MCF 17/12

Ministerie van Financiën

T.B.V. MINISTERIËLE COMMISSIE FRAUDE, D.D. 17 DECEMBER 2013
Aan

De Minister
De Staatssecretaris

Directoraat-Generaal
Belastingdienst

Inlichtingen
[redacted]
T [redacted]
[redacted]@minfin.nl

Datum
13 december 2013

Notitienummer
DGB/2013/6778

Rubriek

Auteur
[redacted]

Van
Cluster Uitvoeringsb[redacted]

Kopie aan
Minister
PA's

Bijlagen

13
2

notitie

Voorbereidingsdossier Ministeriële Commissie aanpak fraude

Paraaf de Minister [redacted]

Paraaf de Staatssecretaris [redacted]

Paraaf [redacted]

Aanleiding

U (Minister) neemt deel aan de Ministeriële Commissie aanpak fraude. Deze Commissie voert de politieke regie op het tot stand brengen van een versterkte duurzaam geborgde rijksbrede fraudeaanpak. Dinsdag 17 december is de vierde bijeenkomst van de Commissie. Onderstaand treft u een korte toelichting en adviezen aan met betrekking tot de agendapunten.

Toelichting per agendapunt

Agendapunt 2.
Rijksbrede aanpak van fraude (Brief van de minister van Veiligheid en Justitie d.d. 9 december, nr. 432544)

Advies

- U kunt instemmen met verzending van de brief met betrekking tot de rijksbrede aanpak van fraude naar de Kamer.
- U kunt een opmerking maken over het verschoningsrecht. In de brief wordt dit primair overgelaten aan de beroepsgroepen zelf. U kunt voorstellen dat ook VenJ eigen onderzoek gaat doen hoe om te gaan met dit spanningsveld.
- Een tweetal tekstuele aanpassingen met betrekking tot het onderdeel afpakken (VenJ) en Adresfraude (BZK) worden nog ambtelijk afgestemd voor de MC vergadering. Deze tekstblokken worden tijdens de MC uitgereikt.
- U kunt aangeven dat u nog enkele tekstuele opmerkingen heeft. Deze zullen ambtelijk worden aangeleverd.

Toelichting:

- Op bladzijde 8, 2e alinea wordt ingegaan op het verschoningsrecht. Het spanningsveld tussen geheimhoudingsplicht/verschoningsrecht en

adequate opsporing en vervolging is goed verwoord. Alleen stellen wij voor dat de overheid dit niet alleen overlaat aan de beroepsgroepen zelf maar daar ook een eigen standpunt over inneemt. Uiteraard in goed overleg met de betrokken beroepsgroepen. Het verschoningsrecht ziet naast notarissen en advocaten ook op fiscaal adviseurs.
Toevoegen als tekst: Daarnaast zal ik eigen onderzoek doen, uiteraard in overleg met de beroepsgroepen, naar de gewenste balans tussen het hiervoor benoemde spanningsveld en zo nodig met voorstellen komen.

Agendapunt 3.
Brief kabinetsvisie aanpak identiteitsfraude - 'Slim voorkomen, vlot herstellen', met als bijlage het rapport 'Identiteit in cijfers' (Brief van de minister van Binnenlandse Zaken en Koninkrijksrelaties, 2013-[redacted])xxxxxxxx

Advies

- U kunt instemmen met verzending van de kabinetsvisie identiteitsfraude naar de Kamer.
- U kunt aangeven dat op pagina 7 2e alinea "te vormen" kan worden verwijderd voor de expertisegroep fraudebestrijding. BZK is met deze aanpassing akkoord. Inmiddels is ook de fysieke locatie voor deze groep in Utrecht beschikbaar en wordt op korte termijn betrokken. Dit is een verdere stap in de goede richting.

Toelichting

- De Kabinetsvisie beschrijft een kader waarbinnen de aanpak identiteitsfraude dit kabinetsperiode verder wordt vormgegeven. Concrete maatregelen volgen begin 2014 in een actieprogramma.
- Op ons aandringen heeft BZK interdepartementaal commitment afgestemd om ongedekte financiële consequenties volgend uit de Kabinetsvisie te voorkomen, het commitment is tweeledig:
    1. Het staand beleid op het terrein van de identiteitsfraude is volledig gedekt en departementen zullen voor de nieuwe maatregelen meewerken aan een businesscase. De businesscases worden vanaf januari 2014 uitgevoerd.
    2. Omdat de financiële consequenties van de aanvullende/nieuwe maatregelen in deze fase nog niet in detail in kaart kunnen worden gebracht, is in de Kabinetsvisie een disclaimer opgenomen: *"Wanneer vanuit de visie nieuwe maatregelen voortvloeien waarvoor nog geen middelen zijn voorzien in de begroting(en), worden business cases opgesteld. De business cases worden getoetst voordat besloten wordt of de maatregelen worden getroffen."*

MCF
pt. 2
+
3

MINISTERRAAD/ONDERRAAD

Met eventuele gecoördineerde opmerkingen uiterlijk retour:

Vrij dag 13/12 vóór 15.00 uur

X			BFB		BJZ		DGFZ	CC	
			FM		AFEP				
			FIN						

Ontvangen d.d.: 11-12-2013

Behandelende afd./bureau: VJFA

Behandelend medewerker:

Medeparaaf:

Geen opmerkingen ☐

Zie bijgevoegde nota*) X

No 6770 Uitvoeringsbeleid

*) Nota met kopieën aanleveren bij

Nota voor RMR/MR óók in WORD-versie via de mail aanleveren.

behandelend medewerker	datum	paraaf
	13/12	
	13/12	

11/12 VJFA

MCF

Handtekening bewindspersoon

Minister van Veiligheid en Justitie

Rijksoverheid

voor MCF

Aanbieding

Van 1 *	Minister van Veiligheid en Justitie
Type voorstel *	Brief aan de Tweede Kamer

Titel en inhoud

Korte titel *	Rijksbrede aanpak van fraude
Inhoud en doelstelling van het voorstel *	Conform eerdere besluitvorming in de MC wordt voor het einde van het jaar een actieplan in de vorm van een brief naar de Kamer gezonden. Aan u wordt voorgesteld om in te stemmen met voorliggend eindconcept. De brief bevat de volgende hoofdlijnen: 1. Fraudebestendige regelgeving 2. Goed functionerende basisregistraties en een verbeterde informatiepositie 3. De bestrijding van faciliterende fraudefenomenen 4. Een gerichte aanpak van fraudeurs. Na de bespreking van het stuk in de MC van 12 november is de brief over de hele linie aangescherpt. Meest fundamenteel is dat de toon aan het begin van de brief is aangepast, zodat duidelijk is dat de burger in beginsel het vertrouwen van de overheid verdient, maar er proportioneel moet worden opgetreden als dit vertrouwen wordt beschaamd.
Voorgesteld besluit *	Het voorstel te aanvaarden.

Behandeltraject

Datum aanbieding *	9 december 2013
Kenmerk *	
Hamerstuk *	☐ Ja ☒ Nee
Voorgaande behandeling *	☒ Ja ☐ Nee
Behandeld door *	Rijksbrede Fraudebestrijding
Datum voorgaande behandeling *	27-nov-2013

Gevolgen en juridisch kader

Gevolgen rijksbegroting *	☐ Ja ☒ Nee
Gevolgen voor regeldruk *	☐ Ja ☒ Nee
Overeenstemming met V&J inzake wetgevingstoets en effectenanalyse *	☐ Ja ☐ Nee, met bijlage ☐ Nee, zonder bijlage ☒ N.v.t.
Aan EU Notificatie voldaan *	☐ Ja ☐ Nee ☒ N.v.t.
Verplichting Int. verdragen en/of Europese regelgeving*	☐ Ja ☒ Nee

Formulier nummer 20130821-01

Interdepartementale afstemming

Overeenstemming BZK inzake beoordelingskader financiele/ bestuurlijke consequenties decentrale overheden en/of Caribisch Nederland *	☐ Ja	☐ Nee	☒ N.v.t.					
Overeenstemming Aruba, Curaçao en Sint Maarten *	☐ Ja	☐ Nee	☒ N.v.t.					
Ambtelijk afgestemd *	☒ Ja	☐ Nee	in	DG-overleg rijksbrede fraudebestrijding				
Overeenstemming bereikt op ambtelijk niveau *	☒ Ja	☐ Nee	☐ N.v.t.					
Overeenstemming bereikt met	☒ AZ	☒ BZK	☒ EZ	☐ I&M	☒ SZW	☐ VWS	☒ W&R	
	☐ BZ	☐ Def	☒ Fin	☒ OCW	☒ V&J	☐ BH&OS		

Omschrijving geschilpunten

Contactpersonen

	Contactpersoon 1	Contactpersoon 2
Naam *		
Afdeling *	DRC/Fraude en ordening	DVB/Bestuurlijke aanpak
Telefoonnummer *		
E-mailadres *	@minvenj.nl	@minvenj.nl

Ministerie van Veiligheid en Justitie

> Retouradres Postbus 20301 2500 EH Den Haag

Aan [redacted] van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Directoraat-Generaal Rechtspleging en Rechtshandhaving
Directie Rechtshandhaving en Criminaliteitsbestrijding
DRC

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/venj

Contactpersoon
[redacted]

T 07[redacted]
F 07[redacted]

Ons kenmerk
[redacted]

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 9 december 2013
Onderwerp Rijksbrede aanpak van fraude

Inleiding
In mijn brief van 3 juli jl.[1] heb ik aangekondigd dat het kabinet in het najaar een actieplan zou presenteren met aanvullende maatregelen ter versterking van de aanpak van fraude met publieke middelen. Mede namens de minister van Sociale Zaken en Werkgelegenheid, de minister van Economische Zaken, de minister van Volksgezondheid, Welzijn en Sport, de minister van Binnenlandse Zaken en Koninkrijksrelaties, de minister voor Wonen en Rijksdienst, de minister van Onderwijs, Cultuur en Wetenschap en de staatssecretaris van Financiën, doe ik die toezegging met deze brief gestand.

Naar een nieuwe balans tussen vertrouwen, dienstverlening en fraudebestrijding
Het afgelopen jaar is in de diverse debatten over fraude met overheidsvoorzieningen aan de orde gekomen dat bij het toekennen van toeslagen en andere inkomensvoorzieningen aan burgers, het opereren op basis van vertrouwen en goede dienstverlening belangrijke uitgangspunten zijn. Tegelijkertijd is gebleken dat een handhavingsstrategie die daar te veel op gebaseerd is, niet altijd voldoende is ingericht om fraudeurs te kunnen weren. Dit levert een zekere spanning op tussen enerzijds de ambitie om als een dienstverlenende overheid op te treden en daarbij uit te gaan van vertrouwen, en anderzijds de noodzaak om scherper in te zetten op maatregelen tegen fraude. Het kabinet presenteert vandaag een pakket maatregelen, waarbij het oog heeft voor een goede balans tussen gerechtvaardigd vertrouwen, goede dienstverlening en fraudebestrijding. Daarbij is het de inzet van het kabinet niet alleen om fraudeurs aan te pakken, maar ook om zo veel mogelijk te voorkomen dat goedwillenden lijden onder de kwaadwillenden. Het beginsel van proportionaliteit in de reactie van de overheid op fraude of misbruik is hierbij cruciaal.

Fraude is niet acceptabel
De effecten van fraude met publieke middelen reiken verder dan alleen de directe financiële schade voor de overheid. Fraude ondermijnt de integriteit van het economisch stelsel, het vertrouwen in de financiële instellingen, tast de

[1] Kamerstukken II 2012/13, 29 911, nr. 82

betaalbaarheid van voorzieningen aan en kan leiden tot een vermindering van het maatschappelijke draagvlak voor sociale voorzieningen en tot aantasting van het rechtsgevoel. Zowel de overheid als burgers en ondernemingen zijn hierbij slachtoffer. Fraudeurs zoeken continu naar zwakke plekken in regelingen of systemen om daarmee financieel of economisch voordeel te behalen. Dit kabinet wil fraude zoveel mogelijk voorkomen en waar fraude ondanks alle maatregelen toch nog heeft plaatsgevonden, zo effectief mogelijk bestrijden. Dat vraagt om een brede en integrale benadering waarbij de rijksoverheid ook zal samenwerken met gemeenten en private partijen, zoals banken en curatoren. Hierbij wordt uiteraard gebruik gemaakt van goede ideeën uit de praktijk en ervaringen op lokaal niveau, waaronder die van het Amsterdamse burgerinitiatief tegen fraude, 'Een Overheid'. Bij de nadere uitwerking van de versterkte aanpak van fraude oriënteert het kabinet zich daarnaast op goede ervaringen in ons omringende landen, zoals België en het Verenigd Koninkrijk.

Definitie en afbakening
Met fraude wordt bedoeld het opzettelijk opgeven van een onjuiste voorstelling van zaken, om hieruit wederrechtelijk voordeel te verkrijgen. In de context van deze brief omvat de rijksbrede fraudeaanpak ook het bredere begrip *misbruik* en het *oneigenlijk gebruik* van regelingen. Van dit laatste is sprake als er niet tegen de letter, maar wel tegen de geest van bepaalde wet- of regelgeving wordt gehandeld. Daarnaast kan er sprake zijn van *vergissingen*, die ook door goedwillende burgers en bedrijven kunnen worden begaan. Het is zaak deze gevallen te detecteren en er op gepaste wijze op te reageren.

De focus van de in deze brief gepresenteerde Rijksbrede aanpak ligt op fraude met publieke middelen. Tegelijkertijd versterkt een groot aantal van de maatregelen tegen deze categorie van fraude ook de aanpak van fraude tegen burgers en bedrijfsleven. De aanpak richt zich immers voor een belangrijk deel op het wegnemen van het instrumentarium van fraudeurs en het weren van beroepsfraudeurs. Deze categorie criminelen maakt geen onderscheid tussen publieke of private gelden.

Rijksbrede anti-fraudestrategie
De recente ervaringen met fraude met diverse regelingen op het gebied van individuele inkomensoverdrachten en subsidies, gecombineerd met het inzicht dat een sluitende aanpak ervan alleen in gezamenlijkheid kan worden gerealiseerd, heeft geleid tot de ontwikkeling van een rijksbrede anti-fraudestrategie. Door middel van risico-analyses is in de afgelopen periode op de belangrijkste beleidsdomeinen van de Rijksoverheid in beeld gebracht welke aanvullende maatregelen nodig zijn. De bijlage bij deze brief bevat een overzicht van de belangrijkste maatregelen die recent *binnen* de specifieke beleidsdomeinen zijn getroffen of binnenkort in gang worden gezet. Het overzicht beperkt zich tot de hoofdlijnen, omdat het een groot aantal maatregelen betreft, waarover uw Kamer veelal al is geïnformeerd.

In aanvulling hierop treft het kabinet een pakket met *domeinoverstijgende* maatregelen. Het gaat hierbij om maatregelen die verschillende overheidsdiensten gezamenlijk moeten nemen, omdat er sprake is van wederzijdse afhankelijkheid. De praktijk laat zien dat deze onmisbaar zijn om te komen tot een sluitende anti-fraudestrategie. De vier hoofdlijnen van deze aanpak licht ik hieronder toe:

1. Fraudebestendige regelgeving

2. Goed functionerende basisregistraties en een verbeterde informatiepositie
3. De bestrijding van faciliterende fraudefenomenen
4. Een gerichte aanpak van fraudeurs.

1. Fraudebestendige regelgeving staat voorop

Het vertrekpunt bij de bestrijding van fraude is het wegnemen van gelegenheden om fraude te kunnen plegen. Dat vergt allereerst dat bij het opstellen en aanpassen van wet- en regelgeving een goede inschatting wordt gemaakt van potentiële zwakke plekken of frauderisico's, zodat deze zoveel mogelijk kunnen worden beperkt. De dynamiek van fraudefenomenen en de vindingrijkheid van beroepsfraudeurs vraagt daarnaast om het voortdurend leren en bijsturen, op basis van actuele kennis van betrokken overheidsdiensten over fraudepatronen, fraudeurs en hun werkwijzen. Binnen de verschillende beleidsdomeinen zijn er al belangrijke stappen gezet en aangekondigd om gebleken frauderisico's weg te nemen, maar het kabinet treft aanvullende maatregelen om wet- en regelgeving structureel en bestendig te blijven toetsen op frauderisico's.

Fraudebestendigheidstoets nieuwe wet- en regelgeving
Sinds 2011 is het kabinetsbeleid dat bij de voorbereiding en toetsing van beleid en regelgeving het zogenaamde Integraal Afwegingskader voor beleid en regelgeving (IAK) structureel wordt toegepast. Hierbij wordt getoetst op alle relevante kwaliteitsaspecten die bij een bepaald voorstel een rol kunnen spelen. Vooralsnog maakt fraudebestendigheid hier niet als zodanig deel van uit. Het IAK zal uiterlijk medio 2014 worden aangescherpt, zodat het meer gericht aandacht besteedt aan de fraudebestendigheid van wet- en regelgeving. Daarbij wordt er gebruik gemaakt van inzichten uit de ontwikkeling van een nieuwe fraudetoets, die momenteel wordt ontwikkeld specifiek voor wet- en regelgeving op het zorgdomein. Deze is door de minister van Volksgezondheid, Welzijn en Sport toegezegd.[2] Het streven is dat de toets eind 2013 gereed is. Doel is dat de beoogde uitvoerders en handhavers tijdig en meer dan voorheen worden betrokken bij het in kaart brengen van de mogelijke frauderisico's.

Producten:
- Ontwikkeling fraudetoets specifiek voor wet- en regelgeving op het zorgdomein (gereed eind 2013)
- Aanscherping Integraal Afwegingskader voor beleid en regelgeving (IAK) op frauderisico's (gereed medio 2014)

Periodieke fouten- en misbruiksignalering
De uitvoering van de regelingen betreffende heffingen, uitkeringen en subsidies is in meerdere of mindere mate gevoelig voor fouten (in de uitvoering of bij de aanvrager/ontvanger) en misbruik (oneigenlijk gebruik of fraude). Daarbij gaat het om uitvoering van regelingen die complex zijn en daarom het risico lopen fout te worden gebruikt, of om regelgeving die niet misbruikbestendig is. Het is noodzakelijk dat bij bestaande regels, en na invoering van nieuwe wet- en regelgeving, bekeken wordt in hoeverre deze feitelijk gevoelig is voor fouten en misbruik.

Hiervoor worden de volgende aanvullende acties voorgesteld:
- Dat zowel bij bestaande wetgeving, als bij de invoering van nieuwe wetgeving die [a] substantiële geldstromen in het financiële verkeer

[2] Kamerstukken II 2012/13, 28 828, nr. 50

tussen rijksoverheid en burger betreft en [b] waarbij wordt getaxeerd is dat er risico's zijn voor fouten- en misbruik, het verantwoordelijke departement daarover periodiek gericht en systematisch signalen uitvraagt. Deze interne en externe signalen, vanuit de uitvoering, maar ook vanuit het domein van de opsporing en toezicht, worden bijeen gebracht en ter beschikking worden gesteld aan de verantwoordelijke minister.

- In het kader van handhavings- en opsporingsactiviteiten stuiten betrokken instanties op situaties die wijzen op een kennelijke kwetsbaarheid voor misbruik. Dat leidt bijvoorbeeld sinds een aantal jaren al tot zgn. *bestuurlijke dossiers* die verstrekt worden aan de politiek-bestuurlijke verantwoordelijke. Zowel de kwaliteit van deze dossiers als het proces van opstellen, verspreiden en opvolgen worden geprofessionaliseerd.

Uiterlijk eind 2014 is binnen alle betrokken ministeries een dergelijke systematiek ingericht. Bovendien wordt in de bedrijfsvoeringsparagraaf van de jaarverslagen van de ministeries over 2013 expliciet aandacht besteed aan de onderkende frauderisico's en de maatregelen die zijn of worden ingezet om deze risico's te beheersen.

2. Basisregistraties en informatiepositie op orde

Uitvoeringsdiensten dienen er op ingericht te zijn om fraude te kunnen signaleren en op te sporen. Het kabinet gaat daarom door met het verbeteren van de beschikbaarheid, juistheid en kennisverspreiding over de inzetbaarheid van de informatie in basisregistraties, zodat beoordelende instanties aanvragen zoveel mogelijk aan de hand van informatie uit een of meerdere basisregistraties kunnen verifiëren en controleren. Vanwege dit gebruik van de basisgegevens in de verschillende ketens en domeinen wordt het steeds essentiëler om bij het ontwerp van wetgeving rekening te houden met het hergebruik van gegevens op verschillende plaatsen in verschillende ketens. Er is daarom blijvende bestuurlijke aandacht voor het oplossen van aan het gebruik van basisgegevens verbonden vraagstukken. Ervaringen uit pilots bieden een goede basis voor de meer structurele oplossingen die de komende jaren gevonden moeten worden.

Bij de uitoefening van het toezicht op regelingen zullen de inzet van risicoprofielen en efficiënte gegevensuitwisseling tussen diensten meer mogelijkheden opleveren om vroegtijdig in te kunnen grijpen bij gevallen van fraude, waarbij vanzelfsprekend de wettelijke kaders ter bescherming van persoonsgegevens gelden De bronhouders van de verschillende basisregistraties hebben steeds meer aandacht voor analyse en signalering om fraude te voorkomen. Zo werken bijvoorbeeld BKWI en Kadaster samen door bij de aanvraag van uitkeringen te controleren welk vastgoed de persoon op naam heeft, en levert het Kadaster gegevens aan Bureau Financieel Toezicht dat integraal toezicht houdt op het notariaat. Ook participeert het Kadaster in een interdepartementale stuurgroep 'aanpak misbruik vastgoed', waarin het zichtbaar maken van 'stromannen' in vastgoedtransacties een speerpunt is. Daarnaast levert de basisregistratie adressen en gebouwen (BAG) waardevolle mogelijkheden bij het uitvoeren van logische controles. Zo gebruiken gemeenten steeds vaker informatie over een woning bij de inschrijving op een adres, waardoor men inzicht heeft in een eventueel disproportionele verhouding tussen het aantal bewoners en de omvang van een pand.

Verbetering kwaliteit Gemeentelijke Basisadministratie (GBA)
De betrouwbaarheid van de gegevens in de GBA is door verbeteracties vanuit gemeenten en uitvoeringsinstanties steeds hoger geworden. De gegevens die niet frequent veranderen –de burgerlijke staat gegevens bijvoorbeeld– zijn nagenoeg 100% betrouwbaar. Voor de gegevens die meer aan verandering onderhevig zijn –de adresgegevens– blijkt uit de laatste meting van april 2013 dat 97,7% van de personen correct staat geregistreerd op een adres.

