraude	132	129	99	67
Card fraude	15	26	16	31
Cyber crime	344	416	922	668
Flessentrekkerij	11	9	4	0
Identiteitsfraude natuurlijke personen	53	156	387	1.390
Identiteitsfraude rechtspersonen	149	152	129	347
Marktplaats/ webwinkel fraude	1.277	987	1.570	3.782

Bron: Fraudehelpdesk, 2021

4.5 Centraal Bureau voor de Statistiek

Sinds 2005 voert CBS periodiek onderzoek uit naar slachtofferschap van diverse vormen van criminaliteit. Zij doet dat met een grootschalige enquête. Sinds 2012 kijkt zij daarbij ook naar identiteitsfraude.

Identiteitsfraude wordt door CBS opgevat als een vorm van digitale criminaliteit die gepleegd wordt ten behoeve van financieel gewin. Een nadere beschouwing leert dat CBS drie vormen van fraude onder het

begrip schaaft: skimming, phishing en pharming. Voor deze drie vormen wordt over de periode 2012-2019 een daling gemeten van 1,5% in 2012 tot 0,5% in 2019. Deze daling hangt vooral samen met de daling van skimming. Door de jaren heen slagen banken er steeds beter in deze vorm van criminaliteit te beteugelen.

	2012	2013	2014	2015	2016	2017	2019
Identiteitsfraude totaal	1,5%	1,3%	0,8%	0,6%	0,4%	0,4%	0,5%
Skimming	1,1%	0,8%	0,4%	0,2%	0,1%	0,1%	0,1%
Pharming/Phishing	0,4%	0,4%	0,4%	0,3%	0,3%	0,3%	0,4%

Bron: Veiligheidsmonitor 2019, CBS

Ten opzichte van de definitie van identiteitsfraude die in voorliggende monitor identiteit wordt gehanteerd, is de definitie van CBS een enge. Zo worden cyberpesten, hacking en koop-/verkoopfraude waarbij iemands identiteitsgegevens zijn misbruikt er buiten gehouden. CBS kijkt wel naar deze vormen van fraude maar schaaft dat niet onder identiteitsfraude.

Met betrekking tot cyberpesten mat CBS tot en met 2017 een stabiel slachtofferpercentage van iets meer dan 3%. Ook voor hacking is het slachtofferpercentage vrij stabiel in vergelijking met de sterk toegenomen digitalisering. Alleen voor koop- en verkoopfraude wordt een duidelijke stijging gemeten.

TABEL 70: Vormen van digitale criminaliteit waarbij ook sprake kan zijn van misbruik van persoonsgegevens

	2012	2013	2014	2015	2016	2017	2019
Koop- en verkoopfraude	2,9%	3,3%	3,5%	3,5%	3,4%	3,9%	4,6%
Hacken totaal	6,2%	5,2%	5,1%	4,9%	4,9%	5,5%	6%
- Ingebroken op computer	1%	1%	0,7%	0,7%	0,7%	0,6%	0,5%
- Ingebroken op e-mailaccount	2,7%	2,4%	2,1%	1,8%	1,5%	1,5%	1,7%
- Ingebroken op website	1,4%	1,7%	1,4%	1,6%	1,7%	1,7%	2,2%
- Anders	2,2%	1,6%	1,3%	1,3%	1,3%	1,4%	1,4%
Cyberpesten	3,3%	3,1%	3,2%	3,2%	3,1%	4,2%	3,1%
- Laster	1%	1,1%	0,9%	1%	1%	1%	1%
- Chantage	0,3%	0,2%	0,2%	0,3%	0,3%	0,3%	1%
- Stalken	0,7%	0,7%	0,7%	0,8%	0,8%	0,8%	0,8%
- Bedreiging met geweld	0,6%	0,6%	0,6%	0,5%	0,6%	0,6%	0,6%
- Anders	1,1%	1,2%	1,1%	1,1%	1,1%	1,1%	1,3%

Bron: Veiligheidsmonitor 2019, CBS

TABEL 71: leeftijd slachtoffers van digitale criminaliteit

	% internetgebruikers (12 jaar of ouder)
Totaal	8,5%
12 tot 18 jaar	12%
18 tot 25 jaar	12,7%
25 tot 35 jaar	11,1%
35 tot 45 jaar	9,8%
45 tot 55 jaar	9,3%
55 tot 65 jaar	5,4%
65 tot 75 jaar	3,9%
75 jaar of ouder	3,3%

Bron: Veiligheidsmonitor 2019, CBS

4.6 Koninklijke Marechaussee, ECID

Het Expertisecentrum Identiteitsfraude & Documenten (ECID) is een landelijk aanspreekpunt voor (vermoedens) van identiteitsfraude. ECID is onderdeel van de Koninklijke Marechaussee en bedient naast de eigen organisatie ook andere publieke en private instanties met vragen over identiteit en identiteitsdocumenten. Zij ondersteunt onder andere

politie, bedrijven, belastingdienst, gemeenten, en IND. ECID rapporteert jaarlijks over haar bevindingen in een statistisch jaaroverzicht. Zij maakt daarbij onderscheid tussen fraude die zij constateerde aan de grens en gevallen van fraude die via andere partijen bij de helpdesk zijn binnengekomen.