Het kabinet heeft onlangs 1 miljoen euro extra geld in opleidingen en examens van 1200 gemeentelijke burgerzaken-ambtenaren geïnvesteerd gericht op het bestrijden van fraude. In het kader van ruim 5.000 adresbezoeken zijn risicoprofielen ontwikkeld en actief gedeeld met alle gemeenten. Deze profielen worden thans gebruikt bij nieuwe adresonderzoeken bij gemeenten, ruim 80 gemeenten hebben reeds aangegeven hiermee aan de slag te gaan. Gemeenten hebben inmiddels inzage in gegevens bij het UWV, de zogenaamde Suwi-inkijk, en inmiddels maakten 184 gemeenten daar 19.500 keer gebruik van. Het evaluatie-instrument waarmee gemeenten de inhoudelijke kwaliteit van de GBA en de processen toetsen wordt met de inwerkingtreding van de wet BRP verplicht voor gemeenten; gemeenten moeten daarmee hun wijze van bijhouding van de GBA controleren.

Naast de eigenstandige verbeteracties is er meer samenwerking in de keten van afnemers van de GBA door het inrichten van een centrale monitoringsfunctie. Om verdachte patronen van in- en uitschrijvingen te kunnen herkennen en zijn er risicoprofielen ontwikkeld. Deze laatste worden gebruikt bij 6000 extra huisbezoeken voor adrescontrole door gemeenten. Dat zal ook weer een nieuwe meting van de kwaliteit van de GBA opleveren. Ook zijn gegevens uit de GBA gecombineerd met actief DigiD-gebruik en signalen van mogelijke fraude in de keten. Dat heeft in 6000 gevallen al geleid tot vermoedens van fraude, dat uiteindelijk leidt tot actief afsluiten van DigiD's.

In de Landelijke Stuurgroep Interventieteams (LSI) werken Belastingdienst, Inspectie SZW, UWV, Gemeenten, SVB, Politie en Openbaar Ministerie samen met als doel belasting- en premiefraude, uitkeringsfraude en illegale tewerkstelling aan te pakken.' Adresfraude is één van de thema's waar de LSI in 2014 op in gaat zetten. Het vaststellen van adresfraude kan leiden tot correcties van heffingen van (gemeentelijke) belastingen en van verleende toeslagen, uitkeringen en studiefinanciering. De samenwerking krijgt projectmatig vorm in zogenaamde interventieteams. In interventie-teamverband wordt adresfraude gezamenlijk aangepakt door kennis en informatie met elkaar te delen en samen op te trekken bij daadwerkelijk in te stellen (fysieke) controles.

Per 1 januari 2014 treedt een wijziging van de Wet SUWI in werking waarin wordt geregeld dat het UWV de uitkering opschort van personen met de status Vertrokken Onbekend Waarheen (VOW) in de GBA . Dit zorgt ervoor dat personen zich niet onvindbaar kunnen maken voor de overheid, terwijl ze wel een uitkering van UWV ontvangen. Gemeenten waarvan signalen bestaan dat zij hun processen onvoldoende op orde hebben, zullen door het ministerie van Binnenlandse zaken actief begeleid worden totdat de processen op orde zijn. Het College Bescherming Persoonsgegevens (CBP) is toezichthouder op de gemeenten op de uitvoering van de wet GBA en kan een last onder dwangsom opleggen. Daarnaast zal in 2014 het inzage- en correctierecht van de burger ondersteund worden via MijnOverheid. Getoond zal ook worden welke gegevens over burgers aan welke instanties verstrekt worden.

De campagne 'Voorkom gedoe kijk het na' wijst burgers op het belang van een goede GBA registratie en de gevolgen van niet correcte registratie. Als gevolg van deze campagne hebben 72.052 mensen de landingspagina (www.voorkomgedoe.nl) reeds bezocht. Dat betekent dat er bij deze burgers bewustwording op gang is gekomen m.b.t. het belang van het checken van de GBA gegevens. Gemiddeld 17% van de bezoekers van landingspagina van de campagne klikken door naar mijn.overheid.nl. Inmiddels gebruiken 112 gemeenten de middelen uit de toolkit die is gemaakt om ook vanuit gemeenten burgers te informeren over het belang van een juiste registratie in de GBA. Tot slot komt er met het invoeren van de Wet BRP de mogelijkheid tot het opleggen van een bestuurlijke boete als de burger in gebreke blijft of opzettelijk verkeerde gegevens registreert. Gemeenten worden via een handreiking geadviseerd hoe ze een boete kunnen opleggen. De handreiking beoogt gemeenten enige standaardisatie te bieden in de uitvoering van het sanctiebeleid.

Instelling van een centraal aandeelhoudersregister
Rechtspersonen zijn onmisbaar in het handelsverkeer, maar worden ook gebruikt en misbruikt om illegale activiteiten te verhullen of crimineel vermogen wit te wassen. Dit kan grote maatschappelijke schade veroorzaken. Om hier effectief tegen op te treden moeten toezichthoudende en handhavende instanties kunnen beschikken over zoveel mogelijk relevante informatie. Dit heeft geleid tot het kabinetsbesluit tot de instelling van een centraal aandeelhoudersregister. Dit heeft betrekking op de registratie van aandelen op naam in besloten of niet-beursgenoteerde naamloze vennootschappen. Het register biedt geautoriseerde publieke diensten de mogelijkheid eenvoudig vast te stellen wie de aandeelhouders van een BV zijn en welke aandelen (in welke rechtspersonen) bepaalde personen hebben.

Inrichting van een verwijzingsportaal bankrekeningen
Bij het opsporen van fraude en het afpakken van criminele winsten is het essentieel dat bankgegevens van fraudeurs tijdig, volledig en op een direct verwerkbare digitale wijze bij de politie en de Bijzondere Opsporingsdiensten beschikbaar zijn. Het gaat hier immers om sporen van verdachten in de systemen van banken. Er worden momenteel al stappen gezet in de digitale uitwisseling van financiële informatie tussen banken en opsporingsdiensten. Dat levert aan beide kanten een enorme besparing in tijd en geld op. Wat nog ontbreekt is een verwijzingsportaal waarmee in het kader van het toezicht en de opsporing kan worden nagegaan welke bankrekeningen een persoon op zijn naam heeft staan. Op dit moment moeten bij financiële onderzoeken en rechtshulpverzoeken alle banken aangeschreven worden om na te kunnen gaan bij welke instellingen een persoon bankrekeningen heeft. Een dergelijke faciliteit is ook van belang voor de verificatie door de Belastingdienst bij het koppelen van een BSN aan één bankrekeningnummer. In het voorjaar van 2014 zal op basis van een onderzoek naar de technische aspecten en het juridisch en financieel kader worden besloten over het al dan niet inrichten van het verwijzingsportaal bankrekeningen.

Gegevensuitwisseling
Een belangrijke manier om fraude te voorkomen, ontdekken en bestraffen is het delen van gegevens of indicatoren voor mogelijke fraude die de overheid of andere organisaties beschikbaar hebben. Het is cruciaal om (*realtime*) informatie te kunnen uitwisselen en in te kunnen grijpen. Het delen van gegevens heeft ook een preventieve functie. In veel gevallen kunnen verdachte gegevens worden gesignaleerd en kan een overtreding al 'aan de digitale poort' worden voorkomen.

Dit geldt zowel voor individuele overheidspartijen als voor de gehele keten van instanties. Het is daarom zaak de mogelijkheden van gegevensuitwisseling en daarmee controle vooraf optimaal te benutten.

Er wordt ingezet op verdere verbetering van de mogelijkheden voor gegevensuitwisseling. Hierbij worden twee sporen gevolgd:

- Ten eerste wordt van een viertal casussen (gefingeerde dienstverbanden, faillissementsfraude, identiteitsfraude en notoire fraudeurs/subjectgerichte fraudebestrijding) geïnventariseerd aan welke gegevensuitwisseling behoefte is. Deze inventarisatie is in het voorjaar van 2014 gereed. Op basis daarvan worden waar mogelijk en opportuun belemmeringen weggenomen, zo nodig met wettelijke maatregelen. Daarbij worden ook de *best practices* betrokken die in de vorm van privacyprotocollen en daarmee vergelijkbare arrangementen voor al bestaande vormen van gegevensuitwisseling in bijvoorbeeld samenwerkingsverbanden zijn ontwikkeld.

- Ten tweede wordt voor generieke knelpunten waarvan wordt vastgesteld dat die alleen met wetgeving zijn op te lossen een verkenning uitgevoerd naar een kaderwet voor de gegevensuitwisseling op het bredere terrein van fraudebestrijding, in plaats van de noodzakelijke maar steeds afzonderlijke wijzigingen van specifieke wetten. Deze verkenning is najaar 2014 gereed. Het kan hierbij gaan om zowel toezicht, handhaving als opsporing, inclusief de mogelijkheden om op verkennende wijze fraudepatronen te onderkennen. Daarbij worden ook de opgedane ervaringen betrokken bij wetgeving die op dit punt al tot stand is gekomen, zoals de Wet tot wijziging van de Wet Suwi en andere wetten aangaande gegevensuitwisseling en het effectief gebruik van binnen de overheid bekend zijnde gegevens[3].

Geheimhoudingsplicht en fraudebestrijding

Bij strafrechtelijk onderzoek naar fraude, witwassen en omkoping stuiten opsporingsdiensten geregeld op correspondentie tussen verdachten van strafbare feiten, en advocaten en notarissen. De vraag die zich dan voordoet is of, en zo ja onder welke voorwaarden, deze stukken in beslag kunnen worden genomen. In mijn brief van 8 april 2011[4] is de positie van bijzondere geheimhouders, in het bijzonder advocaten en notarissen, bij strafrechtelijk onderzoek naar financieel-economische delicten nader uiteengezet. In die brief zijn ook enkele maatregelen aangekondigd om onnodige belemmeringen weg te nemen. Zo is inmiddels de Wet informatieplicht derdengeldenrekening notariaat in werking getreden op grond waarvan de geheimhoudingsplicht van notarissen zich niet meer uitstrekt tot hun derdengeldenrekening. In overleg met de Koninklijke Notariële Beroepsorganisatie (KNB) zal worden bezien of zich in de praktijk nog belemmeringen voordoen en hoe deze kunnen worden weggenomen.

Daarnaast bevat het wetsvoorstel verruiming mogelijkheden bestrijding financieel-economische criminaliteit[5] – thans in behandeling bij de Tweede Kamer – de introductie van beslistermijnen voor rechtbank en Hoge Raad om de

[3] Kamerstukken II 2012/13, 33 579, nr. 2
[4] Kamerstukken II 2010/11, 32 250, nr. 12
[5] Kamerstukken II 2012/13, 33 685, nr. 2

tijd die nu gemoeid is met toetsing van een beroep op het verschoningsrecht tot aanvaardbaar tijdsbestek terug te brengen. In de praktijk moet immers worden vastgesteld dat het soms meer dan een jaar duurt voordat duidelijkheid ontstaat over de vraag of bepaalde stukken in beslag kunnen worden genomen, hetgeen het opsporingsproces ernstig bemoeilijkt .

Een nauw met de geschetste problematiek samenhangend vraagstuk dat in dit verband moet worden genoemd, is het gegeven dat de dienstverlening van advocaten en notarissen zich over een steeds breder terrein uitstrekt, waardoor ook het domein dat wordt bestreken door het sectorale beroepsgeheim zich verder verbreedt. Hierdoor wordt het spanningsveld dat bestaat tussen de geheimhoudingsplicht en het daarmee samenhangende verschoningsrecht enerzijds en het belang van voortvarende opsporing en vervolging anderzijds, vergroot. De vraag naar de wenselijkheid van dit laatste behoeft aandacht, in de eerste plaats van de beroepsgroepen zelf.

3. Versteviging bestrijding van onderliggende fraudefenomenen

De meeste fraudefenomenen bevinden zich binnen de beleidsterreinen van de afzonderlijke departementen, en hebben betrekking op bijvoorbeeld een bepaalde regeling, toeslag of voorziening. Een aantal fraudefenomenen is faciliterend van aard: deze maken het mogelijk dat misbruik of fraude wordt gepleegd met collectieve voorzieningen, of zijn soms zelfs onmisbaar voor het kunnen plegen van dergelijke vormen van fraude. Ook individuele burgers en bedrijven kunnen hiervan de dupe worden. Met het steviger aanpakken van deze onderliggende fraudetypen worden twee doelen gediend: het wordt moeilijker om fraude met collectieve voorzieningen te plegen en tegelijkertijd wordt fraude ten nadele van burgers en bedrijven ermee bestreden. Het gaat in het bijzonder om 'gefingeerde dienstbetrekkingen', 'identiteitsfraude' en faillissementsfraude.

Gefingeerde dienstbetrekkingen
Rechtspersonen worden misbruikt om gefingeerde dienstbetrekkingen te creëren en daarmee op verschillende manieren frauduleus te handelen. Hoofddoel is het misbruik maken van voorzieningen waar iemand met een dienstbetrekking recht op heeft. Veelal zitten achter deze vorm van fraude *facilitators* die de fraude organiseren en mogelijk maken. Bij verschillende overheidsorganisaties liggen er kansen voor het opwerpen van barrières en verscherpte risicodetectie. Cruciaal is het zo spoedig mogelijk, liefst *realtime* uitwisselen van informatie en mogelijkheden om aan de hand daarvan in te grijpen. Een scala aan maatregelen tegen dit fenomeen is in voorbereiding of wordt onderzocht. Hieronder vallen:

- Aanpassing van verschillende werkprocessen bij Belastingdienst en UWV wordt onderzocht: aangescherpte risicodetectie bij bestuurders- en aandeelhouderswisselingen; mutatiemogelijkheid in polisadministratie bij geconstateerde fraude; analyseren gebeurtenisberichten van KvK op vermoedelijke fraude met gefingeerde dienstbetrekkingen;
- Introductie van weigeringsgronden voor inschrijving bij de KvK;
- De introductie van een civielrechtelijk bestuursverbod voor notoire fraudeurs, zoals hieronder toegelicht bij de aanpak van faillissementsfraude.

Identiteitsfraude
Identiteitsfraude is modus operandi bij veel verschillende vormen van fraude, net als bij andere illegale en criminele activiteiten zoals illegale grenspassage, illegale

arbeid, mensensmokkel, drugshandel, terrorisme en het witwassen van geld. Identiteitsfraude maakt daders ongrijpbaar en kost behalve de overheid ook burgers en bedrijven veel geld. De stijgende waarde van identiteitsgegevens en het groeiende aantal mogelijkheden om identiteitsgegevens van anderen te bemachtigen maken identiteitsfraude aantrekkelijker voor criminelen. Vooral identiteitsfraude via internet groeit.

Veel organisaties en sectoren nemen afzonderlijk maatregelen tegen identiteitsfraude. Die maatregelen variëren van publieksvoorlichting tot training van personeel tot de introductie van nieuwe technieken en systemen. Ook wordt er binnen diverse sectoren en ketens ingezet op uitwisseling van kennis en informatie om snel te kunnen reageren en liefst anticiperen op het handelen van fraudeurs.

Met de maatregelen in de verschillende sectoren worden veel problemen aangepakt. Maar de optelsom van afzonderlijke maatregelen is niet voldoende tegenover de geraffineerde werkwijzen van fraudeurs en de veelheid aan kwetsbare plekken waar zij kunnen toeslaan. Een effectieve aanpak van identiteitsfraude vraagt om een gecoördineerde inspanning van overheid, bedrijfsleven, maatschappelijke organisaties en burgers. De impact van initiatieven in diverse sectoren en ketens wordt groter door afstemming in een landelijk netwerk en aansluiting op internationale ontwikkelingen. In de eerste plaats gaat het om het beter en breder benutten van bestaande kennis, technieken en methoden. In de tweede plaats gaat het om het beter op elkaar afstemmen van nieuwe maatregelen die door diverse partijen in publieke en private sector getroffen worden. In de derde plaats gaat het om het afspreken van een gezamenlijke richting voor ontwikkelingen op de lange termijn.

Zoals reeds aangekondigd ontvangt u eind 2013 een aparte visie van het kabinet op de aanpak van identiteitsfraude, in aanvulling op deze brief.

Faillissementsfraude
De mogelijkheid om faillissement aan te vragen is een onmisbaar instrument binnen het economische stelsel. Fraude bij faillissementen is een vorm van criminaliteit die datzelfde stelsel ondermijnt. Van wezenlijk belang voor het bedrijfsleven, voor werknemers en voor de belastingbetaler, is dat bij faillissementen zoveel mogelijk middelen in de boedel blijven. Schuldeisers, waaronder leveranciers en de Belastingdienst maar ook voormalige werknemers van failliete ondernemingen, worden slachtoffer als fraudeurs er in slagen middelen aan de boedel van failliete rechtspersonen te onttrekken. Faillissementsfraude is daarmee een fraudefenomeen dat bij uitstek zowel de overheid als burgers en bedrijfsleven raakt. Daarbij komt dat faillissementsfraude vaak samengaat met andere vormen van fraude, zoals gefingeerde dienstbetrekkingen, uitkeringsfraude en subsidiefraude.

Recent zijn er al meerdere maatregelen getroffen om faillissementsfraude integraal aan te pakken, waaronder de uitbreiding en verbetering van de Garantstellingsregeling Faillissementscuratoren en de inrichting van een centraal meldpunt faillissementsfraude bij de Fiscale Inlichtingen- en Opsporingsdienst (FIOD). Hier wordt onder meer nog aan toegevoegd:

- Een wetgevingsprogramma met drie fraudeonderdelen:
  a) het wetsvoorstel civielrechtelijk bestuursverbod dat in november is aangeboden aan de Raad van State. Met dit nieuwe instrument kan worden

voorkomen dat frauduleuze bestuurders hun activiteiten via allerlei omwegen kunnen blijven voortzetten.
b) het wetsvoorstel herziening strafrechtelijk faillissementsrecht, waarvan de consultatie in oktober is afgerond. Hiermee worden de bepalingen inzake faillissementsfraude gemoderniseerd met het oog op verbetering van de effectiviteit en adequate toepassing van het strafrecht. Voor de opsporingspraktijk ontstaat hiermee een steviger handvat om op te treden tegen faillissementsfraude.
c) het wetsvoorstel versterking positie curator dat dit najaar in consultatie zal worden gebracht. Fraudebestrijding wordt een wettelijke taak van de curator en de informatiepositie van de curator wordt versterkt doordat de failliet een algemene informatie- en medewerkingsplicht jegens de curator krijgt, met inbegrip van de verplichting om de curator medewerking te verlenen bij het verkrijgen van toegang tot eventuele buitenlandse banktegoeden en/of versleutelde digitale bestanden.

In verband met het wetgevingsprogramma herijking faillissementsrecht, worden verschillende financieringsmodaliteiten nader onderzocht, zoals de mogelijkheid van een boedelafdracht[6].

- Landelijke uitrol van de succesvolle Haagse pilot faillissementsfraude die bestaat uit een fraudespreekuur voor curatoren bij een rechter-commissaris (R-C) en vrijgemaakte politie- en vervolgingscapaciteit. Dit tot onder meer tot de opsporing van een aanzienlijk aantal relatief eenvoudige faillissementsfraudezaken die op themazittingen worden afgedaan. Het Functioneel Parket ondersteunt de regioparketten bij de regionale aanpak van faillissementsfraude door *best practices* regionaal onder de aandacht te brengen. Inmiddels is een start gemaakt met de opzet van een dergelijke aanpak in de regio's Midden Nederland en Amsterdam. Het streven is om in 2014 een landelijke uitrol te hebben bereikt.

- Versterken van het systeem van Toezicht op Rechtspersonen (TRACK bij Justis) door een vroegtijdige signaleringsfunctie en meer verfijnde risicoprofielen. Het gebruik van risicomeldingen en terugmelding door afnemers wordt afgestemd en curatoren worden snel en vraaggericht bediend.

4. Gerichte aanpak fraudeurs

Een effectieve en gerichte aanpak van fraudeurs vraagt om een verbinding tussen het strafrecht en andere vormen van handhaving, toezicht en nalevingsbevordering, zodat het strafrecht niet geïsoleerd wordt ingezet wanneer andere maatregelen niet helpen ('ultimum remedium'), maar als inzet die is afgestemd met de acties van anderen in de handhavingsketen ('optimum remedium'). Op die manier is er sprake van meer afgestemde en integrale handhaving waarin het strafrecht tijdig en situationeel wordt ingezet. Dit vertaalt zich onder andere in onderstaande maatregelen.

Subjectgerichte aanpak
Waar gelegenheidsfraude voor een groot deel kan worden voorkomen door in te zetten op preventie, is voor de aanpak van beroepsfraudeurs een andere strategie gewenst. Deze groep maakt zich schuldig aan verschillende vormen van fraude, beschikt over de vaardigheden en posities om fraude te plegen en is actief op

[6] Kamerstukken II 2012/13, 29 911, nr. 74

zoek naar nieuwe mogelijkheden. Het combineren en analyseren van verschillende gegevensbronnen is nodig om bloot te leggen dat een bepaalde frauduleuze handeling onderdeel is van een breder handelingspatroon, en om zicht te krijgen op de groep personen die met verschillende regelingen fraude pleegt. Ook hier gaat het, in aansluiting op wat bij gegevensuitwisseling is opgemerkt, om verkenning van de mogelijkheden om dergelijke analyses en verkenningen te kunnen uitvoeren. Aan de hand hiervan kan gericht worden opgetreden, zowel in toezicht als op het terrein van opsporing en vervolging. Deze subjectgerichte aanpak wordt in samenwerking tussen onder meer Belastingdienst, politie, FIOD en Openbaar Ministerie opgezet. Om de facilitators van systeemfraude integraal te kunnen aanpakken is recent een combiteam aanpak facilitators binnen de Belastingdienst ingericht.

Afpakken, terugvorderen en terughalen

Fraude en andere vormen van criminaliteit mogen niet lonen, en geld dat langs illegale of onregelmatige weg is verkregen moet worden teruggevorderd en teruggehaald. In mijn brief van 3 juli 2013 heb ik de resultaten die in 2012 rijksbreed met terughalen en afpakken in ruimste zin gepresenteerd. Het kabinet bouwt voort op het in die brief uiteengezette beleid, onder meer door integrale samenwerking van betrokken overheidsdiensten, een verbetering van het instrumentarium voor ontneming, en een versterkte inzet op terugvorderen en terughalen in het buitenland. Hierbij wordt het uitgangspunt gehanteerd dat er als één overheid wordt opgetreden; per geval wordt bekeken welke (opsporing)dienst het beste is toegerust om op te treden en de opbrengsten komen ten goede aan de overheid.

a) Integrale samenwerking

Bij het terugvorderen en afpakken wordt opgetreden als één overheid. In Brabant is ruim anderhalf jaar geleden een pilot gestart om dit "integraal afpakken" te versterken, in de vorm van een integraal afpakteam, waarin politie, Belastingdienst, FIOD en Openbaar Ministerie samenwerken. Dit team heeft daar zijn meerwaarde laten zien en de Brabantse pilot zal dan ook de komende jaren worden voortgezet. Ook op andere plekken in het land wordt gewerkt met een integrale aanpak van criminaliteit en het afpakken van crimineel vermogen, zoals het Ketenprogramma Afpakken van het OM en de politie, de RIEC-structuur en de Landelijke Stuurgroep Interventieteams. Deze aanpak wordt in 2014 verder versterkt en verbreed, in samenwerking met het OM, de politie en het ministerie van Financiën. Ook wordt de verbinding gelegd met het lokaal bestuur over de rol die gemeentelijke diensten in deze aanpak kunnen spelen.

b) Verbetering instrumentarium ontneming

Het is van belang dat het instrumentarium voor terugvorderen en terughalen van illegaal verkregen voordeel zo efficiënt en breed mogelijk kan worden ingezet. Een blijvende inspanning om te streven naar verbeteringen in dit instrumentarium is onontbeerlijk. Er wordt onderzocht welke mogelijkheden er zijn om ten behoeve van het terugvorderen en terughalen de bestuurlijke boete met een ontnemingscomponent ruimer in te zetten. In samenspraak met de Rechtspraak wordt bezien hoe in het kader van de mogelijkheden die de nieuwe gebiedsindeling van de rechtspraak biedt een snelle en specialistische behandeling van de complexere ontnemingszaken kan worden bereikt. De komende maanden vindt er een inventarisatie en nadere uitwerking plaats van mogelijke

verbetermaatregelen. In het voorjaar van 2014 zullen trajecten worden gestart om de verbetermaatregelen te kunnen implementeren.

c) Terugvorderen en terughalen in het buitenland

Een belangrijk aspect bij de aanpak van fraude is het terugvorderen en terughalen van financiële middelen uit het buitenland. Met meer kracht en snelheid zal worden opgetreden tegen fraudeurs en wanbetalers die in het buitenland gevestigd zijn, naar het buitenland vertrekken of middelen naar het buitenland verplaatsen. Per type vordering (straf- of bestuursrechtelijke boetes of maatregelen, misbruik van overheidsgelden, langs criminele weg verkregen vermogen, belasting- en studieschulden) zal worden bezien welke maatregelen er zijn om effectief in het buitenland op te treden. Hiertoe worden de verschillende maatregelen van de verschillende departementen in kaart gebracht en vergeleken. Daarbij wordt bezien of de juridische basis voor invordering in het buitenland moet worden versterkt. Vervolgens wordt bezien in hoeverre maatregelen breder of effectiever kunnen worden toegepast. Deze verkenning is eind eerste kwartaal 2014 gereed . De afzonderlijke overheden gaan beter samenwerken bij het opsporen van personen in het buitenland, onder meer door uitwisseling van (adres)gegevens. Is de persoon gevonden, dan worden de krachten waar zinvol gebundeld, bijvoorbeeld door de afzonderlijke vorderingen te bundelen en gezamenlijke (juridische) stappen te ondernemen. Voorts zal worden onderzocht hoe gezamenlijk kan worden aangejaagd dat het buitenland waar wenselijk wetswijzigingen of procesmatige wijzigingen overweegt.

Aanpak fraude tegen burgers en bedrijven (horizontale fraude)
In het Inrichtingsplan van de Nationale Politie is een totale capaciteit voor financieel-economische criminaliteit (FinEC) voorzien van 1.156 fte. De opsporing van financieel-economische criminaliteit is belegd zowel op regionaal als landelijk niveau. Een deel van deze capaciteit wordt gericht ingezet ten behoeve van de fraudebestrijding. Binnen de Dienst Regionale Recherche van de eenheden van het korps worden separate FinEC / fraudeteams ingericht. Kerntaken van deze teams zijn in ieder geval het zelfstandig uitvoeren van onderzoeken naar vormen van horizontale fraude. Met de inrichting van deze teams wordt de inzet op het thema fraude op regionaal niveau gewaarborgd. Het landelijk niveau kent ook een uitvoeringsteam dat is belast met zeer complexe fraudezaken. Voor de aanpak van (complexe) fraudezaken kan aan de specialistische fraude-expertise generieke en specialistische capaciteit toegevoegd worden (bijv. digitale expertise).

Met het Ketenprogramma Afpakken zijn er al concrete resultaatafspraken per jaar gemaakt. Jaarlijks wordt oplopend tot 20 miljoen Euro in de strafrechtketen geïnvesteerd met als doel om om –in een oplopende reeks- vanaf 2018 jaarlijks 100 miljoen Euro af te pakken. De afgelopen periode zijn met de intensivering van het afpakken al positieve resultaten geboekt. Hierover informeerde ik uw Kamer bij brief van 3 juni jongstleden . In de huidige landelijke prioriteiten is voor de aanpak van criminele samenwerkingsverbanden bovendien afgesproken dat standaard de mogelijkheid tot financieel rechercheren en de bestuurlijke aanpak moet worden onderzocht. Dit om het terugvorderen van crimineel verkregen vermogen te borgen binnen de aanpak van criminele samenwerkingsverbanden.

Er zijn voor 2014 op regionaal niveau afspraken gemaakt tussen het Openbaar Ministerie en de politie over de aanpak van horizontale fraude, waaronder faillissementsfraude. Het gaat hierbij om minimumafspraken over aantallen te

behandelen fraudezaken tussen de parketten van het OM en de eenheden van de politie. In 2014 worden ook de landelijke prioriteiten en de bijbehorende resultaatafspraken van de politie vastgesteld voor de periode 2015 tot en met 2018,Dit zal gebeuren op basis van de afspraken over 2014, een recent door politie en OM uitgevoerde inventarisatie van de huidige inspanningen op gebied van horizontale fraudebestrijding en de inzichten uit het nationaal dreigingsbeeld Georganiseerde Criminaliteit.

AFM, BFT en fraudebestrijding

Tijdens de behandeling van de begroting van Veiligheid en Justitie heb ik naar aanleiding van een vraag van het lid Oskam toegezegd om in te gaan op de rol van het Bureau Financieel Toezicht (BFT) en de Autoriteit Financiële Markten (AFM) bij de aanpak van fraude. Het BFT valt primair onder mijn verantwoordelijkheid en is belast met het toezicht op onder andere advocaten, notarissen en belastingadviseurs. De AFM is gedragstoezichthouder op de financiële markten, zoals bedrijven of personen die werkzaam zijn bij financiële dienstverleners (zoals accountants), banken en beleggingsinstellingen. Beide organisaties spelen een belangrijke rol bij het voorkomen, signaleren en bestrijden van fraude, in die zin dat zij toezicht houden op beroepsgroepen, zoals notarissen en accountants, die in het kader van hun taakuitoefening een cruciale rol kunnen spelen. Voor BFT zowel als AFM geldt dat regelgeving tot stand is gekomen om hen daartoe (nog) beter in staat te stellen. Zo is met ingang van 1 januari jl. is de wettelijke toezichtstaak van het Bureau Financieel Toezicht (BFT) op het notariaat uitgebreid, met een uitbreiding van de inzagebevoegdheden ten aanzien van de dossiers van de notaris, waardoor eventuele onregelmatigheden, zoals het plegen van fraude, eerder aan het licht kunnen komen. Daarnaast besteedt het BFT in 2014 het grootste deel van zijn onderzoekscapaciteit aan risicogerichte onderzoeken, met als belangrijkste doelen het bevorderen van de integriteit van het financiële stelsel en van de informatiepositie van de opsporingsinstanties.

Voor de AFM geldt dat de nadruk van de belangrijkste toezichtthema's voor 2014 onder meer ligt op de kwaliteit van de governance en de accountantscontrole, het verminderen van het schadelijk gedrag op de financiële markt en het bestrijden van financiële criminaliteit. Met ingang van 1 januari a.s. is bovendien de Wet financieel toezicht gewijzigd waardoor de informatie uitwisseling tussen AFM en een groot aantal toezichts- en opsporingsdiensten in het kader van de borging van een integere financiële sector wordt geoptimaliseerd. Deze samenwerking en informatie-uitwisseling vindt vooral plaats binnen het (permanente) samenwerkingsverband Financieel Expertise Centrum (FEC), dat speciaal is opgezet voor de versterking van de integriteit van de financiële sector. Op basis van het bovenstaande ben ik van oordeel dat beide organisaties fraude op de juiste wijze prioriteren en goed zijn toegerust om preventief toezicht te houden, repressief op te treden en zo nodig signalen van onregelmatigheden te melden voor eventuele strafrechtelijke vervolging.

Budgettaire consequenties

De maatregelen die in dit actieplan worden aangekondigd, zijn door de betreffende departementen van dekking voorzien. Voor zover maatregelen nog onderwerp zijn van nader onderzoek, zullen bij dit onderzoek ook de financiële effecten in beeld gebracht worden, waar nodig via business cases.

Tot slot

Fraude zal nooit volledig uitgebannen kunnen worden, maar het kabinet wil de mogelijkheden tot fraude zo veel mogelijk beperken, de fraudebestendigheid van beleid en regelgeving vergroten en het gezamenlijke optreden van overheidsdiensten bij fraudegevallen flink verstevigen. Ik ben ervan overtuigd dat deze doelstellingen met het hierboven beschreven pakket aan maatregelen een forse nieuwe impuls kunnen krijgen.

De voortgang en resultaten van de maatregelen zullen goed worden gemonitord. De diverse bewindslieden zullen de Kamer op de gebruikelijke manier –via de departementale jaarverslagen en andere reguliere rapportages- informeren over de stand van zaken op de onderscheiden beleidsdomeinen. Daarnaast zal de Kamer eenmaal per jaar worden geïnformeerd over de voortgang en de stand van zaken van de rijksbrede anti-fraudestrategie.

De Minister van Veiligheid en Justitie,

I.W. Opstelten

Bijlage

1. Sociale voorzieningen

Het draagvlak voor onze sociale zekerheid brokkelt af als fraude en misbruik onbestraft blijven. Solidariteit impliceert dat alleen een beroep wordt gedaan op publieke middelen en de sociale zekerheid als dat strikt noodzakelijk is. Per 1 januari 2013 is de *Fraudewet*[7] van kracht. Daarmee is in gang gezet dat onrechtmatig verkregen voordeel en boetes altijd moeten worden (terug)betaald. Bovendien zijn de boetes verhoogd. Hier gaat niet alleen een preventieve werking vanuit, maar dit bevestigt ook de lijn dat fraude niet loont.

Op 4 oktober jl. is uw Kamer reeds geïnformeerd over de nieuwe maatregelen die de minister en staatssecretaris van SZW nemen op het terrein van fraude, handhaving en naleving.[8] Het bestrijden van fraude en het niet naleven van regels berust op opsporing, strikte handhaving, preventie en fraudebewustzijn. De maatregelen op het terrein van opsporing en strikte handhaving zijn gericht op het intensiveren van de handhaving door de inzet van meer mensen bij UWV, de SVB en Inspectie SZW, het koppelen van gegevens, het beter samenwerken in de keten en het verhogen van de (gepercipieerde) pakkans. Dit leidt tot een snellere en efficiënte aanpak van fraude. De maatregelen op het terrein van preventie van fraude en misbruik zijn gericht op het vereenvoudigen en begrijpelijk maken van de regels, het voorlichten over de plicht van uitkeringsgerechtigden om zich in te spannen om werk te vinden en te houden en een cultuuromslag bij professionals, waardoor fraude en misbruik sneller worden herkend en voorkomen.

Intensivering handhaving

- Inzet van meer mensen bij UWV, de SVB en Inspectie SZW. De capaciteit bij UWV, de SVB en Inspectie SZW wordt de komende vier jaar uitgebreid met 260 fte., waarvoor cumulatief 100 miljoen euro beschikbaar wordt gesteld. De verwachte opbrengst van deze uitbreiding is naast een eerlijker systeem (misbruik wordt bestraft), een financiële netto opbrengst van naar verwachting 189 miljoen euro.
- Het wetsvoorstel *Fraudeaanpak door bestandskoppelingen*[9], dat op 1 oktober jl. door de Eerste Kamer is aangenomen, legt de wettelijke basis voor het instrument Systeem Risico Inventarisatie (SyRI). Hiermee kunnen, in het kader van integraal overheidsoptreden in een samenwerkingsverband, bestanden van gemeenten, UWV, SVB, Inspectie SZW en Belastingdienst worden gekoppeld. Zo kan op basis van risicoanalyses worden bepaald bij welke personen of bedrijven het grootste risico op regelovertreding aanwezig is. Daarnaast zijn een aantal nieuwe bestandskoppelingen mogelijk. Zo wordt onder meer geregeld dat het ministerie van Buitenlandse Zaken gegevens over gedetineerden in het buitenland mag verstrekken aan uitvoerders in de sociale zekerheid. Daarnaast wordt geregeld dat informatie over gastouders gekoppeld kan worden aan bijstandsgegevens.

[7] Wet aanscherping handhaving en sanctiebeleid SZW-wetgeving.

[8] Kamerstukken II 2013/14, 17 050, nr. 439

[9] Wetsvoorstel tot wijziging van de Wet SUWI en enige andere wetten in verband met fraudeaanpak door gegevensuitwisselingen en het effectief gebruik van binnen de overheid bekend zijnde gegevens (33 579).

Betere ketensamenwerking en verhogen pakkans

- Inzet interventieteams op landelijke thema's met hoog frauderisico. Hierin werken Belastingdienst, Inspectie SZW, UWV, VNG, Divosa, SVB, politie en Openbaar Ministerie samen met als doel belasting- en premiefraude, uitkeringsfraude en illegale tewerkstelling aan te pakken.
- Begin 2012 is het *Programma Aanpak Malafide Uitzendbureaus* aan uw Kamer aangeboden. Daarover is in de Voortgangsbrief 'Aanpak malafide uitzendbureaus' d.d. 15 oktober 2013 aan uw Kamer gerapporteerd.[10] De aanpak van malafide uitzendbureaus wordt via twee sporen georganiseerd. Ten eerste wordt de handhaving en opsporing versterkt. Ten tweede wordt ingezet op het vergroten van transparantie van de uitzendbranche. Een gezamenlijke aanpak met de sector is hierbij van groot belang. Ook is in het wetsvoorstel aanpak fraude toeslagen en fiscaliteit een depotplicht voor inleners van niet-gecertificeerde uitzendbureaus ingevoerd. De boetes voor het niet voldoen zijn fors verhoogd. Voor de niet-gecertificeerde uitlener bedraagt de boete € 19.500 en voor de inlener € 7.800.
- Uw Kamer is op 11 april 2013 het actieplan *Bestrijden van schijnconstructies* aangeboden[11]. Op dit moment werken wij door samenwerking in de keten met betrokken partijen, waaronder sociale partners, Algemene Bond Uitzendondernemingen (ABU), Kamer van Koophandel, Openbaar Ministerie, IND en Regionale Centra Fraudebestrijding, UWV, Inspectie SZW, Belastingdienst en andere ministeries aan de aanpak van schijnconstructies. Binnenkort ontvangt uw Kamer informatie over de voortgang. Op 26 november jl. heeft uw Kamer informatie over de voortgang ontvangen[12].

Preventie

- Samen met UWV, SVB en gemeenten wordt de bestaande voorlichting tegen het licht gehouden en wordt gekeken waar deze begrijpelijker, inzichtelijker en eenvoudiger kan.
- De campagne *'Voorkom problemen. Weet hoe het zit'* wijst burgers en werkgevers op hun rechten en plichten. Deze campagne wordt verbreed. Er zal ook worden voorgelicht over het naleven van de arbeids- en re-integratieverplichtingen (de zogenaamde inspanningsplicht: de plicht om je in te spannen om werk te vinden, te aanvaarden en te behouden).
- Ter bevordering van het zelfreinigend vermogen en toezicht van branches is een registratieplicht ingevoerd bij de Kamer van Koophandel voor ondernemingen die arbeidskrachten ter beschikking stellen. De Inspectie SZW heeft daarnaast in samenwerking met brancheorganisaties 'zelfinspectie tools' ontwikkeld.
- Handhaving staat of valt met vakbekwaamheid van de uitvoerders. Met het in 2012 ingezette project *Impuls vakmanschap* wordt op het verder professionaliseren van de klantmanagers bij gemeenten ingezet door het ontwikkelen van competenties en het vergroten van kennis en vaardigheden.

2. Toeslagen en fiscaliteit

[10] Kamerstukken II 2013/2014, 17 050, nr. 442
[11] Kamerstukken II 2012/2013, 17 050, nr. 428
[12] Kamerstukken II 2013/2014, 17 050, nr. 447

Bij brief van 10 mei 2013 heeft de staatssecretaris van Financiën, mede namens de minister van Binnenlandse Zaken en Koninkrijksrelaties, de minister van Veiligheid en Justitie, de minister van Sociale Zaken en Werkgelegenheid, de minister van Volksgezondheid, Welzijn en Sport en de minister voor Wonen en Rijksdienst diverse aanvullende maatregelen aangekondigd om systeemfraude met toeslagen tegen te gaan. De aard van deze maatregelen is zoveel mogelijk preventief. Zij grijpen in een zo vroeg mogelijk stadium aan vanuit de overweging dat fraude en criminaliteit niet mogen lonen. Als er geen sprake is van gerechtvaardigd vertrouwen zal fraudebestrijding adequaat worden opgepakt. Het betreft hier zowel zorg-, huur- als kinderopvangtoeslagfraude.

Overzicht maatregelen:

-De beslistermijn voor het toekennen van toeslagen om aanvragen met een verhoogd fraude-risico te kunnen behandelen wordt verlengd.
-De weigeringsgronden voor het uitbetalen van voorschotten worden uitgebreid, bijvoorbeeld voor gevallen waarbij er onvoldoende gegevens bekend zijn of waarbij er twijfel is over iemands adres.
- Twee categorieën van aanvragers worden uitgezonderd van de mogelijkheid een voorschot te krijgen: a) aanvragers aan wie in een periode van 5 jaar voorafgaand aan de aanvraag door de Belastingdienst een vergrijpboete is opgelegd of een strafrechtelijke sanctie onherroepelijk is geworden; b) aanvragers die pas na afloop van het toeslagjaar een aanvraag indienen.
- Binnenkort kan bij medeplichtigen, doen plegers en ook een bestuurlijke boete worden opgelegd bij fraude met toeslagen.
-Uitbreiding van aansprakelijkheidsstelling bij uitbetaling van toeslagen aan derden.
- Uitbreiding mogelijkheden inzet ANPR naar toeslagschulden.
-Om onder meer carrouselfraude te bestrijden, wordt het opzettelijk niet betalen op aangifte strafbaar gesteld.
- Ook komt er een vergrijpboete voor het opzettelijk indienen van een onjuiste voorlopige teruggave Inkomstenbelasting.
- Geen voorlopige aanslag of tot een lager bedrag opleggen indien een vergrijpboete op grond van de AWR of Awir is opgelegd of sprake is van een strafrechtelijke veroordeling voor een daaraan soortgelijk misdrijf.
- Geen voorlopige aanslag of tot een lager bedrag opleggen indien niet of niet binnen de gestelde termijn is voldaan aan de aangifteplicht voor de inkomstenbelasting.
- Depotplicht voor niet-gecertificeerde uitzendbureaus+ stortingsplicht inlener i.c.m. forse boetes bij niet naleving en aansprakelijkheid.
- Aansprakelijkheid van derde op wiens bankrekening teruggaaf IB/OB is uitbetaald.
- Om de facilitators van systeemfraude integraal te kunnen aanpakken is recent een combiteam aanpak facilitators binnen de Belastingdienst ingericht.
- Versterking inzet risicoprofielen door gemeenten (BZK).
- Onderzoek en afspraken gemeente, Belastingdienst en BZK naar risico's in de keten.
- Bij de Douane zijn twee fraudeteams geformeerd op het gebied van

Douane en Accijns.

3. Studiefinanciering

Fraude in de studiefinanciering wordt zoveel mogelijk voorkomen en waar nodig actief bestreden. Bij het bestrijden wordt door DUO een mix van maatregelen ingezet, waarbij door een gelaagde inzet een maximaal resultaat wordt bereikt. De eerste aanzet is het via voorlichting en communicatie beïnvloeden van de doelgroep om *compliance* te stimuleren. De volgende stap is het treffen van feitelijke maatregelen om misbruik en fraude te onderkennen, te corrigeren en te sanctioneren.

Om de mogelijkheden tot fraude en misbruik zoveel mogelijk te beperken, bestaat er een uitgebreid controlesysteem. Per onderdeel van de studiefinanciering voert de Dienst Uitvoering Onderwijs (DUO) controles voorafgaand aan de toekenning uit, controles tijdens de toekenningsperiode en controles achteraf. Voor het bepalen van het recht op studiefinanciering wordt zoveel mogelijk uitgegaan van gegevens verstrekt door overheidsinstanties en onderwijsinstellingen (basisregistraties). Wanneer deze gegevens niet voor de volledige 100% betrouwbaar zijn, wordt fraude en misbruik 'geïmporteerd'. Wanneer gegevens niet beschikbaar zijn bij overheidsbronnen, worden de gegevens bij de burger zelf opgevraagd.

De werking van het controlesysteem wordt bewaakt. Indien daar aanleiding toe is, wordt de specifieke controles aangepast. Daarnaast is er ook aandacht voor het voorlichtingsbeleid (preventieve werking) en sanctiebeleid (repressie). In het jaarverslag van OCW wordt gerapporteerd over de risico's met een financieel beslag van meer dan € 2,5 miljoen.

Overzicht belangrijkste maatregelen:

De afgelopen periode is of wordt de aanpak op een aantal onderdelen versterkt, waarvan de belangrijkste worden hieronder genoemd.