TABEL 72: Aantal zaken met betrekking tot identiteits- en documentfraude gemeld bij ECID

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Aantal zaken identiteits- en/of documentfraude aangetroffen op de Nederlandse grenzen	1034	979	1015	841	868	1053	989	883	947	950	1036	878
Aantal documenten waarmee identiteits- en/of documentfraude werd gepleegd op de Nederlandse grenzen.	1392	1308	1394	1172	1163	1567	1446	1256	1435	1436	1487	
Aantal zaken identiteits- en/of documentfraude in het Nederlandse binnenland (aangedragen bij ID-Desken)	995	702	811	745	722	904	870	919	1048	1260	1135	939

Bron: Expertisecentrum Identiteitsfraude en documenten (ECID), KMar, 2020

Van de 1.036 fraudezaken die voorkwamen uit controles van de KMar aan de grens, heeft driekwart (76%) betrekking op passagiers die door de lucht reisden.

TABEL 73: Aantal zaken met betrekking tot identiteitsfraude naar segment

	2019	2020
Segment lucht	792	600
Segment land	171	234
Segment maritiem	73	44
Totaal	1.036	878

Bron: Expertisecentrum Identiteitsfraude en documenten (ECID), KMar, 2021

Naast de zaken die voortkomen uit controles aan de landsgrenzen worden jaarlijks door uiteenlopende partijen zaken bij ECID aangedragen. Onder andere van de politie, financiële instelling en gemeenten.

TABEL 74: Aantal zaken identiteits- en documentfraude binnenland, naar meldende instantie

	2017	2018	2019	2020 ¹⁵
Nationale Politie	399	425	514	440
KMar	231	277	182	82
Financiële instellingen	42	66	55	
Gemeenten	33	44	50	
Fraudehelpdesk¹⁶	-	-	34	
Anders (o.a. IND, Ned. Spoorwegen, KvK, FIOD)	343	448	300	
Totaal	1048	1260	1135	939

Bron: Bron: Expertisecentrum Identiteitsfraude en documenten (ECID), KMar, 2021

¹⁵ Over 2020 wordt niet afzonderlijk gerapporteerd over het aantal zaken dat is aangedragen door andere partijen dan Nationale Politie en KMar.

¹⁶ Over de jaren 2017 en 2018 is niet afzonderlijk gerapporteerd over het aantal meldingen dat via Fraudehelpdesk binnenkwam.

Bijlage 1: Onderzoeksverantwoording

De resultaten die zijn gegeven in hoofdstuk 2 en 3 hebben betrekking op dat deel van de bevolking dat ouder is dan 16 en jonger dan 80 jaar. De resultaten van hoofdstuk 2 zijn gebaseerd op een enquête die online is uitgevoerd onder 2.471 mensen die deelnemen aan het panel van veldwerkbureau IPSOS. Dit panel wordt voortdurend gecontroleerd op representativiteit, onder andere op basis van leeftijd, geslacht en opleidingsniveau.

	(n=2.471)	(n=13.557.100)	
GESLACHT (16-80 jaar)	steekproef	populatie	verschil
Man	46,6%	49,8%	3,2%
Vrouw	53,4%	50,2%	-3,2%

Bron: enquête onder bevolking

	(n=2.473)	(n=13.557.100)	
LEEFTIJD (16-80 jaar)	steekproef	populatie	verschil
16 tot 20 jaar	2,8%	6,2%	-3,4%
20 tot 30 jaar	10,8%	16,2%	-5,4%
30 tot 40 jaar	18,0%	15,6%	2,4%
40 tot 50 jaar	16,6%	16,1%	0,5%
50 tot 60 jaar	21,4%	18,5%	2,9%
60 tot 70 jaar	20,5%	15,4%	5,1%
70 t/m 80 jaar	9,9%	12,1%	-2,2%

Bron: enquête onder bevolking

	(n=2.473)	(n=13.557.100)	
Hoogste opleiding die is afgemaakt (16-80).	steekproef	populatie	verschil
Geen onderwijs / basisonderwijs	0,4%	8,2%	-7,8%
LBO / VBO / VMBO (kader- of beroepsgericht) / MBO1	9,5%	12,1%	-2,6%
MAVO / HAVO of VWO (overgegaan naar 4e klas) / (M)ULO / VMBO (theoretische of gemengd) / voortgezet speciaal onderwijs	11,4%	7,4%	4,0%
MBO 2, 3, 4 of MBO voor 1998	35,3%	32,6%	2,7%
HAVO of VWO (met diploma afgerond) / HBS / MMS	9,9%	9,3%	0,6%
HBO of universitair propedeuse / HBO of universitair bachelor/kandidaats	21,5%	19,6%	1,9%
HBO of universitair master/doctoraal/postdoctoraal	12,1%	10,9%	1,2%

Bron: enquête onder bevolking

Ten aanzien van de representativiteit van het geraadpleegde panel gelden twee belangrijke beperkingen.