- -Aanpak misbruik uitwonendenbeurs. DUO voert sinds 2010 huisbezoeken uit om te controleren of een student inderdaad op het door hem opgegeven GBA-adres woont. Studenten worden geselecteerd op basis van een risicoprofiel. In 2012 en 2013 blijkt circa 50 procent van de gecontroleerde studenten niet op het aangegeven adres te wonen.
- - Eénoudertoeslag. Er wordt intensiever gecontroleerd of er sprake is van eenoudergezin (éénoudertoeslag) of dat er toch een partner is.
- -Meeneembare studiefinanciering. Met Nederlandse studiefinanciering kan er in het buitenland worden gestudeerd. Naar aanleiding van enkele recente fraudegevallen met gefingeerde inschrijvingen bij instellingen in het buitenland worden de controles uitgebreid.
- -Debiteuren in het buitenland. Oud-studenten die hun studieschuld niet terugbetalen en zich (in het buitenland) onzichtbaar houden voor de

Nederland overheid worden opgespoord en tot betaling aangezet. Maatregelen zijn getroffen[13].

- Fraude door EU-studenten. EU-studenten kunnen Nederlandse studiefinanciering ontvangen wanneer ze migrerend werknemer zijn. Soms wordt er niet daadwerkelijk gewerkt en is men in dienst bij fake-bedrijfjes (gefingeerd werknemerschap). De controle hierop wordt in samenwerking met andere overheidsorganisaties aangescherpt.

4. Zorg

Fraude en oneigenlijk gebruik in de zorg tasten de betaalbaarheid van ons zorgstelsel aan en bedreigen de solidariteit. Bestrijding van fraude en de aanpak van oneigenlijk gebruik van zorg zijn daarom een prioriteit in het beleid. Zowel op het gebied van de langdurige zorg, de maatschappelijke ondersteuning als de curatieve zorg zijn en worden veel acties in gang gezet om fraude en oneigenlijk gebruik terug te dringen of te voorkomen. De maatregelen die genomen zijn, en nog genomen zullen worden, zijn gericht op het voorkomen alsmede het opsporen en bestrijden van fraude en oneigenlijk gebruik, zodat de financiële middelen die voor de zorg bestemd zijn ook komen waar ze horen, namelijk bij de zorg voor de patiënt of cliënt die deze zorg nodig heeft. Dit vergt een sluitende keten waarbij de samenhang tussen preventie, toezicht, opsporing en strafrechtelijke vervolging geborgd is door een intensieve samenwerking tussen alle betrokken partijen. Een intensivering van de opsporing alleen zal onvoldoende bijdragen aan een effectieve bestrijding van oneigenlijk gebruik en fraude in de zorg. De minister en staatssecretaris van VWS hebben op 16 september 2013 aan uw Kamer hun plan van aanpak voor fraudebestrijding in de zorg gestuurd[14]. Daarin zijn de volgende maatregelen aangekondigd:

- Het versterken opsporingsfunctie in de zorg door extra fte vanaf 2014.
- De start van een Expertisecentrum Zorgfraude Bestrijding (samenwerking tussen Belastingdienst, CIZ, ZN, FIOD, OM, IGZ, VWS, I-SZW, NZa) per 1 oktober 2013
- Het aanscherpen wettelijke bevoegdheden en sanctiemogelijkheden van toezichthouders in wet- en regelgeving. Hierbij wordt waar nodig ook gekeken naar mogelijkheden van het doorbreken van het medisch beroepsgeheim bij (ernstige) vermoedens van fraude.
- Het toetsen van nieuwe wet- en regelgeving en bekostigingssystemen op fraudegevoeligheid voordat deze worden ingevoerd
- Het vergroten van transparantie bij aanbieders, onder andere door vergroten bewustwording en verbeteren administratieve organisatie en interne controle (AO/IC)
- Een Onderzoek naar omvang van fraude en witte vlekken in het systeem door de NZa

In december 2013 wordt een tweede voortgangsrapportage aan de Tweede Kamer toegezonden.

Belangrijk aandachtspunt in de tweede voortgangsrapportage is de voortgang van een aantal ontwikkelingen rond de AWBZ. Om fraude met persoonsgebonden budgetten (PGB-fraude) tegen te gaan is de afgelopen periode ingezet op onder meer een betere informatievoorziening.

[13] Kamerstukken II 2012/13, 24724, nr. 119

[14] TK 2012-1013, 28828 nr. 50

- Zo worden personen die voor het eerst een indicatie aanvragen met een voorkeur voor een PGB, gezien door het Centrum Indicatiestelling Zorg (CIZ) en wordt door de zorgkantoren allereerst een bewust keuzegesprek gevoerd met deze personen. Bovendien zijn bestaande budgethouders nagelopen.
- In de periode juli 2013 tot eind 2014 zullen de zorgkantoren ca. 30.000 van de in totaal ca.130.000 mensen met een PGB thuis bezoeken. Deze huisbezoeken zijn om na te gaan of cliënten het slachtoffer zijn van fraudeurs of dat de budgethouders zelf fraude plegen.
- Om dit op een effectieve manier te kunnen doen is de capaciteit van de zorgkantoren uitgebreid, en is via Zorgverzekeraars Nederland een gestandaardiseerde manier van werken ontwikkeld en wordt maandelijks kennis gedeeld. Om effectiever op te kunnen sporen en sancties te kunnen opleggen is bij de ISZW een aparte eenheid ingericht en is capaciteit vrijgemaakt.
- Tot slot krijgt personen met een PGB niet langer hun budget contant op hun rekening gestort, maar is een systeem ingevoerd dat vergelijkbaar is met internetbankieren. Op deze wijze kan PGB-fraude eerder en beter worden opgespoord.
- Om resterende knelpunten weg te nemen en om fraudeurs zoveel mogelijk gelegenheid te ontnemen, wordt bovendien bezien hoe een juridisch instrumentarium kan worden ontwikkeld om een PGB te mogen weigeren. Bevoegdheden van zorgkantoren worden uitgebreid om bemiddelingsbureaus effectiever aan te kunnen pakken en de capaciteit in de keten van indicatiestelling, toewijzing, controle, opsporing wordt vergroot.

Daarnaast wordt bij het CIZ een aantal maatregelen genomen om de indicatiestelling voor risicogroepen aan te scherpen.

5. Subsidies en inkomensoverdrachten Economische Zaken

Agentschap NL

Binnen Agentschap NL wordt thans risicogericht handhaven uitgerold. Het systeem van eerste- en tweedelijns handhaving is reeds vergaand operationeel. In de tweede lijn, waar onderzoek naar misbruik en fraude plaatsvindt, en bij de [redacted] is de schakel met het OM belegd. Een ICT-tool zal in dit kader zorgen voor steekproefselectie, registratie van onderzoeksresultaten en inzicht bij bedrijfsbezoeken. Medewerkers hebben een training gehad voor effectiever uitvoeren van controlebezoeken. Periodiek worden de risico's en resultaten van de handhavingsmaatregelen geëvalueerd en, indien nodig, bijgesteld. Door risicoanalyse en handhaving komen de belangrijkste risico's in beeld. Door permanente evaluatie wordt de handhaving steeds gerichter.

Nederlandse voedsel- en warenautoriteit

Wederzijdse afspraken over de opsporing, prioriteiten en de afhandeling van opsporingsonderzoeken tussen het FP van het OM, EZ en VWS en de NVWA-Inlichtingen en Opsporingsdienst (IOD) zijn opgenomen in een handhavingsarrangement. Op basis van risicoanalyses die worden uitgevoerd op de verschillende beleidsdomeinen van de NVWA, worden thema's afgeleid die in het handhavingsarrangement worden benoemd. Fraude met (EU-) subsidies is in 2012 aangemerkt als een meerjarige prioriteit van de NVWA-IOD. In vervolg hierop wordt onderzoek naar geldstromen en financiële fraude, waaronder subsidiefraude, in 2013 en 2014 meegenomen in de verdere ontwikkeling van het Domein Gericht Inwinnen. Dit is een thematische, geïntegreerde en cyclische aanpak met een doorlopende inspanning op de verschillende domeinen met als

doel een permanent en actueel beeld van (fraude)risico's op de beleidsterreinen van de NVWA, waaronder ook (EU)subsidies.

Om een effectievere en meer geïntegreerde aanpak van fraude op de verschillende vakgebieden te realiseren is al in 2012 de samenwerking op het gebied van afpakken tussen de IOD en andere BOD-en geïntensiveerd. Hiermee wordt ook uitvoering gegeven aan het principe dat misdaad niet mag lonen. BOD-breed wordt ingezet op intensivering van afpakken. Dit levert een jaarlijks groeiend resultaat op. In 2012 is gestart met samenwerking vanuit een expertpool, waarin specialisten op het gebied van afpakken vanuit alle BOD-en en het FP zijn verenigd. Deze samenwerking is in 2013 verder geïntensiveerd. Door versterking van de samenwerking van met het toezicht in de vorm van assistentie, begeleiding en coaching, wordt ook zoveel mogelijk crimineel voordeel afgepakt in inspectieonderzoeken en bij de bestuurlijke handhaving. Tot slot spant de IOD zich in om waar mogelijk vermogensbestanddelen in een zo vroeg mogelijk stadium te detecteren en veilig te stellen ten behoeve van afpakken en vooral ten behoeve van de belangen van slachtoffers.

Dienst Regelingen
Voor de Europese subsidies is in EU-regelgeving nauwkeurig vastgelegd welke werkzaamheden in dit kader door DR moeten worden verricht en op welke wijze dit dient te gebeuren. Voor de uitvoering van andere taken wordt ingezet op programmatisch handhaven. NVWA voert administratieve nacontroles uit bij ondernemingen die verrekeningen hebben ontvangen uit het Europees Landbouwgarantiefonds (ELGF). Gesignaleerde risico's worden afgedekt door 100% administratieve controles op alle ontvangen steunaanvragen. Deze controles dienen ter vaststelling dat aan de subsidiabiliteitsvoorwaarden is voldaan. Daarnaast worden aan de hand van een steekproef (deels aselect en deels risicoanalyse) op een percentage van de aanvragen of totaalbedrag voor steun controles ter plaatse uitgevoerd. Dit percentage wordt verhoogd als belangrijke onregelmatigheden worden geconstateerd. Onregelmatigheden ((on)opzettelijke handelingen die leiden tot negatieve gevolgen voor Europese fondsen) moeten worden vastgelegd in een onregelmatigheidsregister. Onregelmatigheden vanaf € 10.000 moeten worden gemeld bij de Europese Commissie (EC). Omdat de EU-verordeningen voldoende mogelijkheden bieden om misbruik aan te pakken is slechts in een beperkt aantal gevallen aanleiding voor een strafrechtelijk vervolg.

MCF
pt. 3

MINISTERRAAD/ONDERRAAD

Met eventuele gecoördineerde opmerkingen uiterlijk retour:

..... Vrij ..... dag ..... 13/12 vóór 15.00 uur! .....

X			BFB		BJZ		DGFZ	CC	
			FM		AFEP				
			FIN						

Ontvangen d.d.: 13-12-2013

Behandelende afd./bureau: BZK

Behandelend medewerker:

Medeparaaf:

	datum	paraaf
behandelend medewerker	13/12	

Geen opmerkingen ☐

Zie bijgevoegde nota*) ☒

No 6778 Uitvoeringsbeleid

*) Nota met kopieën aanleveren bij

Nota voor RMR/MR óók in WORD-versie via de mail aanleveren.

13/12 B2K

MCF

Handtekening bewindspersoon



Minister van Binnenlandse Zaken en Koninkrijksrelaties

Rijksoverheid

Aanbiedingsformulier voor MCF

Aanbieding

Van 1 *	Minister van Binnenlandse Zaken en Koninkrijksrelaties
Mede namens 2	N.v.t.
Type voorstel *	Brief aan de Tweede Kamer

Titel en inhoud

Korte titel *	Kabinetsvisie op identiteitsfraude en Monitor Identiteitsfraude
Inhoud en doelstelling van het voorstel *	Met deze brief wil het kabinet een integrale visie op de aanpak van identiteitsfraude delen met de Tweede Kamer. Na een analyse van het probleem vindt u een visie op de aanpak van identiteitsfraude zoals het kabinet beoogt. Contouren visie: 1. Gezonde weerstand organiseren bij burgers en bedrijven 2. Betrouwbare controles. Investeren in ijkmomenten identiteitsvaststelling 3. Vroege diagnose door inzetten intelligence 4. Snel herstellen van identiteit 5. Effectieve repressie van fraude Ook wordt beschreven dat er een internationale component is. Tevens bij de brief een eerste monitor Identiteit in Cijfers. De monitor Identiteit in Cijfers beoogt een compleet beeld te presenteren van het veld van identiteit en identiteitsmanagement. Zowel over het publieke als het private domein bevat deze monitor cijfers op de thema's identiteiten, identiteitsmanagement en identiteitsfraude.
Voorgesteld besluit *	Het ontwerp te aanvaarden en na vaststelling in het kader van nahang aan de Staten-Generaal te zenden.

Behandeltraject

Datum aanbieding *	09-dec-2013
Kenmerk *	2013
Hamerstuk *	☐ Ja ☒ Nee
Voorgaande behandeling *	☐ Ja ☒ Nee

Gevolgen en juridisch kader

Gevolgen rijksbegroting *	☐ Ja ☒ Nee
Gevolgen voor regeldruk *	☐ Ja ☒ Nee
Overeenstemming met V&J inzake wetgevingstoets en effectenanalyse *	☐ Ja ☐ Nee, met bijlage ☐ Nee, zonder bijlage ☒ N.v.t.
Aan EU Notificatie voldaan *	☐ Ja ☐ Nee ☒ N.v.t.
Verplichting Int. verdragen en/of Europese regelgeving*	☐ Ja ☒ Nee

Formulier nummer 20131009-01

Interdepartementale afstemming

Overeenstemming BZK inzake beoordelingskader financiele/ bestuurlijke consequenties decentrale overheden en/of Caribisch Nederland *	☒ Ja	☐ Nee	☐ N.v.t.					
Overeenstemming BZK toelichting *								
Overeenstemming Aruba, Curaçao en Sint Maarten *	☐ Ja	☐ Nee	☒ N.v.t.					
Ambtelijk afgestemd *	☒ Ja	☐ Nee	☐ N.v.t.	in	Hoofdenoverleg rijksbrede fraude			
Overeenstemming bereikt op ambtelijk niveau *	☒ Ja	☐ Nee	☐ N.v.t.					
Overeenstemming bereikt met	☐ AZ	☒ BZK	☒ EZ	☐ I&M	☒ SZW	☐ VWS	☒ W&R	
	☐ BZ	☐ Def	☒ Fin	☐ OCW	☒ V&J	☐ BH&OS		
Omschrijving geschilpunten								

Contactpersonen

	Contactpersoon 1	Contactpersoon 2
Naam *		
Afdeling *	Identiteit	Programma Identiteit op orde
Telefoonnummer *		
E-mailadres *	@minbzk.nl	minbzk.nl

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

> Retouradres Postbus 20011 2500 EA Den Haag

Aan [redacted] van de Tweede Kamer
Postbus 20018
2500 EA DEN HAAG

Directoraat-generaal Bestuur en Koninkrijksrelaties
Directie Burgerschap en Informatiebeleid

Turfmarkt 147
Den Haag
Postbus 20011
2500 EA Den Haag
www.rijksoverheid.nl

[redacted]

Uw kenmerk

Datum 11 december 2013
Betreft Kabinetsvisie aanpak identiteitsfraude - 'Slim voorkomen, vlot herstellen'

Op 10 april 2013 had ik overleg met de vaste commissie voor Binnenlandse Zaken over de toekomstbestendigheid van de identiteitsinfrastructuur. De deelnemers aan dat overleg deelden het besef dat identiteitsfraude een serieus en groeiend probleem is. Er was steun voor de gepresenteerde maatregelen. Tegelijkertijd bestond het beeld dat de aanpak wat gefragmenteerd was. Met deze brief wil ik namens het kabinet een integrale visie op de aanpak van identiteitsfraude delen met uw Kamer. Deze visie hangt samen met de Rijksbrede aanpak van fraude, waarover u door de minister van V&J wordt geïnformeerd. Het kabinet biedt u deze visie op de aanpak van identiteitsfraude samen aan met de eerste monitor 'Identiteit in Cijfers'. Doel is om die monitor jaarlijks op te stellen, om een altijd actueel en met de jaren steeds scherper inzicht te hebben in ontwikkelingen op het gebied van identiteit en identiteitsfraude.

Visie in het kort – slim voorkomen, vlot herstellen
Het kabinet heeft een toekomst voor ogen waarin alerte en goed geïnformeerde burgers en organisaties zich uitstekend weten te weren tegen pogingen tot identiteitsfraude. Identiteitsfraudeurs stuiten op een hecht web van actuele kennis en slimme technologische toepassingen. En áls ergens een identiteitsfraudeur toeslaat, dan wordt dit vroeg ontdekt en met vereende krachten vlot verholpen.

Voorkomen en herstellen van identiteitsfraude vraagt om een integrale, informatie gestuurde aanpak waarin partners in publieke en private sector de krachten samenballen[1]. Grote organisaties en zware ketens zijn kwetsbaar tegenover de kleine, creatieve, wendbare dadergroepen die hen bestoken en makkelijk van aanvalsstrategie kunnen veranderen. Het antwoord op identiteitsfraude komt van moderne netwerken die snel reageren en slim anticiperen op identiteitsfraude.

Preventie staat voorop. Voorkomen is beter dan genezen. Dat vraagt vooral om hogere barrières tegen de snel toenemende identiteitsfraude in de digitale wereld. Het beoogde eID-stelsel moet hier een verbetering leveren. Ook zijn betrouwbare ijkpunten van de identiteitsinfrastructuur nodig: zorgvuldige controles op cruciale momenten, in face-to-face contacten tussen overheid en burgers. Daarnaast moet met het oog op preventie én detectie de kennis over daders en hun methoden beter worden gedeeld.

[1] Europol pleit in haar Threat Assessment Internet Facilitate Organised Crime IOCTA, File nr: 2530-264 (pag 8) uit 2011 nadrukkelijk voor publiek en private samenwerking.

Aanleiding - structurele maatschappelijke schade

Identiteit is goud waard. Wie zich op betrouwbare wijze kan identificeren, heeft toegang tot een snel groeiend aanbod van diensten en producten wereldwijd en weet zich gezekerd van de rechten die verbonden zijn aan woonstaat en nationaliteit. De meeste mensen gaan hier eerlijk mee om. Maar de stijgende waarde van identiteitsgegevens en het groeiende aantal mogelijkheden om identiteitsgegevens te bemachtigen trekt wereldwijd fraudeurs aan.

Identiteitsfraude is modus operandi bij veel verschillende vormen van illegale en criminele activiteiten, zoals illegale grenspassage, illegale arbeid, mensensmokkel[2], drugshandel, terrorisme, witwassen van geld en vele typen fraude. Identiteitsfraude maakt daders ongrijpbaar of laat verkeerde mensen opdraaien voor een sanctie. Ze brengt de overheid financiële schade toe: voorzieningen worden verleend aan mensen die daar geen recht op hebben. Ook bij fraude tussen burgers onderling of tussen burgers en bedrijfsleven speelt identiteitsfraude een grote rol: uit het recente Nationaal Dreigingsbeeld blijkt dat in 80% van alle fraudegevallen gericht tegen burgers, bedrijfsleven en financiële instellingen sprake is van enige vorm van misbruik van identiteiten. Bijna 2 miljoen Nederlanders zijn tussen 2007 en 2012 slachtoffer geweest van enige vorm van identiteitsfraude[3]. Zij hebben naar schatting 2,8 miljard euro schade geleden[4]. Ook de emotionele impact kan ingrijpend zijn voor slachtoffers, net als de reputatieschade die zij ondervinden.

Identiteitsfraude berokkent de samenleving structurele schade en zal dat bij verdere toename nog sterker gaan doen. Ze ondermijnt het vertrouwen in de financiële instellingen, tast de betaalbaarheid van voorzieningen aan en kan leiden tot een vermindering van het maatschappelijke draagvlak voor sociale voorzieningen en tot aantasting van het rechtsgevoel. Ingrijpende incidenten in de digitale dienstverlening kunnen wantrouwen losmaken tegenover de digitale economie en de digitale overheid. En de relatie tussen een persoonlijk profiel en geautomatiseerde handelingen van apps, robots en op termijn zelfs elektronische implantaten brengt uiteenlopende gezondheids- en veiligheidsrisico's met zich mee. Een betrouwbare en sterk beveiligde identiteit wordt in de toekomst een kwestie van levensbelang.

Aanpak vandaag – veel initiatieven, meer samenwerking nodig

Voor het voorkomen van identiteitsfraude en het herstellen van de schade die erdoor ontstaat zijn betrouwbare identiteitsinfrastructuren nodig die het mensen mogelijk maken om hun identiteit (of aspecten daarvan) voor anderen op een verifieerbare wijze kenbaar te maken, om de door anderen geclaimde identiteit (of relevante aspecten daarvan) te verifiëren en om in het geval van misbruik vast te stellen wie erachter zit, waar en wanneer misbruik heeft plaatsgevonden, hoe de gevolgen van misbruik kunnen worden hersteld en hoe verdere gevolgen kunnen worden voorkomen.

Dergelijke identiteitsinfrastructuren worden ontwikkeld door diverse private en

[2] Uit de Criminaliteitsbeeldanalyse Mensensmokkel 2012 bleek dat misbruik van identiteits- en verblijfsdocumenten de meest voorkomende modus operandi is van mensensmokkelaars.
[3] Bron: PWC 2013. Recenter onderzoek van het CBS bevestigt dit beeld: in 2012 waren bijna 370.000 mensen slachtoffer van fraude bij aan- of verkopen via internet. Dat komt neer op drie procent van de Nederlandse bevolking van 15 jaar en ouder.
[4] Bron: Update onderzoek 'Omvang van identiteitsfraude en maatschappelijke schade in Nederland', PWC, juni 2013

publieke partijen, zoals bijvoorbeeld banken die hun klanten voorzien van een rekeningnummer, bankpas en identifier en een veilige omgeving voor online bankieren, of ziekenhuizen die medische en administratieve gegevens van hun patiënten veilig bewaren en patiënten een pas met foto meegeven voor identificatie. Kenmerkend voor Nederland is dat veel van deze infrastructuren zijn gebaseerd op de identiteitsinfrastructuur die door de overheid wordt onderhouden, met als kernelementen de Gemeentelijke Basisadministratie (GBA), het Burgerservicenummer (BSN), paspoort, ID-kaart, rijbewijs en DigID en voor buitenlanders die naar Nederland komen de Basisvoorziening voor Vreemdelingen (BVV) en een verblijfsdocument.

Zowel de overheid als private partijen werken permanent aan verbeteringen van hun identiteitsinfrastructuren en het beheer en gebruik ervan[5], vanuit de soms niet eenvoudig te verenigen perspectieven van betrouwbaarheid, privacy, gebruikersgemak en efficiëntie. Tegenover hen staan fraudeurs, die met steeds geraffineerdere methoden kwetsbare plekken in de identiteitsinfrastructuren vinden. Aan beide zijden worden steeds nieuwe methoden en technieken ontwikkeld en toegepast; bedreiging en beveiliging zijn in een permanente wedloop met elkaar verwikkeld. Identiteitsfraudeurs en de 'facilitators' die hen bedienen zijn doorgaans goed geïnformeerd, innovatief en technisch competent. Ze opereren als criminele organisaties over landsgrenzen heen. Daarbij hebben ze het verrassingselement aan hun zijde: de keuze waar, hoe en wanneer ze toeslaan. Als de preventie of opsporing op één plek wordt versterkt, wijzigen ze makkelijk van aanvalsstrategie.

Het aantal plekken waar identiteitsfraudeurs kunnen toeslaan neemt toe. Er is vooral een sterke toename van fraude in de digitale wereld. Het potentieel voor voorkomen en herstellen van identiteitsfraude dat daar tegenover staat, wordt nog onvoldoende ontsloten. Gelukkig komt identiteitsfraude steeds beter in beeld, veel organisaties en sectoren nemen maatregelen en er is een ontwikkeling gaande richting meer samenwerking. Dat zijn drie positieve uitgangspunten waarop het kabinet zijn visie baseert voor een integrale aanpak van identiteitsfraude.

Gezamenlijke verantwoordelijkheid - burgers, bedrijfsleven en overheid
We mogen niet verwachten dat identiteitsfraude ooit is uit te bannen. Het is net als met gezondheid. Mensen zijn door de eeuwen heen altijd en overal wel bestookt door ziektekiemen – oude bekende of nieuwe. We ontwikkelen daar generatie op generatie een steeds sterkere weerstand tegen. Maar vroeg of laat wordt iedereen wel eens getroffen. Het is dan belangrijk om er op tijd bij te zijn en de juiste behandeling toe te passen. Zo is het ook met identiteitsfraude. Er zijn altijd wel criminelen op zoek naar kwetsbare plekken in het systeem – met oude en nieuwe methoden. De meeste mensen en organisaties ontwikkelen er een gezonde weerstand tegen door voorzichtig om te gaan met gegevens en door steeds betere technieken en methoden te benutten. Maar iedereen kan wel eens slachtoffer worden van identiteitsfraude. Dan is het zaak om de fraude zo snel mogelijk te detecteren en adequaat te behandelen.

Burgers, overheid en bedrijfsleven hebben een gezamenlijke verantwoordelijkheid voor het voorkomen en herstellen van identiteitsfraude. Burgers moeten er zelf voor zorgen dat ze een gezonde weerstand hebben tegen pogingen tot identiteitsfraude, door voldoende waakzaam te zijn en door de beschikbare

[5] De bijlage geeft een analyse die tot deze visie heeft geleid, met o.a. maatregelen in diverse sectoren.

middelen – zoals beveiligingssoftware – op de juiste manier te gebruiken. Zij zijn ook de eersten die in actie moeten komen als ze slachtoffer zijn van identiteitsfraude, of een poging daartoe.

Datzelfde geldt voor organisaties, in publieke en private sector: zij zijn zelf verantwoordelijk voor een gezonde weerstand tegen identiteitsfraude. Van organisaties mag daarnaast worden verwacht dat ze hun klanten zo goed mogelijk beschermen tegen identiteitsfraude, door zorgvuldig om te gaan met het verwerven, beveiligen en gebruiken van persoonsgegevens, door verzoeken om correctie en verwijdering van gegevens adequaat te behandelen en door klanten actief te voorzien van informatie en middelen om identiteitsfraude te voorkomen.

De rol van de overheid bij het voorkomen en herstellen van identiteitsfraude: zij zorgt online en offline voor een robuuste identiteitsinfrastructuur met betrouwbare ijkpunten: contactmomenten tussen burgers en overheid waarin goed opgeleide professionals met hulp van geavanceerde apparatuur een identiteit met de grootst mogelijke zekerheid vaststellen, registreren en verifiëren. De overheid borgt een aantal elementaire identificerende gegevens voor alle Nederlanders en iedereen die in Nederland verblijft. De overheid stelt heldere richtlijnen vast voor de veiligheid en betrouwbaarheid van particuliere identiteitsinfrastructuren en identificatiemiddelen en voor de begeleiding van slachtoffers van identiteitsfraude en -fouten. De overheid werkt samen met het bedrijfsleven en maatschappelijke organisaties aan een integrale aanpak van identiteitsfraudeurs. En de overheid monitort voortdurend de ontwikkelingen in de wereld van identiteitsfraude en verkent de grenzen van de bestrijding van deze groeiende tak van misdaad, samen met experts in publieke en private sector in binnen- en buitenland.

De visie in vijf beleidslijnen - gezamenlijke aanpak van identiteitsfraude
Burgers, overheid en bedrijfsleven staan het sterkst wanneer zij samen optrekken tegen identiteitsfraude. In de eerste plaats gaat het om het beter en breder benutten van kennis, technieken en methoden. In de tweede plaats gaat het om het beter op elkaar afstemmen van nieuwe maatregelen die door diverse partijen in publieke en private sector getroffen worden. In de derde plaats gaat het om het afspreken van een gezamenlijke richting voor ontwikkelingen op de lange termijn. Het kabinet onderscheidt daarbij vijf samenhangende beleidslijnen:

1. Gezonde weerstand
Voorkomen is beter dan genezen. De preventie van identiteitsfraude moet permanent evolueren met nieuwe vormen van bedreiging. Kennis en alertheid zijn sleutelfactoren, gedragen door bewustwordingscampagnes en fraude-alerts. Bundeling van initiatieven uit publieke en private sector moet de algehele preventie versterken, doordat kennis en informatie een bredere doelgroep bereiken en doordat geldende regels en beschikbare middelen langs verschillende wegen onder de aandacht worden gebracht.

De menselijke factor zal op termijn echter niet voldoende blijken tegenover de steeds ingrijpender impact van identiteitsfraude. Er zullen zeker veel mensen zijn die zich met de meest actuele kennis en middelen goed weten te weren tegen identiteitsfraudeurs, maar er zullen ook altijd mensen zijn die daar niet of beperkt toe in staat zijn. Daarom wil het kabinet de weerstand tegen identiteitsfraude op termijn zo goed mogelijk 'hard' organiseren: zo hoog mogelijke fysieke barrières opwerpen tegen identiteitsfraude.

Dat begint bij het minimaliseren van het gebruik van identificerende gegevens en bij het veilig bewaren ervan. Op beide punten gaan het borgen van privacy en het voorkomen van identiteitsfraude hand in hand. Overheid en bedrijfsleven zijn gebonden aan het principe van dataminimalisatie[6]. Dat principe geeft aan dat persoonsgegevens slechts mogen worden verwerkt als daartoe een noodzaak bestaat. Het principe is leidend bij het registreren en bewaren van gegevens in systemen. Bij de rijksdienst bijvoorbeeld wordt met het toetsmodel privacy impact assessment beoordeeld of systemen zo worden gebouwd dat er zo min mogelijk persoonsgegevens in worden opgeslagen en bewaard. De campagne 'laat je niet zomaar kopiëren' was een invulling van het dataminimalisatieprincipe voor kopietjes van identiteitsbewijzen. De ID-cover van de NVVB (Nederlandse Vereniging voor Burgerzaken) is daar een slim en praktisch hulpstuk bij. De digitalisering van de dienstverlening van overheid en bedrijfsleven en de toenemende betrouwbaarheid van digitale verificatie- en autorisatieprocessen zorgen ervoor dat kopietjes van identiteitsbewijzen en papieren correspondentie in de toekomst minder nodig zijn, waardoor criminelen minder kans maken om aan identiteitsgegevens te komen door kopietjes te bemachtigen of in brievenbussen te vissen. Voor wat betreft het veilig bewaren van gegevens is op termijn winst te boeken met het compartimenteren van identiteiten[7] en het enkelvoudig en waar nodig versleuteld opslaan van gegevens: hackers hebben minder kansen naarmate identiteitsgegevens op minder plaatsen zijn opgeslagen. Dat is technisch mogelijk door niet dezelfde gegevens in veel verschillende systemen te bewaren, maar slechts op één goed beveiligde plek, met voor verschillende partijen een beveiligde toegang tot per situatie verschillende deelverzamelingen van die gegevens. De BRP zet met de enkelvoudige opslag van gerelateerde persoonsgegevens een belangrijke stap in die richting.

Tegelijkertijd moet er rekening mee worden gehouden dat er altijd wel gegevens in handen komen van kwaadwillenden en dat niet is na te gaan hoeveel gegevens er al in het criminele circuit bekend zijn. Hackers voorspellen dat alle gegevens die in databases zijn opgeslagen op een dag gehackt kunnen worden – zij het op afstand, zij het door handlangers aan de bron. En het is een feit dat de virtuele wereld niet aan geheugenverlies lijdt: eenmaal verstrekte gegevens verspreiden zich snel en laten zich moeilijk vernietigen. Daarom wil het kabinet richting een situatie waarin de combinatie van naam, adres, Burgerservicenummer en andere persoonsgegevens nergens nog voldoende is voor het plegen van identiteitsfraude. Dat kan door in de toekomst bij controles altijd te vragen om een persoonlijke 'sleutel' die fraudeurs moeilijk kunnen bemachtigen. Het eID-stelsel zal daar een belangrijke bijdrage aan leveren.

Een goede persoonlijke sleutel bestaat uit slimme en voor de situatie voldoende betrouwbare toepassingen van de drie-eenheid '*wie je bent, wat je weet en wat je hebt*'. Het hoogste betrouwbaarheidsniveau – online en offline – bestaat uit een combinatie van een betrouwbaar fysiek middel (*wat je hebt;* bijvoorbeeld een pas met een chip en een identifier of smart phone), tweestapsverificatie (*wat je weet;* bijvoorbeeld met een dubbel wachtwoord, pincode, sms of een persoonlijke vraag-

[6] De Wbp legt het principe van dataminimalisatie neer. Persoonsgegevens mogen slechts worden verwerkt als daarvoor een noodzaak bestaat (art 8). Art. 11, lid 1 bepaalt daarnaast dat persoonsgegevens slechts mogen worden verwerkt voor zover zij, gelet op de doeleinden waarvoor zij worden verzameld of vervolgens worden verwerkt, toereikend, ter zake dienend en niet bovenmatig zijn (relevantie-eis). Verder is van belang dat verwerking van gevoelige persoonsgegevens in principe verboden is (art. 16-23 Wbp), en slechts onder strikte(re) voorwaarden is toegestaan.

[7] Het principe van compartimenteren van identiteiten is vergelijkbaar met het compartimenteren van olietankers: als er midscheeps een gat ontstaat, stroomt niet meteen de hele tanker leeg.

antwoordcombinatie) en biometrische kenmerken (*wie je bent*; bijvoorbeeld stem- of gelaatsherkenning). Veel landen verkennen nieuwe technieken en concepten. Datzelfde geldt voor innovatieve trendsetters als Apple, Google en Facebook. Het kabinet wil goed luisterend naar het maatschappelijke debat over dit thema onderzoeken hoe nieuwe technologie in uiteenlopende situaties optimaal ingezet kan worden voor het voorkomen van identiteitsfraude, het beschermen van privacy, het vergroten van de mogelijkheden voor burgers om zelf gegevens te beheren en delen en het bevorderen van economische kansen voor Nederland.

2. Betrouwbare controles

Een goede en efficiënte dienstverlening in publieke en private sector is slechts mogelijk dankzij betrouwbare identiteitsgegevens. Dat betekent voor veel instanties zoveel als een paradigmawijziging – zeker in een context van vergaande digitalisering van de dienstverlening: door de identiteit van burgers op de juiste momenten zorgvuldig te controleren, leveren organisaties grote winst op voor heel het maatschappelijk en economisch verkeer, doordat die controles ruimte scheppen voor efficiënte dienstverlening en burgers beschermen tegen identiteitsfraude. Zorgvuldige controles bedienen de burgers.

Dat vraagt om een investering in de 'ijkpunten' van de Nederlandse identiteitsinfrastructuur: face-to-face contacten tussen burgers en overheid waarbij goed opgeleide professionals met hulp van geavanceerde apparatuur een identiteit met de grootst mogelijke zekerheid vaststellen, registreren en verifiëren. Een belangrijk initiatief in die richting is het programma 'Naar betrouwbare persoonsgegevens' van de NVVB, dat zich richt op de ontwikkeling van kennis en vaardigheden van ambtenaren burgerzaken.

Ook een regionale concentratie van kennis en apparatuur, met ondersteuning van landelijke expertisecentra, kan de ijkpunten van de identiteitsinfrastructuur naar een hoger betrouwbaarheidsniveau tillen. In Oost-Nederland is positief gereageerd op een voorstel van de burgemeesters van Enschede, Apeldoorn en Zwolle om samen te werken aan de inschrijving in de GBA.

Het kabinet wil onderzoeken op welke slimme manieren extra controles kunnen worden toegepast bij het verstrekken van overheidsmiddelen en onder welke omstandigheden de overheid bepaalde identiteitsmiddelen kan intrekken. Om fraudeurs niet in de kaart te spelen is het van belang ook aandacht te besteden aan minder voorspelbare identiteitscontroles.

Op termijn moeten partijen met actuele kennis over identificerende gegevens een betere plek krijgen in het beheer en de validatie van gegevens die voor veel partijen van belang zijn. Dat geldt zowel voor identiteitsvaststelling bij geboorte en immigratie, als voor identiteitsverificatie bij emigratie en overlijden, als voor correctie van gegevens wanneer registraties onjuist blijken. Het gaat hier om het beter benutten van specifieke kennis en kunde van onder andere gemeenten, politie, Koninklijke Marechaussee, IND, buitenlandse posten, Belastingdienst, zorginstellingen en financiële dienstverleners.

3. Vroege diagnose

Een vroege diagnose van gevallen van identiteitsfraude is van groot belang om snelle behandeling mogelijk te maken en om verspreiding te voorkomen. Opgave voor de betrokkenen van de diverse disciplines is om als netwerk te opereren en

om integrale defensiestrategieën te ontwikkelen en implementeren. Dat moet op een manier gebeuren die beantwoordt aan de creativiteit en wendbaarheid van criminele organisaties en hun internationale speelveld.

Er zijn al diverse initiatieven tot interdisciplinaire samenwerking, zoals bij het Centrum voor Informatiebeveiliging en Privacy (CIP) onder regie van het UWV, de infobox Crimineel en Onverklaarbaar Vermogen (iCOV), de te vormen expertisegroep fraudebestrijding onder regie van de Belastingdienst en de samenwerking tussen de Nationale Politie en de Koninklijke Marechaussee in de oprichting van vreemdelingenpolitieloketten en ID-desks. Dat zijn grote stappen die de 'intelligence' versterken vanwaaruit identiteitsfraude en andere vormen van fraude kunnen worden bestreden. De Ministeriële Commissie Fraude is in het leven geroepen voor een integrale aanpak van fraude met overheidsmiddelen.

De crux voor een vroege diagnose is het goed registeren van identiteitsfraude, het stapelen van casussen, het herkennen van patronen en het doorrechercheren op onregelmatigheden in het gedrag van groepen of individuen. Voorwaarde daarvoor is dat gegevens of indicatoren voor mogelijke fraude die de overheid of andere organisaties beschikbaar hebben met de juiste partijen worden gedeeld, met waarborgen voor privacy en voor rechtsbeginselen als het non-discriminatiebeginsel, gelijkheidsbeginsel en verbod op willekeur en met waarborgen tegen 'false positives' (de onterechte veronderstelling dat iemand fraudeert). De aanpak hiervan staat beschreven in de Rijksbrede antifraudestrategie die de minister van V&J u zal toezenden.

4. Adequate behandeling

Voor slachtoffers is het van belang dat zij zich erkend voelen in hun probleem, dat zij beschermd worden tegen hernieuwd slachtofferschap en dat zij ondersteuning krijgen bij aangifte en bij schadeloosstelling en herstel. Van de eerste aangifte van identiteitsfraude bij de politie tot het geheel oplossen van de zaak wil het kabinet dat de slachtoffers centraal staan.

Belangrijkste is dat de schade zich niet verder verspreidt. Dat is mogelijk door het direct ontwaarden van gestolen (of verloren) identificatiemiddelen: slachtoffers moeten hun identiteitsdocumenten, pasjes en digitale identiteiten onmiddellijk kunnen blokkeren en instanties kunnen oproepen tot verhoogde alertheid op hun gegevens. Ook moet online verifieerbaar zijn welke identiteitsdocumenten geldig en welke ongeldig zijn. Repressie haakt hier in op preventie.

Iedere instantie in publieke en private sector heeft zelf de verantwoordelijkheid om slachtoffers van fraude (en fouten) te helpen door foutieve of gecorrumpeerde gegevens te verwijderen of te corrigeren. Wanneer het probleem zich verspreidt over meerdere administraties, moet herstel vanuit het netwerk komen. Dat vraagt om maatwerk: de beste methode is dat afgevaardigden van betrokken instanties samen aan tafel zitten om een probleem op te lossen. Voor schrijnende gevallen is er hulp van het Centraal Meld- en Informatiepunt Identiteitsfraude en -fouten (CMI) en de Fraudehelpdesk. Het kabinet zet in op een geïntensiveerde samenwerking tussen het CMI, Fraudehelpdesk en andere organisaties die er zijn om slachtoffers te helpen.

Voor de publieke sector geldt dat ruim 600 organisaties gebruik maken van de Gemeentelijke Basisadministratie (GBA). Cruciaal voor een adequate behandeling van identiteitsfraude is dan ook dat burgers op tijd signaleren wanneer er iets loos

is met hun gegevens in de GBA en dat fouten vlot hersteld worden. Het kabinet roept burgers op om er zelf voor te zorgen dat hun gegevens in de GBA kloppen, wat in 2013 is onderstreept met de campagne 'Voorkom gedoe, kijk het na'.

Op de lange termijn moet het spreiden van de gevolgen van fraude en fouten voorkomen worden door de eerder genoemde enkelvoudige opslag van gegevens.

5. Effectieve repressie

Bij de bestrijding van identiteitsfraude zijn het opwerpen van barrières en een verhoogde alertheid van private en publieke partijen in het handelsverkeer van doorslaggevend belang. Een effectieve en gerichte aanpak van fraudeurs vraagt om een verbinding tussen het strafrecht en andere vormen van handhaving, toezicht en nalevingsbevordering. Op die manier is er sprake van meer afgestemde en integrale handhaving waarin het strafrecht tijdig en situationeel wordt ingezet. De minister van V&J gaat hier in zijn antifraudebrief nader op in.

Bij een effectieve repressie van identiteitsfraude mag niet vergeten worden dat misbruik van identiteiten overwegend een faciliterende handeling is om een delict te plegen. Identiteitsfraude is geen doel op zich, maar een middel, wat ook uit de gehanteerde definitie voortvloeit. De aanpak van identiteitsfraude staat dan ook niet op zichzelf, maar maakt deel uit van de aanpak van criminaliteitsfenomenen waarbij identiteitsfraude modus operandi is.

Fraude met identiteitsdocumenten is strafbaar volgens artikel 231 van het Wetboek van Strafrecht[8]. Fraude met identificerende persoonsgegevens (bijvoorbeeld het aannemen van een valse naam of een valse hoedanigheid) vormt onderdeel van meer algemene delictsomschrijvingen als oplichting (artikel 326 Sr), flessentrekkerij (artikel 326a Sr) en bedreiging (artikel 284 e.v. Sr)[9]. Voorts kent het Wetboek van Strafrecht specifieke strafbaarstellingen voor de aanpak van misdrijven waartoe fraude met identificerende persoonsgegevens vaak de opstap vormt. Bij die misdrijven gaat het bijvoorbeeld om mensensmokkel, witwassen, bank- of uitkeringsfraude, terrorisme of drugs- en wapengerelateerde misdrijven.

Strenge repressiemaatregelen moeten in combinatie met stevige preventiemaatregelen een afschrikkende werking vormen: bij potentiële fraudeurs moet het verhaal rondgaan dat identiteitsfraude in Nederland een onbegonnen zaak is.

[8] Wetboek van Strafrecht, Artikel 231: "1. Hij die een reisdocument valselijk opmaakt of vervalst, of een zodanig stuk op grond van valse gegevens doet verstrekken dan wel een aan hem of een ander verstrekt reisdocument ter beschikking stelt van een derde, met het oogmerk het door deze te doen gebruiken als ware het aan hem verstrekt, wordt gestraft met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie. 2. Met dezelfde straf wordt gestraft hij die in het bezit is van een reisdocument waarvan hij weet of redelijkerwijs moet vermoeden, dat het vals of vervalst is, dan wel opzettelijk gebruik maakt van een niet op zijn naam gesteld reisdocument."

[9] Voetnoot: wetsvoorstel wijziging van het Wetboek van Strafrecht en de Wegenverkeerswet 1994 in verband met de verbetering van de aanpak van fraude met identiteitsbewijzen en wijziging van het Wetboek van Strafvordering, de Beginselenwet justitiële jeugdinrichtingen en de Wet DNA-onderzoek bij veroordeelden in verband met de verbetering van de regeling van de identiteitsvaststelling van verdachten en veroordeelden (33352). Dit wetsvoorstel voorziet erin dat meer fraudeleuze gedragingen met identiteitsbewijzen strafbaar worden gesteld. Voorst wordt hiermee misbruik van identificerende persoonsgegevens afzonderlijk strafbaar gesteld en meer op één lijn gesteld met misbruik van reisdocumenten en identiteitsbewijzen waarvoor artikel 231 van het Wetboek van Strafrecht wel een aparte strafbaarstelling kent.

Internationale aanpak
Een integrale aanpak van identiteitsfraude op Europees niveau is nog veel complexer dan een aanpak met Nederlandse partners: de lidstaten hebben alle hun eigen historie van vaststellen, registreren en verifiëren van persoonsgegevens en daaruit zijn heel verschillende wetten, regels, systemen en middelen voortgevloeid. Het spreekt voor zich dat de aanpak op mondiaal niveau nog complexer is.