- In de eerste plaats zijn Nederlanders met beperkte digivaardigheid en/of een beperkt computer-/internetgebruik niet in het panel vertegenwoordigd
- Verder is er een ondervertegenwoordiging van mensen die de Nederlandse taal niet of beperkt machtig zijn.

Bijlage 2: In welke situaties identificeren mensen zich op welke manier?

	% van alle ondervraagden dat aangeeft dit gedaan te hebben in de afgelopen 12 maanden	% dat zich daarbij heeft geïdentificeerd	% dat aangeeft daarbij een kopie te hebben overhandigd of opgestuurd	% dat zich daarbij online/per mail identificeerde	meest gebruikte ID middel
Werk en opleiding					
een nieuwe werkgever gekregen	12%	83%	91%	37%	paspoort
ingeschreven bij een uitzendbureau	3%	61%	81%	51%	NIK
bezoek gebracht aan het UWV	4%	56%	38%	nvt	NIK
ingeschreven voor een opleiding	5%	59%	65%	71%	DigiD
Financiën					
een bankrekening geopend	9%	74%	69%	71%	paspoort
een hypotheek, lening, krediet of credit card afgesloten	7%	85%	82%	55%	paspoort
beleggingsrekening geopend	5%	72%	82%	90%	paspoort
een nieuwe/andere zorgverzekering afgesloten	5%	54%	38%	83%	DigiD
zaken geregeld bij de notaris	4%	94%	60%	gg	paspoort
cryptovaluta aangeschaft	8%	87%	81%	gg	paspoort
Gezondheid					
laten testen op Covid 19	50%	100%		nvt	NIK
laten vaccineren tegen Covid	76%	100%		nvt	NIK
Corona check app of het papieren bewijs gebruikt	76%	50%		nvt	rijbewijs
geregistreerd bij een ziekenhuis/zorginstelling/ dokter/ therapeut	25%	70%	13%	18%	rijbewijs
geregistreerd bij een vereniging/sportschool	6%	35%	24%	10%	rijbewijs
Wonen					
verhuisd naar een andere huurwoning	6%	74%	61%	43%	NIK
gebruik gemaakt van een makelaar	5%	60%	56%	30%	PASPOORT
Kopen en verkopen					
telefoonabonnement afgesloten	14%	52%	52%	74%	NIK
iets gekocht of verkocht op een online marktplaats	30%	8%	19%	36%	NIK
pakje in ontvangst genomen bij een afhaalpunt/postkantoor	47%	74%		nvt	rijbewijs
aangetekende brief ontvangen	5%	59%		nvt	NIK
alcohol of sigaretten gekocht (lft < 26)	22%	90%		10%	NIK
telefoonabonnement afgesloten	19%	62%	61%	37%	NIK
Reis en verblijf					
vliegreis gemaakt	16%	98%		nvt	paspoort
internationale reis per trein, boot of bus gemaakt	4%	64%	20%	nvt	paspoort
in een hotel, pension, camping of particuliere huurwoning overnacht	34%	58%	16%	5%	paspoort
auto gehuurd	6%	81%	42%	15%	rijbewijs
iets anders dan een auto of woning gehuurd, zoals gereedschap	3%	43%	42%	15%	rijbewijs
Zaken met de overheid					
Gestemd bij de laatste Tweede Kamer verkiezingen	68%	100%		nvt	NIK
een geboorte, overlijden of voorgenomen huwelijk aangegeven	4%	100%		gg	paspoort
een identiteitsbewijs aangevraagd	11%	100%		gg	
bezoek gebracht aan het Juridisch Loket	2%	50%	55%	nvt	NIK (en DigiD want vereist)
een subsidie, vergunning of ontheffing aangevraagd	4%	75%	41%	87%	DigiD
ingeschreven bij de Kamer van Koophandel	3%	100%	68%	nvt	paspoort (en DigiD want vereist)
aangifte gedaan bij de politie	5%	55%	15%	65%	NIK / DigiD
aangehouden door de politie of een BOA	1%	74%	20%	nvt	NIK
ongeval/ aanrijding in het verkeer gehad	2%	58%	7%	nvt	rijbewijs
betrokken geweest bij een rechtszaak	1%	59%	32%	gg	paspoort / NIK
bezoek gebracht aan een overheidsinstelling	5%	64%		nvt	NIK

Colofon

De Monitor Identiteit wordt uitgevoerd in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Auteurs:

Guido Brummelkamp, Ruud Hoevenagel, Auke Witkamp,
Marierose Heineken-van Dooren (IPSOS)

Maart 2022

Grafisch ontwerp: [Streeff.nl](https://streeff.nl)

Fotografie:

Intro:	Cristina Zaragoza
Inleiding:	CardMapr
Bezit & gebruik / Fraude & Misbruik:	Streeff.nl
Kengetallen:	Mediatheek Rijksoverheid (bewerking Streeff.nl)
Deze pagina:	David Dvořáček

Brummelkamp
beleidsonderzoek