Toch is een internationale aanpak cruciaal voor preventie en bestrijding van identiteitsfraude. De georganiseerde misdaad kent geen grenzen. Hoe sterk ook de nationale aanpak, via kwetsbare plekken in andere landen blijven de gevolgen van identiteitsfraude Nederland bereiken. Daarnaast zijn internationaal opererende dadergroepen niet te bereiken met een nationale aanpak. Het grensoverschrijdende karakter van identiteitsfraude – in het bijzonder in de digitale wereld - levert grote uitdagingen op voor Europese en internationale samenwerking. Het kabinet pleit daarom voor intensiveren van de samenwerking op EU-niveau voor het voorkomen en bestrijden van identiteitsfraude.

Uitvoeringsagenda aanpak identiteitsfraude
De visie die u in deze brief is voorgelegd zal worden uitgewerkt in een uitvoeringsagenda Aanpak Identiteitsfraude. Die agenda zal recht doen aan de vele initiatieven die al worden genomen in de aanpak van identiteitsfraude. Het gaat dan zeker om de initiatieven waarbij deskundigen van verschillende disciplines en sectoren elkaar opzoeken om samen te leren en samen zaken aan te pakken – regionaal, nationaal en internationaal. Het zijn dergelijke verbeteringen die het netwerk van fraudebestrijders het fijnmazige karakter geven dat nodig is om fraudeurs te slim af te zijn. Wanneer vanuit de visie nieuwe maatregelen voortvloeien waarvoor nog geen middelen zijn voorzien in de begroting(en), worden business cases opgesteld. De business cases worden getoetst voordat besloten wordt of de maatregelen worden getroffen.

Voor de zomer van 2014 zal het kabinet u een voorstel voor deze uitvoeringsagenda sturen. Het kabinet hecht eraan hierbij het belang van het verbreden van de visie en het uitwerken van een uitvoeringsagenda in publiek-private samenwerking te benadrukken, net als de hoofdrol die burgers zelf vervullen bij de aanpak van identiteitsfraude.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,

dr. R.H.A. Plasterk

Bijlage bij de kabinetsvisie op de aanpak van identiteitsfraude

Definities identiteit en identiteitsfraude

Er bestaan veel definities van identiteitsfraude – nationaal en internationaal[1]. Dat maakt het lastig om de problemen gerelateerd aan identiteitsfraude en de aanpak ervan eenduidig in kaart te brengen. Het kabinet geeft in deze visie een brede uitleg aan het begrip identiteit:

> Een *identiteit* is een verzameling eigenschappen waarmee een individu zich onderscheidt van anderen. Die verzameling kan in diverse situaties anders van samenstelling zijn, met natuurlijke (of biometrische) eigenschappen (zoals geslacht, lengte, gewicht, stem en de structuur van gelaat, ogen, oren, handen, huid en DNA), eigenschappen die het 'verhaal' van iemand vertellen (zoals naam, geboortedatum, familie, opleiding, werk en hobby's, maar ook voorkeur voor winkels en muziek, online surfgedrag en politieke kleur) en eigenschappen met een administratieve waarde (zoals BSN, adres en bankrekeningnummer).

In 2007 introduceerde het WODC een definitie van identiteitsfraude[2] waaronder alle vormen van criminaliteit vallen waarbij iemand met kwade bedoelingen bewust de schijn oproept van een identiteit die niet bij hem hoort, daarbij gebruik makend van de identiteit van een bestaande of gefingeerde persoon. Het kabinet sluit in deze visie aan bij die definitie:

> *Identiteitsfraude* is het opzettelijk (en) (wederrechtelijk of zonder toestemming) verkrijgen, toe-eigenen, bezitten of creëren van valse identificatiemiddelen en het daarmee begaan van een wederrechtelijke gedraging of: met de intentie om daarmee een wederrechtelijke gedraging te begaan.

Het begrip identificatiemiddelen moet hier breed worden uitgelegd: ook bijvoorbeeld het verhaal waarmee een fraudeur zich voordoet als verkoper van een bedrijf geldt als identificatiemiddel, of een kostuum dat de indruk moet wekken dat iemand een bepaalde functie bekleedt, of een e-mailaccount of een website onder de naam van iemand anders.

Analyse: steeds kwetsbaarder voor identiteitsfraude

Particulieren, overheden en bedrijfsleven worden steeds kwetsbaarder voor identiteitsfraude. Belangrijkste oorzaken:

1. *Het aantal kwetsbare plekken waar fraudeurs kunnen toeslaan neemt toe.*
2. *Daders kennen geen grenzen en gebruiken steeds geraffineerdere methoden.*
3. *Het potentieel voor voorkomen en herstellen wordt onvoldoende ontsloten.*

1. Het aantal kwetsbare plekken waar fraudeurs kunnen toeslaan neemt toe.

In Nederland bestaat een algemeen gebrek aan alertheid voor identiteitsfraude. Het zit niet in de Nederlandse omgangsvormen om de identiteit van een ander te wantrouwen. Niet aan de deur, niet aan de telefoon, niet in de winkel of aan de balie. Een zorgvuldige controle van een identiteitsbewijs wordt al gauw als onvriendelijk ervaren. Ook in situaties waar een bepaalde mate van professionele waakzaamheid functioneel kan zijn. Dat levert veel plekken op waar fraudeurs kunnen toeslaan.

Dat gebrek aan alertheid maakt burgers, bedrijven en overheidsinstanties kwetsbaar voor identiteitsfraude. Meer dan een miljoen mensen hebben professioneel te maken met het vaststellen, registreren en verifiëren van persoonsgegevens (bij gemeenten, IND, politie, Koninklijke Marechaussee, banken, uitzendbureaus, verzekeringsorganisaties, ziekenhuizen, kamer van koophandel, notarissen, horeca, beveiligingsbedrijven, et cetera). Behalve alertheid zijn ook kennis en vaardigheden in veel sectoren onvoldoende aanwezig. En waar kennis aanwezig is, is zij vaak moeilijk te borgen door de mobiliteit van medewerkers. Het gaat hier om kennis van documenten en echtheidskenmerken, van 'look-alike fraude' (het gebruik van een document door iemand die lijkt op de rechtmatige documenthouder) en van de verschillende (veranderende) fraudevormen. Daarnaast ontbreken op veel plaatsen vaak de nodige technische hulpmiddelen en de steun van een gespecialiseerd backoffice. Ook staat identiteitsverificatie onder druk van eisen aan dienstverlening (snelheid, klantvriendelijkheid).

[1] De diverse landen, VN en OECD hanteren verschillende definities.
[2] Deze definitie is afkomstig uit het onderzoek 'Identiteitsfraude, een afbakening; een internationale begripsvergelijking en analyse van nationale strafbepalingen' dat de Universiteit Utrecht in 2007 in opdracht van het WODC heeft gehouden (www.wodc.nl/onderzoeksdatabase/identiteitsfraude.aspx?cp=44&cs=6796).

1910888 01409

Het aantal plekken waar fraudeurs kunnen toeslaan neemt vooral toe door het toegenomen internetgebruik. Miljoenen Nederlanders zijn steeds actiever aanwezig in de online wereld. Openheid is de norm. "Ik deel, dus ik besta." Dat leidt tot een toename van mogelijkheden voor fraudeurs om identiteitsgegevens te vergaren en te misbruiken. Via Google en Facebook, bijvoorbeeld, kunnen fraudeurs nauwkeurige profielen opstellen om mee aan de haal te gaan.

Ook de overheid en private partijen zijn steeds actiever in de digitale wereld. "Digitaal waar mogelijk, persoonlijk waar nodig", in de benadering van de Manifestgroep[3]. Digitale dienstverlening prikkelt tot slimmer en zuiniger werken en biedt uitstekende kansen voor economische groei. Het kabinet zet dan ook in op vergaande digitalisering van de dienstverlening van de overheid in 2017 en heeft met de EU een ambitieuze digitale agenda. Maar digitalisering van de dienstverlening creëert ook nieuwe openingen voor fraudeurs.

2. Daders kennen geen grenzen en gebruiken steeds geraffineerdere methoden.
Identiteitsfraudeurs en de 'facilitators' die hen bedienen zijn doorgaans goed geïnformeerd, innovatief en technisch competent. Ze opereren als criminele organisaties over landsgrenzen heen. En als de preventie of opsporing op één plek wordt versterkt, duiken ze ergens anders weer op.

Het zoeken naar nieuwe kwetsbare plekken is te zien in de verschuiving van methoden die identiteitsfraudeurs gebruiken. Het vervalsen van reisdocumenten, bijvoorbeeld, is steeds moeilijker geworden. In 1981 stelde de Raad van de Europese Unie een resolutie vast die betrekking heeft op de beveiliging van paspoorten en andere reisdocumenten tegen vervalsingen. Deze resolutie wordt periodiek aangepast. In 2000 is deze resolutie ingrijpend aangevuld. Toen zijn ook minimumveiligheidsnormen opgenomen. Als gevolg van de steeds hogere drempel voor vervalsing van identiteitsdocumenten uit EU-landen duiken nu fraudeurs op die zich richten op de manier waarop documenten worden verstrekt en op look-alike fraude. Jaarlijks worden een kwart miljoen Nederlandse reisdocumenten en rijbewijzen als verloren of gestolen opgegeven. Dat is een groot potentieel voor look-alike fraude alleen al met Nederlandse documenten.

Daarnaast is een verschuiving te zien naar het onder andermans of gefingeerde naam aanvragen van identiteitsdocumenten, bijvoorbeeld door fraude met geboorte- of huwelijksakten: die zijn nauwelijks beveiligd tegen namaak en vervalsing. Er bestaan internationaal ook geen standaards voor. In veel landen worden geboortes bovendien niet geregistreerd, waardoor de deur voor identiteitsfraude – onder andere gerelateerd aan kinderhandel – open staat.

Een veelgebruikte vorm van identiteitsfraude is misbruik van kopieën van identiteitsbewijzen[4]. Via een kopie komen fraudeurs in het bezit van naam, geboortedatum en BSN: op veel plaatsen genoeg om financiële transacties aan te gaan. De methoden om aan persoonsgegevens te komen, zijn gewiekst en brutaal, variërend van vissen in brievenbussen, tot het ensceneren van een sollicitatiegesprek ('vacatureripping') of van de verhuur van een huis.

Er is vooral een steile groeicurve te zien in identiteitsfraude gefaciliteerd door het internet. In 2012 was ongeveer 40 procent van de ondernemers slachtoffer van cybercrime[5]. Ook particulieren worden bestookt met phishing mails, malware/ spyware en hyperlinks naar kopieën van vertrouwde websites (pharming). Met de identiteitsgegevens van een ander, of met valse gegevens, kunnen fraudeurs op afstand zaken doen bij publieke en private instellingen. Daarnaast zijn op online marktplaatsen veel fraudeurs actief onder valse identiteiten. Internetfraude is zeer aantrekkelijk voor criminelen: het is een low-risk crime (misdaad wordt niet in persoon gepleegd, maar via computers), de doelgroep is reusachtig, de pakkans is laag (alleen zichtbaar voor specialisten), fraudeurs kunnen vrij van grenzen opereren en online diensten en toepassingen

[3] De Manifestgroep (MFG) is een informeel samenwerkingsverband van AgentschapNL, Belastingdienst, Centraal Administratiekantoor (CAK), Centraal Bureau voor de Statistiek (CBS), Centraal Justitieel Incassobureau (CJIB), Centrum Indicatiestelling Zorg (CIZ), College van Zorgverzekeringen (CVZ), Dienst Regelingen, Dienst Uitvoering Onderwijs (DUO), Immigratie- en Naturalisatiedienst (IND), Kadaster, Kamers van Koophandel (KVK), RDW, Sociale Verzekeringsbank (SVB) en Uitvoering Werknemersverzekeringen (UWV).
[4] Identiteitsfraude met kopieën van identiteitsbewijzen is geanalyseerd in het Bestuurlijk Dossier Identiteitsfraude, OM Parket Noord-Nederland, 2013.
[5] http://www.politie.nl/onderwerpen/cybercrime.html#feiten-en-cijfers

komen steeds met nieuwe versies, die nieuwe kwetsbaarheden hebben, waarover de kennis zich snel verspreidt.

3. Het potentieel voor voorkomen en herstellen wordt onvoldoende ontsloten.
Veel organisaties en sectoren nemen maatregelen tegen identiteitsfraude. Vaak betreft het publieksvoorlichting. De Consumentenbond, internetproviders, banken en een grote groep partners van 'Alert Online' bijvoorbeeld geven burgers en bedrijven tips voor veilig online gedrag. In veel sectoren wordt personeel getraind op het herkennen van identiteitsfraude. Soms worden grootscheeps nieuwe technieken en systemen geïntroduceerd, zoals de overstap met het pinnen 'van strip naar chip' in 2005. En soms levert een slimme truc veel winst op, zoals het standaard blokkeren van bankpassen in landen waar skimmen nog mogelijk is, of het overmaken van 1 cent voor identificatie via de bankrekening bij het afsluiten van een nieuwe telefoonabonnement.

In diverse sectoren wordt gemonitord op risicopatronen. Webwinkels bijvoorbeeld worden gealarmeerd door opmerkelijk surfgedrag. Creditcardmaatschappijen bellen hun klanten bij een vermoeden van misbruik. Ook bestaan binnen een aantal sectoren registers waarin signalen over incidenten worden gedeeld, zoals het Incidentenwaarschuwingssysteem van financiële instellingen en het Fraude en Informatiesysteem Systeem Holland (FISH) van verzekeraars.

Ook in het publieke domein wordt de aanpak van identiteitsfraude met diverse maatregelen verbeterd. Het Centraal Meld- en informatiepunt voor Identiteitsfraude en -fouten (CMI), de Fraudehelpdesk en het Landelijk Meldpunt Internetoplichting geven voorlichting en helpen slachtoffers bij het doen van aangifte en het oplossen van hun zaak. Binnen de Belastingdienst is de hulp aan slachtoffers van identiteitsfraude sinds anderhalf jaar beter georganiseerd en dankzij een landelijke registratie is het mogelijk patronen te herkennen en daders sneller op te sporen. Het wijzigen van bankrekeningnummers bij de Belastingdienst is veiliger geworden door voorbevestigingen en wordt nog veiliger met de komst van het nieuwe proces "wijzigen bankrekeningnummers" (april 2014). De minister van SZW heeft een pilot aangekondigd met de ID12 pas in de champignonsector, die naar Zweeds voorbeeld inzicht moet verschaffen in wie op welke werkplek werkt en daarmee het toezicht versterkt en zwart werken bemoeilijkt[6]. En er worden voorbereidingen getroffen voor een eID-stelsel: een publiek-privaat stelsel waarbinnen burgers, consumenten en ondernemers zowel publieke als private authenticatiemiddelen gebruiken, waarmee ze veilig online zaken kunnen doen met de overheid en het bedrijfsleven[7].

Veel verbeteringen in de publieke sector hebben te maken met een verbeterde samenwerking tussen verschillende instanties. Het programma Identiteit op Orde heeft met dat doel experts van veel verschillende organisaties bij elkaar gebracht en brengt een kennisplatform van wetenschappers voort. De verschillende overheidsdiensten als de Koninklijke Marechaussee, politie, IND, OM en RDW weten elkaar steeds beter te vinden op het gebied van identiteit en identiteitsfraude, onder andere in regionale samenwerkingsverbanden. Ook landelijke expertisecentra als het Expertisecentrum voor Identiteitsfraude en Documenten (ECID), Expertisecentrum Rijbewijzen, Bureau Documenten, het Nederlands Forensisch Instituut (NFI) en het Expertisecentrum Vreemdelingen en Mensenhandel (ECVM) kijken breder dan het eigen domein. Vanwege het belang van de GBA als noodzakelijk informatiesysteem voor veel overheidstaken is eind 2011 de kwaliteitsagenda GBA gestart om met name de adresgegevens op een zo hoog mogelijk niveau te brengen[8]. Er wordt gebouwd aan de Basisregistratie Personen (BRP), die de actualiteit en kwaliteit van gegevens moet verbeteren en die mogelijkheden moet bieden voor het leggen van verbanden tussen in de GBA geregistreerde personen door enkelvoudige opslag van gerelateerde persoonsgegevens. Er zijn afspraken over koppeling van gegevens van de SVB, het UWV en de Belastingdienst aan de GBA. Gemeenten signaleren afwijkende vestigingspatronen die ook van belang zouden kunnen zijn voor andere gemeenten. Met

[6] Kamerstukken 2013, 29 407, nr. 173
[7] PM verwijzing naar brief aan Kamer over eID stelsel; momenteel in voorbereiding
[8] Deze kwaliteitsagenda heeft als doel om de gemeenten als bijhouders van de GBA en de gebruikers van de gegevens optimaal te ondersteunen bij hun taakuitvoering. Over de vele maatregelen en de stand van zaken heeft BZK bij brieven van 5 juli 2012 en 23 mei 2013 de Tweede Kamer geïnformeerd (Kamerstukken 27 859, nrs. 57, 58, 60 en 65). In de brieven en het debat rond fraude met toeslagen (Kamerstuk 17 050, nr 435) is aangekondigd om de kwaliteitsagenda versterkt in te zetten: de risicoprofielen die zijn ontwikkeld door de gemeenten in relatie tot het inschrijven van personen worden actief gedeeld met alle gemeenten, voorts komt er meer samenwerking in de keten van afnemers van de GBA en is sprake van intensivering van de deskundigheidsbevordering van GBA-ambtenaren.

het programma Identiteitsmanagement en Immigratie (IDMI) is fors geïnvesteerd in de vreemdelingenketen: aangezien identiteit daar van wezenlijk belang is voor het krijgen van een verblijfsvergunning, is in de vreemdelingenketen bij uitstek bijzondere aandacht voor identiteitsfraude, door Koninklijke Marechaussee, IND, Vreemdelingenpolitie en Dienst Terugkeer en Vertrek (DTV). Ook in de strafrechtketen krijgt identiteit bijzondere aandacht: verdachten hebben belang bij identiteitsfraude voor het ontlopen van straf of minder straf doordat relevante antecedenten onder water verdwijnen. Om deze reden is de WIVVG (Informatie voor Verdachten en/ of Veroordeelden) ingevoerd. Deze wet maakt gebruik van biometrische kenmerken mogelijk bij verdachten van misdrijven waarvoor voorlopige hechtenis is toegestaan. De kern is dat de politie (of een andere opsporingsdienst) identificeert en ketenpartners de identiteit in het vervolg (vervolging, berechting en executie van straf) steeds kunnen verifiëren, zodat er zekerheid is over de juiste identiteit van verdachten en veroordeelden.

Met al deze maatregelen worden veel van de geschetste problemen al aangepakt. Maar het is niet voldoende tegenover de geraffineerde werkwijzen van fraudeurs en de veelheid aan kwetsbare plekken waar zij kunnen toeslaan. Het ontbreekt aan een integrale, informatie gestuurde aanpak waarin partners in publieke en private sector de krachten samenballen[9]. Grote organisaties en zware ketens zijn nooit zo efficiënt en effectief in hun verdediging als de kleine, creatieve, wendbare dadergroepen die hen bestoken en makkelijk van aanvalsstrategie kunnen veranderen. Dat maakt dat de pakkans te laag is en de handhaving onvoldoende. Het antwoord zal niet komen van klassieke bolwerken, maar van moderne netwerken die snel reageren en slim anticiperen op identiteitsfraude.

Bij het ontwikkelen van deze visie met fraudedeskundigen uit publieke en private sector werd breed erkend dat identiteitsfraude een gemeenschappelijk probleem is. De motivatie om dat probleem samen aan te pakken is groot. Dat biedt een goede kans om het potentieel van mensen en maatregelen beter te benutten.

[9] Europol pleit in haar Threat Assessment Internet Facilitate Organised Crime iOCTA, File nr: 2530-264 (pag 8) uit 2011 nadrukkelijk voor publiek en private samenwerking.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Identiteit in Cijfers

Versie 1

Datum 12 december 2013
Status Versie 1

Inhoud

Voorwoord 3

1 Bevindingen in het kort 4

2 Definities & Afbakeningen 5

2.1 Identiteit 5

2.2 Identiteitsbewijzen, -dragers en online identiteiten 6

2.3 Identiteitsfraude 7

3 Identiteit in Cijfers 8

3.1 Bevolkingscijfers 8

3.2 Identiteitsmanagement 8

3.3 Identiteitsbewijzen, -dragers en online identiteiten 11

3.4 Beschouwing 14

4 Identiteitsfraude 15

4.1 Publieke sector 15

4.2 Private Sector 18

4.3 Burgers 20

4.4 Beschouwing 22

1910888 01409

Voorwoord

Identiteit is goud waard. Wie zich op betrouwbare wijze kan identificeren, heeft toegang tot een snel groeiend aanbod van diensten en producten wereldwijd en weet zich gezekerd van de rechten die verbonden zijn aan een woonstaat en nationaliteit. De centrale vraag is: "Ben jij wie je zegt wie je bent? Dan kunnen we zaken doen." De meeste mensen gaan hier eerlijk mee om. Maar de stijgende waarde van identiteitsgegevens en het groeiende aantal mogelijkheden om identiteitsgegevens te bemachtigen trekt wereldwijd fraudeurs aan.

Aandacht voor identiteit en identiteitsmanagement wordt dan ook steeds belangrijker. Hoewel er momenteel veel aandacht voor deze thema's is, ontbreekt het aan een compleet beeld dat de diverse deelthema's aan elkaar koppelt.

De monitor "Identiteit in Cijfers" beoogt dit beeld te presenteren. Zowel over het publieke als het private domein bevat deze monitor cijfers op de thema's identiteiten, identiteitsmanagement en identiteitsfraude. Daarmee is deze publicatie de eerste in zijn soort. Aan de hand van deze informatie wordt in de toekomst mede inzichtelijk hoe het veld zich ontwikkelt en welke aanknopingspunten voor beleid er zijn.

Deze eerste editie van de monitor is gebaseerd op het materiaal dat reeds beschikbaar is in diverse bronnen en bij stakeholders in het veld. Zowel uit de publieke als de private sector is medewerking verleend aan de totstandkoming van deze monitor. Het beeld is echter nog niet compleet. Informatie over identiteit wordt nog niet systematisch geregistreerd en ontsloten. De komende jaren zal de monitor Identiteit in Cijfers nader vorm krijgen naarmate er meer cijfers geregistreerd en ontsloten worden.

Hoofdstuk 1 bevat de belangrijkste bevindingen uit deze -eerste- editie van de monitor. In de daarop volgende hoofdstukken wordt achtereenvolgens ingegaan op definities & afbakeningen (H2), identiteitsbewijzen, dragers en online identiteiten (H3) en identiteitsfraude (H4). De cijfers in deze monitor hebben betrekking op het jaar 2012 en zijn zoveel mogelijk gebaseerd op het gehele jaar. Waar dit niet het geval is, is dit expliciet aangegeven.

1910888 01409

1 Bevindingen in het kort

Er zijn miljoenen middelen in omloop waarmee mensen zich identificeren, zowel bij de overheid, bedrijven als tussen burgers onderling. Voor de door de overheid uitgegeven identiteitsbewijzen (ID-kaart, paspoort, rijbewijs en verblijfsdocument) komt dit uit op ruim 25 miljoen geldige documenten. In de private sector wordt een veelvoud aan identiteitsdragers uitgegeven. Alleen al het aantal in omloop zijnde bankpassen (27,7 mln.) en creditcards (5,6 mln.) gaat dit aantal te boven. Daarnaast bevatten ook persoonlijke OV-chipkaarten, zorgpassen, bibliotheekkaarten, klantenkaarten etc. identiteitsgegevens.

In de publieke sector worden identiteitsgegevens vastgelegd in de Gemeentelijke Basisadministratie (GBA). Diverse publieke afnemers (875) maken gebruik van de GBA. die beheerd wordt door gemeenten. Jaarlijks worden 240 miljoen GBA-berichten verzonden en krijgen gemeenten enkele miljoenen (2,2 mln.) wijzigingen te verwerken als gevolg van demografische gebeurtenissen zoals geboorte, overlijden, (internationale) verhuizing en verbintenissen tussen personen. De GBA kent een hoge kwaliteit met 97,7% van de adressen en bijna 100% van de overige gegevens juist geregistreerd. In de private sector worden aparte registraties bijgehouden.

Per jaar zijn meer dan 1 miljoen mensen in meer of mindere mate in hun werk betrokken bij het controleren van de identiteit van personen.

Als gevolg van de verdergaande digitalisering van de maatschappij neemt het belang van online identiteiten toe. Zowel het publieke DigID (9,8mln) als het private aantal gebruikers van internetbankieren (11 mln.) en online shoppers (10,6 mln.) zijn de afgelopen jaren in aantal toegenomen. En deze groei lijkt nog niet op zijn eind te zijn. Identiteit en identiteitsmanagement spelen zich, met andere woorden, steeds meer af in het digitale domein.

Over de volle breedte van de maatschappij komt identiteitsfraude voor en wordt aanzienlijke (financiële) schade geleden als gevolg daarvan. Bovendien kost het aanpakken van deze fraude geld, waardoor publieke en private organisaties dubbel geraakt worden.

In 2012 waren naar schatting 612.000 mensen slachtoffer van identiteitsfraude. Er is een sterke stijging zichtbaar sinds 2007 toen er 75.000 slachtoffer waren. Sindsdien is er jaarlijks een groter aantal burgers slachtoffer. Op dit moment is naar schatting 16,3% van de Nederlandse bevolking ooit slachtoffer geweest van identiteitsfraude. In 2012 is door burgers voor 355 miljoen euro schade geleden.

Een uitspraak over de totale omvang en schade van identiteitsfraude is (nog) niet te geven. Daarvoor ontbreekt het op dit moment nog aan een volledig en precies overzicht. Duidelijk is dat de jaarlijkse omvang van de schade substantieel is, en dat de daadwerkelijke schade groter zal zijn dan in deze editie van de monitor is gepresenteerd.

2 Definities & Afbakeningen

Bij het inrichten van deze monitor zijn keuzes gemaakt in de afbakening van begrippen. In dit hoofdstuk worden de gekozen definities en afbakeningen benoemd.

2.1 Identiteit

Ieder mens heeft allerlei eigenschappen die hem of haar als individu onderscheiden van anderen. Dit kunnen natuurlijke (of biometrische) eigenschappen zijn, eigenschappen die het verhaal van iemand vertellen en eigenschappen die tot uitdrukking komen in gedrag. Het geheel of delen van deze onderscheidende eigenschappen noemen we een identiteit. Per situatie zal de precieze definitie van wat identiteit is echter verschillen.

De overheid kent burgers een formele identiteit toe die in breder verband gebruikt wordt dan alleen overheidsdienstverlening. Tegelijkertijd hebben burgers ook diverse private identiteiten waarmee zij zich identificeren voor bedrijven. De monitor maakt onderscheid tussen de identiteit vanuit het perspectief van dienstverlening van de overheid aan burgers en overige identiteiten.

Identiteit bij dienstverlening aan burgers

Centraal binnen dit perspectief zijn de gegevens die voor de overheid mede de sleutel vormen met betrekking tot de rechten en plichten van burgers. Het gaat hierbij om die gegevens die uniek zijn voor een persoon. Enerzijds gaat het om administratieve gegevens en anderzijds om fysieke en biometrische eigenschappen. Tabel 1 geeft een overzicht van de gegevens. Voor zover deze gegevens geregistreerd worden, wordt dit in de Gemeentelijke Burgeradministratie gedaan. Dit betreft met name de administratieve gegevens.

Tabel 1 – Identiteitsgegevens vanuit overheidsperspectief

Burgerservicenummer	Geslacht
Volledige naam	Gelaatskenmerken (foto)
Burgerlijke staat	DNA-profiel
Nationaliteit	Vingerafdrukken
Geboorteplaats en -land	Handschrift / Handtekening
Geboorte- en overlijdensdatum	
Persoonsgegevens niet zijnde identiteitsgegevens	
Woonadres (waar je woont)	
Samenstelling huishouden (met wie je woont)	
Familiaire relaties (bv. aantal kinderen)	

In de tabel staan persoonsgegevens opgenomen die strikt genomen niet tot identiteitsgegevens te rekenen zijn. In de relatie tussen overheid en burger betreffen dit echter belangrijke gegevens die gebruikt worden in het proces van vaststellen van het recht op voorzieningen en regelingen en nauwe verwantschap hebben met identiteitsgegevens. Voor wat betreft het woonadres is met het overnemen van het amendement[1] op

1 *Kamerstuk, 2012-2013, 33.352 nr. 7*

1910888 01409

zelfstandige strafbaarstelling van identiteitsfraude van kamerlid Dijkhoff adres ook als identificerend gegeven benoemd.

Identiteit in overige situaties
Naast de formele identiteit die de overheid burgers toekent, hebben burgers ook private identiteiten. Deze bestaan doorgaans uit een combinatie van identiteitsgegevens zoals benoemd in tabel 1 en identificerende gegevens die vanuit de private partijen aan burgers worden toegekend (tabel 2).

Tabel 2 - Identificerende gegevens vanuit overig perspectief

Bankrekeningnummer	Wachtwoord
Telefoonnummer	E-mailadres
Verzekeringsnummer	IP-adres
Klantnummer	Pincode

Deze gegevens kennen een zeer sectorspecifieke toepassing en vormen geen schakel in de toekenning van rechten en plichten aan burgers door de overheid, maar kunnen wel gebruikt worden in de uitvoeringspraktijk van overheidsdienstverlening.

2.2 Identiteitsbewijzen, -dragers en online identiteiten

In de praktijk zijn er verschillende verschijningsvormen van identiteit. Deze hebben ook verschillende waardes in de contacten met de overheid, met bedrijven en als burgers onderling. In de monitor wordt onderscheid gemaakt in drie verschijningsvormen.

Identiteitsbewijzen
Identiteitsbewijzen zijn de formele door de Nederlandse overheid verstrekte identiteitsbewijzen: Nederlandse identiteitskaart, paspoorten, verblijfsdocumenten voor vreemdelingen en vluchtelingen en rijbewijzen. Deze identiteitsbewijzen zijn dragers, zowel in digitale als analoge zin, van identiteitsgegevens en vormen een middel waarmee iemand zijn identiteit kan aantonen.

Identiteitsdragers
Naast de van overheidswege verstrekte gegevensdragers zijn er private dragers van identiteits- en persoonsgegevens. Hierbij kan gedacht worden aan bank- en verzekeringspassen en de persoonlijke OV-chipkaart, maar ook aan persoonlijke klantenkaarten etc.. Afhankelijk van het doel van het betreffende middel staan er meer of minder identiteits- en persoonsgegevens op deze gegevensdrager, al dan niet digitaal.

Identiteitsbewijzen kunnen zowel in de publieke als private sector gebruikt worden als identificatiemiddel. Identiteitsdragers daarentegen hebben een specifieke functie binnen het private domein en zijn dan ook alleen voor dat doel te gebruiken.

Online identiteiten
Door de digitalisering van het maatschappelijk verkeer is er steeds vaker sprake van online identificatie, dus via internet. Dit gebeurt aan de hand van online identiteiten. Deze kennen diverse verschijningsvormen zoals accounts(inlognaam/wachtwoord) en kaartlezers (bij online bankieren).

1910888 01409

DigID is de huidige vorm van de online identiteit die door de overheid is uitgegeven en ook in de relatie tussen overheid en burger gebruikt kan worden.

2.3 Identiteitsfraude

De monitor volgt de definitie met bijbehorende uitleg zoals die door het kabinet wordt gehanteerd in de Kabinetsvisie op de aanpak van Identiteitsfraude. Deze definitie, opgesteld door het WODC, luidt:

"*Identiteitsfraude is het opzettelijk (en wederrechtelijk of zonder toestemming) verkrijgen, toe-eigenen, bezitten of creëren van valse identificatiemiddelen en het daarmee begaan van een wederrechtelijke gedraging of met de intentie daarmee een wederrechtelijke gedraging te begaan.*"

Het begrip 'identificatiemiddelen' wordt hier breed uitgelegd: ook bijvoorbeeld het verhaal van een fraudeur om anderen te misleiden, of een kostuum dat vertrouwen moet wekken, of een e-mailaccount en een website die datzelfde doel hebben, gelden als identificatiemiddel. Bij het vaststellen van identiteitsfraude wordt binnen de monitor het volgende uitgangspunt gehanteerd:

Er is sprake van identiteitsfraude vanuit overheidsperspectief wanneer bij het plegen van identiteitsfraude één of meerdere elementen van de set identiteitsgegevens (zie tabel 1, p5) anders voorgedaan worden dan feitelijk juist is. Er is sprake van identiteitsfraude vanuit overige perspectief wanneer alleen identificerende persoonsgegevens van buiten de set kerngegevens (zie tabel 2, p6) anders voorgedaan worden dan juist.

Met name bij het identificeren van identiteitsfraude in de uitvoering van regelingen en voorzieningen is dit onderscheid van belang omdat het helpt bij het trekken van duidelijke grenzen.

1910888 01409

3 Identiteit in Cijfers

Dit hoofdstuk geeft cijfermatig inzicht in het domein identiteit.

3.1 Bevolkingscijfers

Ontwikkelingen in de bevolking van Nederland bepalen voor een belangrijk deel de werkzaamheden op het terrein van identiteit. Gegevens over demografische ontwikkelingen geven daarmee het kader waarbinnen de verdere gegevens in deze monitor geplaatst kunnen worden. Tabel 3 geeft een overzicht van bevolkingscijfers voor het jaar 2012.

Tabel 3 Bevolkingscijfers

Aantallen burgers	
Aantal inwoners (31/12/12)	16.779.575
Aantal geborenen	175.959
Aantal overledenen	140.813
Geboorteoverschot	35.146
Migratiecijfers	
Immigratie	158.374
Emigratie	144.491
Vestigingsoverschot	13.883
Interne mobiliteit	
Verhuisd binnen eigen gemeente	869.002
Verhuisd naar andere gemeente	609.859
Relaties tussen personen	
Aantal huwelijken	70.315
Aantal partnerschapregistraties	9.224
Aantal echtscheidingen	33.273
Huwelijksontbinding door overlijden	56.703

Bron: Centraal Bureau voor de Statistiek

3.2 Identiteitsmanagement

Identiteitsmanagement kent twee kanten. Enerzijds betreft het de wijze waarop identiteitsgegevens gemanaged worden, het systeem. Anderzijds betreft het de mensen die het feitelijke identiteitsmanagement verrichten en werken binnen het systeem.

De gemeentelijke basisadministratie (GBA) vormt een belangrijke spil als het gaat om identiteitgegevens binnen de dienstverlening van de overheid aan burgers. Daarnaast voeren zowel in de publieke als private sector grote aantallen medewerkers in hun dagelijks werk controles uit op de identiteit van personen.

Gemeentelijke basisadministratie

Voor zover de gegevens van burgers in tabel 1 door de overheid worden geregistreerd, zijn deze opgenomen in de GBA. De GBA werkt als een cumulatief systeem. Door geboorten en immigratie worden nieuwe

inschrijvingen aan de GBA toegevoegd. Overlijden en emigratie leiden ertoe dat de persoonslijst van een persoon opgeschort wordt. Deze wordt dan niet verwijderd uit de GBA, maar krijgt een aantekening dat de persoonslijst (tijdelijk) niet meer in gebruik is. Alle wijzigingen/veranderingen die in tabel 3 zijn benoemd, impliceren wijzigingen in de GBA. Jaarlijks komt dit neer op enkele miljoenen gebeurtenissen die aanleiding vormen tot een wijziging.

Afnemers (875) kunnen gebruik maken van (een deel van) de informatie in de GBA. Dit zijn publieke organisaties die voor de uitvoering van hun wettelijke taak gebruik maken van de GBA. Daarnaast kunnen organisaties die een publieke taak uitvoeren of maatschappelijk belang dienen voor die taak als afnemer gebruik maken van de GBA (bijvoorbeeld zorgverzekeraars en pensioenfondsen). In 2012 zijn er 240 miljoen GBA berichten verstuurd[8].

Een kwalitatief hoogwaardige GBA is van groot belang in de dienstverlening van de overheid aan burgers. Bestuursorganen die GBA-informatie afnemen zijn verplicht in het geval van gerede twijfel over de juistheid van de GBA-informatie middels zogenaamde terugmeldingen te laten blijken dat er een mogelijke onjuistheid in de GBA-registratie bestaat. In 2012 vonden ongeveer 30.000 geautomatiseerde terugmeldingen plaats.[2]

Tabel 4 Gemeentelijke Basisadministratie

Inhoud van GBA[3]	
Aantal BSN-nummers actief[4]	16,8 miljoen
Aantal BSN-nummers inactief i.v.m. emigratie[4,5]	1,4 miljoen
Aantal BSN-nummers inactief i.v.m. overlijden[4,5]	2,6 miljoen
Aantal als vreemdelingen geregistreerden[6]	786.100
Aantal als emigrant geregistreerden[5]	944.000
Aantal als VOW'er geregistreerden[7]	427.000
Gebruik van GBA	
Aantal afnemers	875
Aantal verzoeken tot informatie GBA-netwerk[8]	149.438.165
Aantal verzoeken tot informatie GBA-V (webservice)[8]	89.369.940
Kwaliteit van GBA	
Aantal terugmeldingen	Ongeveer 30.000
Aandeel nog in onderzoek	10% meldingen
Statische gegevens (geboortedatum etc.)	Nagenoeg 100%
Adresgegevens	97,7%

Bron: Centraal Bureau voor de Statistiek, Agentschap BPR

2 Naast geautomatiseerde terugmeldingen vinden ook op papier terugmeldingen plaats.
3 De cijfers onder dit kopje hebben allemaal een peildatum. Het betreft dus het aantal in de GBA aanwezige gegevens op een specifieke datum.
4 Deze cijfers hebben peildatum 23-11-2013
5 Een BSN komt niet te vervallen. De registratie in de GBA blijft intact, ook wanneer een persoon is overleden of emigreert. In het laatste geval is er sprake van tijdelijk inactiviteit en zal bij eventuele remigratie het BSN met bijbehorende registratie in de GBA weer geactiveerd worden.
6 Dit cijfer heeft peildatum 1-1-2012
7 Dit cijfer heeft peildatum 20-11-2012
8 Dit getal betreft het aantal verstuurde GBA berichten. Dit zijn berichten aan gemeenten onderling, wijzigingen die automatisch (spontaan) in de GBA worden doorgevoerd waardoor organisaties automatisch over de laatste stand van zaken beschikken en wanneer er actief iets wordt opgevraagd uit de GBA.

Uit audits op de GBA is gebleken dat de huidige kwaliteit van de GBA hoog is. Nagenoeg alle, vrijwel statische gegevens (burgerlijke staat, geboortedatum, familiaire relaties etc.) zijn correct geregistreerd in de GBA. Voor wat betreft het adres is gemeten dat 97,7% van alle personen op een juist adres ingeschreven staat[9].

Tegelijk is er ook sprake van een groep mensen die met de status "vertrokken onbekend waarheen", VOW'ers. In 2012 waren dit er 427.000. Doordat er jaarlijks meer mensen met onbekende bestemming vertrekken dan zich opnieuw melden bij een gemeente en de GBA cumulatief werkt, wordt het totale aantal VOW'ers jaarlijks hoger. Bezien over een periode van 5 jaar komen er jaarlijks gemiddeld 25.000 VOW'ers bij. Verondersteld wordt dat een deel van deze mensen naar het buitenland is verhuisd[10].

Personeel met ID-controlerende taken

Zowel in de publieke als private sector zijn medewerkers werkzaam die in hun dagelijks werk de identiteit van personen vaststellen middels een toets op de geldigheid en authenticiteit van de identiteitsbewijzen en verificatie van de match tussen de gegevens in de document met de persoon die zich met het document legitimeert. Deze zijn grofweg in twee categorieën in te delen.

De eerste categorie komt voort uit de werkgeverstaak de identiteit van nieuwe werknemers te controleren. In totaal zijn er in Nederland 638.000 werkgevers die verplicht zijn loonbelasting te innen. Bij elk van deze organisaties zal er minimaal één persoon zijn die de identiteit van de werknemers vaststelt.

De tweede categorie betreft de werknemers die in het kader van een wettelijke plicht of betalingsgarantie een identiteitscontrole, in welke vorm dan ook, uitvoeren. Binnen de private sector is dit met name aan de orde bij de sectoren financiële en zakelijke dienstverlening, beveiliging, horeca, zorg, telecom, juridische diensten en bij verhuur van goederen. Een grove raming voor de private sector komt uit op 142.000 personen die in de uitvoering van hun werk op enigerlei wijze betrokken zijn bij het controleren van de identiteit van personen.

In de publieke sector betreft het bijvoorbeeld operationele medewerkers bij de politie (51.000), medewerkers burgerzaken (6.000) bij gemeenten, medewerkers bij de immigratie- en naturalisatiedienst (3.478[11]), medewerkers in de justitieketen (37.000[11]), medewerkers bij de UWV (19.000[11]) en SVB (3.000[11]) en de operationele werknemers van de marechaussee (6.800[11]). In principe zullen alle overheidsmedewerkers die in het dagelijks werk in contact komen met burgers op enig moment de identiteit van deze burgers vaststellen.

Bij elkaar zou dit betekenen dat meer dan 1 miljoen personen in hun werk de identiteit van personen controleren. Hierbij zal de striktheid en de werkwijze van de controle afhangen van wettelijke verplichtingen en de

9 ICTU, 2013, Eindrapportage Adresonderzoek 'Samen Leren'

10 http://www.cbs.nl/nl-NL/menu/themas/bevolking/cijfers/incidenteel/maatwerk/2013-vow-mw.htm

11 Deze cijfers betreffen het gehele werknemersbestand van de betreffende organisaties. Afhankelijk van de specifieke functie is er wel of geen contact met burgers in het dagelijks werk. In de gebruikte bronnen wordt echter geen onderscheid gemaakt tussen medewerkers met of zonder burgercontacten.

mate van frauderisico bij het desbetreffende uitvoeringsproces. Het ligt in de verwachting dat in de publieke sector en in de meer fraudegevoelige sectoren (bv financiële dienstverlening) controles strikter zijn dan bij bijvoorbeeld de verhuur van bouwapparatuur.

3.3 Identiteitsbewijzen, -dragers en online identiteiten

Identiteitsbewijzen, -dragers en online identiteiten vormen de middelen waarmee burgers zich identificeren bij de overheid, bij bedrijven en als burgers onderling. In paragraaf 2.2 is reeds toegelicht wat het onderscheid tussen deze middelen is. Deze paragraaf gaat in op de aantallen.

Identiteitsbewijzen

Er zijn in Nederland tientallen miljoenen geldige identiteitsbewijzen in omloop. Vele burgers hebben meer dan één Nederlands identiteitsbewijs in hun bezit. In veel gevallen betreft het een combinatie van een reisdocument en een rijbewijs, maar er zijn ook veel burgers die zowel een paspoort als een identiteitskaart bezitten.

Tabel 5 Identiteitsbewijzen

Reisdocumenten	
Aantal nieuwe paspoorten	2.339.286
Aantal nieuwe identiteitskaarten	1.743.813
Aantal geldige reisdocumenten in omloop[12]	Schatting 17.000.000
Aantal paspoorten gestolen/vermist geregistreerd	49.197
Aantal identiteitskaarten gestolen/vermist geregistreerd	129.903
Aantal uitgiftepunten in Nederland[13]	408
Aantal uitgiftepunten in buitenland (afgerond)	140
Rijbewijzen	
Aantal nieuwe rijbewijzen[14]	1.204.723
Aantal rijbewijzen in omloop	10.906.244
Aantal gestolen/vermist	101.666
Aantal ongeldig verklaard i.v.m. rijontzegging (nov 2013)	7.119
Aantal uitgiftepunten[13]	408
Verblijfsdocumenten	
Aantal nieuwe verblijfsdocumenten	218.700
Aantal verblijfsdocumenten gestolen/vermist	5890
Aantal uitgiftepunten	9

Bron: Agentschap BPR, Rijksdienst Wegverkeer, Immigratie- en Naturalisatiedienst

12 Dit cijfer is berekend aan de hand van het aantal in de afgelopen vijf jaar geproduceerde reisdocumenten, onder aftrek van gestolen/vermiste documenten. Het Agentschap BPR heeft aangegeven niet te kunnen aangeven hoeveel reisdocumenten er in omloop zijn omdat er geen centrale reisdocumentenadministratie is.

13 Dit betreft het aantal Nederlandse gemeenten die de uitgifte verzorgen. Het aantal feitelijke loketten ligt hoger doordat diverse gemeenten vanuit meerdere locaties werken.

14 Dit cijfer betreft het aantal nieuw uitgegeven documenten. Het aantal personen dat in 2012 het rijbewijs heeft gehaald lag op 173.962.

Jaarlijks worden er ongeveer 4 miljoen nieuwe reisdocumenten geproduceerd[15], ruim 1 miljoen nieuwe rijbewijzen en 218.000 verblijfsdocumenten uitgegeven. Deels betreft dit vervanging van de ongeveer 270.000 gestolen of vermiste documenten.

De uitgifte van identiteitsdocumenten is voor het grootste gedeelte gekoppeld aan de Nederlandse gemeenten. Voor reisdocumenten geldt dat ook bijvoorbeeld Nederlandse consulaten in het buitenland als uitgiftepunt voor documenten gelden. Bij vreemdelingendocumenten ligt het aantal uitgiftepunten beduidend lager, doordat alleen de IND-loketten deze uitgifte verzorgen.

Identiteitsdragers

Private identiteitsdragers zijn er in vele vormen en soorten. Ook in aantal zijn private identiteitsdragers talrijk. Zo beschikt iedere tegenwoordig wel over een zorgpas en een bankpas en een deel ook over een creditcard en een persoonlijke OV-chipkaart. Zelfs al zou dit beperkt zijn tot gemiddeld drie private identiteitsdragers per persoon, dan spreken we in totaal al over enkele tientallen miljoenen identiteitsdragers in omloop in Nederland. Een precies aantal weten we niet. Het volgende is wel bekend:

- Volgens de Nederlandse Vereniging van Banken waren in 2012 ongeveer 24,7 miljoen passen in omloop. Er is geen zicht op het aantal buitenlandse bankpassen.
- Daarnaast zijn er in Nederland naar schatting van De Nederlandse Bank ongeveer 5,8 miljoen Nederlandse creditcards in omloop. Er is geen zicht op het aantal buitenlandse creditcards of creditcards uitgegeven door bijvoorbeeld warenhuizen.
- Deze bankpassen en creditcards zijn gekoppeld aan 22,7 miljoen betaalrekeningen.
- Translink meldt in het jaaroverzicht dat er eind 2012 ongeveer 7,5 miljoen bruikbare persoonlijke OV-chipkaarten in omloop zijn.
- In 2011 waren, zo blijkt uit de bibliotheekmonitor, 1,8 miljoen volwassenen lid van de bibliotheek.

Andere voorbeelden van private identiteitsdragers zijn klantenkaarten, werknemerspasjes, tankpassen en verzekeringspassen. Hoewel deze andere private identiteitsdragers mogelijk minder direct kunnen leiden tot financiële schade en identiteitsfraude, is hun gezamenlijk aantal waarschijnlijk een veelvoud van de hierboven benoemde identiteitsdragers. Daarmee ontstaan veel mogelijkheden identiteitsgegevens te verliezen.

Online identiteiten

Net als bij identiteitsdragers zijn er vele mogelijkheden als het gaat om online identiteiten. Ook hier zit een grote variëteit in de mate waarin het gevoelige identiteitsgegevens betreft. In deze monitor wordt ingezoomd op drie vormen van online identiteiten: het publieke DigID en het private online bankieren en online winkelen. Tabel 6 geeft een overzicht.

15 Het daadwerkelijk aantal uitgegeven documenten ligt lager als gevolg van het bijvoorbeeld niet op halen van documenten en documenten die bij controle foutieve gegevens blijken te bevatten. In 2012 zijn 4.063 documenten om diverse redenen retour gekomen bij de producent.

DigID is te beschouwen als de vanuit de overheid verstrekte online identiteit. Met DigID kan de burger een deel van het contact met de overheid online afhandelen en de eigen gegevens zoals die bij diverse publieke diensten zijn geregistreerd inzien. De huidige DigID kent nog geen private toepassing[16].

Bijna 10 miljoen burgers beschikten in 2012 over een DigID. In totaal zijn deze DigID's ruim 75 miljoen keer gebruikt ter online identificatie. Het grootste aantal authenticaties komt voort uit de sectoren financiën (21 mln), werk & inkomen (21 mln) en jeugd & onderwijs (10 mln). Bij 554 publieke organisaties is het inmiddels mogelijk online te identificeren middels DigID.

Tabel 6 Online identiteiten

DigID	**2009**	**2012**
Aantal uitgegeven DigID (31-12)	7.455.033	9.872.935
Aantal machtigingen DigID (31-12)		325.126
Aantal authenticaties met DigID	24.785.857	75.502.486
Aantal DigID accepterende organisaties	487	554
Online bankieren	**2012**	
Aantal gebruikers online bankieren	Ongeveer 11.000.000	
Aandeel in totaal aantal gebruikers	Bijna 4 op 5 Nederlanders	
Aandeel in totaal overschrijvingen	93%	
Thuiswinkelen	**2009**	**2012**
Aantal actieve internetters	11.200.000	12.000.000
Aantal consumenten met online aankoop	8.600.000	10.580.000
Aandeel actieve internetters online aankoop	76,8	88,1%
Aantal bestellingen	53.488.000	88.000.000

Bron: Logius, Nederlandse Vereniging van Banken, Thuiswinkel markt monitor

In de private sector is online zaken doen steeds gebruikelijker. Internetbankieren is niet meer weg te denken. Slechts een minderheid van de consumenten, één op de vijf, met een klein deel van de totale overboekingen (7%) doet de zaken nog via de post. Ook overige dienstverlening van banken verloopt steeds vaker online.

Online aankopen doen is de afgelopen tien jaar ook sterk toegenomen. Bijna 11 miljoen mensen (9 miljoen in 2009) hebben ooit via internet een aankoop gedaan. Een iets kleiner aantal heeft dit één of meerdere malen in 2012 gedaan. Van alle mensen met internet koopt bijna 9 van de 10 wel eens iets via internet.

Bij internetbankieren en online aankopen wordt gebruik gemaakt van een online identiteit. Qua beveiliging zijn er grote verschillen in online identiteiten, variërend van een inlognaam met zelfgekozen wachtwoord tot het gebruik van een combinatie van bankpas, pincode en kaartlezer. Bij sommige online aankopen is een afgeronde betaling voldoende om een aankoop af te ronden en vindt er geen verdere identiteitscontrole plaats.

16 Uitzondering hierop vormen diverse pensioenfondsen, zorgverleners en zorgverzekeraars. Deze partijen hebben het recht gebruik te maken van het BSN in hun administratie en kunnen daardoor ook gebruik maken van DigID.

3.4 Beschouwing

Uit het voorafgaande kan afgeleid worden dat het domein identiteit een breed karakter heeft en qua omvang van de werkzaamheden en "gebeurtenissen" ook groot is. De identiteit van mensen kent vele vormen in verschillende mate van belangrijkheid en mate waarin er middels die identiteit toegang verkregen kan worden tot (zeer gevoelige) persoonsinformatie.

Duidelijk wordt ook dat digitalisering van de interactie tussen bedrijven, overheden en burgers ook in belang toeneemt. Het is een ontwikkeling die implicaties heeft voor de wijze waarop identiteitsgegevens worden gebruikt.

Het praktische feit dat burgers nu een breed scala aan middelen in bezit hebben waarmee zij zichzelf bij overheden en private partijen kunnen identificeren biedt tegelijkertijd ook een breed scala aan mogelijkheden voor kwaadwillende personen om misbruik te maken van die gegevens. Zeker wanneer de bescherming van gegevens vanuit het oogpunt van gemak en efficiëntie wordt beperkt – een binnen het private domein veelgemaakte afweging – ontstaan risico's op identiteitsfraude.

Het is van belang om meer gedetailleerd zicht te krijgen op het aantal identiteiten in omloop, zowel publiek als privaat, daar ieder identiteitbewijs of iedere identiteitsdrager een risico op verlies en misbruik van persoonlijke gegevens met zich meebrengt.

4 Identiteitsfraude

Je identiteit is goud waard. Daarmee zou het dus ook kunnen lonen om misbruik te maken van identiteitsgegevens van anderen en daar vervolgens mee te frauderen. Dat identiteitsfraude leidt tot schade voor de maatschappij is een gegeven. Hoeveel schade er in totaal wordt geleden als gevolg van identiteitsfraude is echter onduidelijk. In dit hoofdstuk wordt de beschikbare informatie over de omvang en schade van identiteitsfraude bijeengebracht. Hierbij wordt gekeken naar de schade van zowel publieke organisaties, private organisatie als naar burgers.

4.1 Publieke sector

Vanuit het perspectief van de overheid en haar verantwoordelijkheid voor een zorgvuldige identiteitsvaststelling en uitgifte van identiteitsbewijzen zijn er twee manieren om naar identiteitsfraude te kijken. De eerste betreft de geldigheid van de documenten. Een ongeldig document of een geldig document in verkeerde handen kan gebruikt worden om te frauderen en de overheid en derden schade te berokkenen. De tweede wijze betreft de fraude die gepleegd wordt in de uitvoering van regelingen en voorzieningen van de overheid.

Ongeldige documenten

Een compleet overzicht van in hoeverre er binnen de uitvoering van regelingen en voorzieningen van de overheid valse en ongeldige documenten worden gesignaleerd is niet op te stellen. Daarvoor wordt er momenteel onvoldoende eenduidig geregistreerd.

Over het aantreffen van valse documenten aan de grens zijn wel cijfers bekend, namelijk de praktijkcijfers van het Expertise Centrum Identiteitsfraude en Documenten (ECID). Het ECID is het landelijke knooppunt op het gebied van identiteitsfraude en identiteitsgerelateerde documenten. Zij beoordelen onder andere reisdocumenten op echtheid en vervullen een belangrijke expertisefunctie voor zowel publieke als private organisaties.

In totaal heeft het ECID in 2012 ongeveer 35.000 documenten beoordeeld op hun echtheid. Het grootste deel van dit werk komt voor uit het personenverkeer op schiphol. Een kleiner deel komt voort uit mobiel toezicht veiligheid alsmede de ad hoc adviesverzoeken. In 2012 zijn ruim 2100 valse documenten of gefalsificeerde kopieën van echte documenten geconstateerd. Hierbij waren ruim 1500 verdachten betrokken. Het overgrote deel van de geconstateerde fraude betreft fraude met buitenlandse documenten.

Tabel 7 Praktijkcijfers ECID

Falsificaten Schiphol Desk	
Aantal gecontroleerde documenten	33.307
Geconstateerde fraude met documenten	806
Geconstateerde fraude %	2,4%
Aantal aanhoudingen verdachten	578
Overige locaties	
Aantal aanhoudingen verdachten	263
In beslag genomen documenten	358
Helpdeskfunctie ECID	
Aantal aanhoudingen verdachten	745
Geconstateerde fraude met documenten	966
Zaken met Nederlandse documenten	
Geconstateerde gevallen van fraude originele documenten	78
Geconstateerde gevallen van fraude kopieën	233

Bron: ECID, Statistische Jaaroverzicht Documentfraude 2012

De cijfers in bovenstaande tabel geven alleen de geconstateerde fraude weer. Hierdoor kan de indruk ontstaan dat er weinig fraude met documenten wordt gepleegd. Er is echter ook sprake van ongedetecteerde identiteitsfraude met valse identiteitsbewijzen. Een vorm waarbij dit aan de orde zou kunnen zijn is fraude met look-a-likes. Het ECID constateert over 2012 een daling van het aantal onderkende gevallen van misbruik van geldige documenten door look-a-likes. Het ECID voegt hier aan toe dat een stijging was verwacht, maar dat mogelijk door zorgvuldiger geworden mensensmokkelorganisaties de documenten beter matchen en daardoor lastiger te detecteren zijn.

Bij regelingen & voorzieningen

Identiteitsfraude staat niet op zich. Daar waar sprake van fraude is, is ook geregeld sprake van manipulatie van informatie waar de persoonlijke situatie anders wordt voorgedaan dan die is. Daar waar het de manipulatie van identiteitsgegevens uit tabel 1 betreft, kan ook gesproken worden van identiteitsfraude vanuit overheidsperspectief. Indien in de uitvoering van overheidsregelingen gefraudeerd wordt met andere gegevens, dan betreft het reguliere fraude.

Bij regelingen en voorzieningen is geregeld sprake van fraude met de nauw aan de persoon gerelateerde gegevens zoals die zijn benoemd in tabel 1, bijvoorbeeld het woonadres. In de eerste plaats betreft het hier woonadresfraude. Daarnaast is er sprake van nauwe verwantschap met identiteitsfraude.

Voorbeelden hiervan treffen we aan bij de sociale verzekeringen. In de grondslagen van diverse uitkeringen (bv WWB en AOW) zijn het woonadres en de samenstelling van het huishouden van belang bij het vaststellen van het recht op uitkering. Zo wordt bij de bijstand het totale gezinsinkomen als uitgangspunt genomen. Ook bij de AOW geldt dat twee afzonderlijk wonende AOW'ers meer uitkering krijgen dan wanneer er een gezamenlijk huishouden wordt gevoerd.

1910888 01409

Volgens de integrale rapportage handhaving van het ministerie van SZW was bij de bijstand in 2011 sprake van woonfraude (19.4 mln) en partnerfraude (7,6 mln). In het jaarverslag van de Sociale Verzekeringsbank blijkt dat in 2012 voor €17,4 miljoen is gefraudeerd. De aandelen van fraude met de inlichtingenplicht omtrent samenwonende partner voor de regeling AOW en fraude met de kinderbijslag voor in het buitenland verblijvende kinderen hierin is onduidelijk.

Eenzelfde analyse zou gemaakt kunnen worden voor de fraude met studiefinanciering. Met het opgeven van een ander woonadres, kunnen studenten aanspraak maken op een uitwonende beurs, terwijl ze hier geen recht op hebben wanneer zij nog thuis wonen. In 2012 is bij in totaal 1.724 studenten fraude met de uitwonendenbeurs geconstateerd. Hiermee was een bedrag van ten minste 12 miljoen gemoeid. Daarnaast hebben 213 studenten kort voor het huisbezoek hun beurs omgezet van uit- naar thuiswonend[17].

Een andere vorm van aan identiteitsfraude verwante fraude doet zich voor binnen het domein van illegale arbeid. Met het vervalsen van werkvergunning of identiteitsdocumenten krijgen de werknemers onterecht toegang tot de Nederlandse arbeidsmarkt. In 2012 heeft de InspectieSZW 2.555 illegaal tewerkgestelden geconstateerd[18]. De schade hiervan is niet bekend, maar er zijn op grond van de Wet arbeid vreemdelingen 1.904 bestuurlijke boetes opgelegd met een totale waarde van 33,4 miljoen.

Ook binnen andere regelingen en voorzieningen binnen de publieke sector cq met een publiek belang is identiteitsfraude of aan identiteitsfraude verwante fraude denkbaar. Een voorbeeld hiervan betreft de identiteitsfraude met toeslagen zoals die zich in 2011 voordeed[19]. Ook zijn er signalen dat bij de verhuur van woningen fraudeurs onder valse voorwendselen en met valse papieren woningen huren, een huurachterstand opbouwen en vervolgens met onbekende bestemming vertrekken. Daarnaast is er bijvoorbeeld sprake van opgave van valse namen bij boetes voor zwartrijden en verkeersboete. In welke mate dit voorkomt en welke schade hiermee maatschappelijk geleden wordt, is niet bekend.

Strafbaarstelling

Een momenteel aanhangig wetsvoorstel[20] maakt het mogelijk om strafrechtelijk op te treden tegen verschillende vormen van identiteitsfraude met identiteitsbewijzen. Bij inwerking treden van deze wet is het strafbaar om een identiteitsbewijs, zoals een rijbewijs of een vreemdelingendocument, van een ander te gebruiken. Nu geldt dit alleen voor reisdocumenten. Door die aanpassing wordt het gemakkelijker de zogeheten look-a-like fraude aan te pakken. Fraude met identificerende persoonsgegevens is op dit moment niet afzonderlijk strafbaar gesteld. De reden daarvan is dat fraude met identificerende persoonsgegevens onderdeel vormt van meer algemene delictsomschrijvingen als oplichting

17 www.rijksoverheid.nl/nieuws/2013/08/13/meer-dan-1700-studenten-gepakt-voor-gesjoemel-met-beurs.html
18 Jaarverslag 2012 InspectieSZW
19 Zie bijvoorbeeld Aanhangsel Handelingen, vergaderjaar 2010-2011, nr. 3427.
20 Wijziging van het Wetboek van Strafrecht en de Wegenverkeerswet 1994 in verband met de verbetering van de aanpak van fraude met identiteitsbewijzen en wijziging van het Wetboek van Strafvordering, de Beginselenwet justitiële jeugdinrichtingen en de Wet DNA-onderzoek bij veroordeelden in verband met de verbetering van de regeling van de identiteitsvaststelling van verdachten en veroordeelden, 33 352

(artikel 326 Sr), flessentrekkerij (artikel 326a Sr) en bedreiging (artikel 284 e.v. Sr). Met behulp van die bepalingen kan op dit moment strafrechtelijk tegen deze vorm van identiteitsfraude worden opgetreden. Het amendement van de heer Dijkhoff[21] zal het misbruik van identificerende persoonsgegevens meer op één lijn stellen met het misbruik van reisdocumenten en identiteitsbewijzen waarvoor artikel 231 van het Wetboek van Strafrecht een aparte strafbaarstelling kent. Daarnaast kent het Wetboek van Strafrecht specifieke strafbaarstellingen voor de aanpak van misdrijven waartoe fraude met identificerende persoonsgegevens vaak de opstap vormt. Bij die misdrijven gaat het bijvoorbeeld om mensensmokkel, witwassen, bank- of uitkeringsfraude, terrorisme of drugs- en wapengerelateerde misdrijven.

4.2 Private Sector

Private organisaties kunnen net als burgers en overheidsinstellingen last hebben van identiteitsfraude. Juist omdat er vele vormen van identiteitsfraude zijn en de registraties hiervan weinig specifiek, is het lastig te komen tot een eenduidig beeld van de omvang en schade van identiteitsfraude in de private sector. In deze monitor bekijken we een aantal sectoren waar identiteitsfraude een grote impact kan hebben.

Bankensector

Binnen de bankensector wordt scherp gekeken naar identiteitsfraude. De directe koppeling tussen financiële middelen en de fraude maakt dat inzichtelijk is welke fraude er heeft plaatsgevonden en wat de schade hiervan was. Belangrijk is de notie dat wanneer er aantallen passen worden benoemd die aantallen passen betreffen waar daadwerkelijk fraude mee is gepleegd.

Tabel 8 Identiteitsfraude bankensector

Fraude met passen	
Aantal gestolen/verloren passen	6.000 bankpassen 1.600 creditcards
Aantal geskimde passen	51.200
Schade van skimming	28,9 miljoen
Fraude met internetbankieren	
Aantal geslaagde pogingen	10.900
Schade bij internetbankieren	34,8 miljoen
Fraudeurs	
Aantal records frauderegister (EVA)	Bijna 28.000
Aantal records toegevoegd in 2012	Ruim 4.700
Aantal raadplegingen	12,5 miljoen
Aantal hits op register	Ruim 28.000

Bron: Nederlandse Vereniging van Banken

In totaal is er in de bankensector in 2012 voor ruim 60 miljoen schade geleden als gevolg van identiteitsfraude. Ten opzichte van eerdere jaren is een sterke daling, met name bij skimming, ingezet. Dit mede als gevolg van de overstap van magneetstrip naar chip en het blokkeren van passen buiten Europa.

21 Kamerstuk, 2012-2013, 33.352 nr. 7

Tabel 9 Historische cijfers ID-fraude bankensector (in miljoenen)

Fraudevorm	2009	2010	2011	2012	2013, 1e helft
Internetbankieren	1,9	9,8	35	34,8	4,2
Skimming	31	19,7	39	28,9	5,9

Bron: Nederlandse Vereniging van Banken

Voor wat betreft skimming ontstaat een sterk contrast met het beeld dat uit het onderzoek onder burgers naar voren is gekomen. De verklaring hiervoor ligt in een combinatie van de berekeningswijze en het perspectief op slachtofferschap. Banken tellen de feitelijke schade en benoemen het daadwerkelijk misbruikte aantal passen. Tegelijk wordt er bij een vermoeden van skimapparatuur op een pinautomaat een hele reeks mogelijk geskimde passen geblokkeerd. Deze passen hoeven uiteindelijk niet misbruikt te zijn, maar worden preventief geblokkeerd. Vanuit het perspectief van de burger bezien is het denkbaar dat dit beschouwd wordt als slachtofferschap omdat er een nieuwe pas en pincode aangevraagd moeten worden en men er hinder van ondervindt. Bij het burgeronderzoek is gevraagd of men slachtoffer is geweest waardoor het cijfer in het burgeronderzoek hoger uitgevallen kan zijn.

Indien er fraude wordt geconstateerd, worden de (misbruikte) gegevens[22] van de betreffende (rechts)persoon geregistreerd in de Externe Verwijzingsapplicatie (EVA). Dit systeem verbindt de frauderegisters van banken en financieringsondernemingen met elkaar. Het register bevat ten tijde van het opstellen van de monitor gegevens van bijna 28.000 (rechts)personen, waarvan ruim 4.700 toegevoegd in 2012. In 2012 heeft het systeem ruim 28.000 maal een "hit" gehad. Dit cijfer is mogelijk vertroebeld door dubbele controles door medewerkers en "shoppende" fraudeurs waardoor het hoger uitvalt.

Thuiswinkelen

In paragraaf 3.3 is reeds gemeld dat een groot deel van de Nederlandse bevolking gebruik maakt van webwinkels en de mogelijkheden van online aankopen. Verwachting is dat dit eerder zal toenemen dan afnemen. Het gemak speelt hierbij een grote rol. Uitgebreide controles op identiteit en betaling met creditcards verhogen de veiligheid, maar beperken ook het gemak. Daar zit voor de webwinkels dan ook de afweging qua balans tussen inkomsten en veiligheid.

Primair is er voor webwinkels geen motivatie de identiteit van klanten te controleren. Net als in een reguliere winkel geldt dat wanneer het product betaald is de koop gesloten is. Het gaat echter mis wanneer blijkt dat de klant niet is wie hij zegt dat hij is en bestellingen onderschept worden bij aflevering of op rekening van anderen worden gedaan. Zowel de burger als de webwinkel kan hier slachtoffer van zijn en financiële schade lijden.

De omvang van deze schade is echter onduidelijk. Nieuwsberichten en publicaties uit de afgelopen jaren schetsen een diffuus beeld lopend van enkele tot vele tientallen miljoenen schade als gevolg van identiteitsfraude. Gegeven de omvang van de sector, zal dit mogelijk ook lastig vast te stellen zijn. In de meldingen van identiteitsfraude bij het

22 De geregistreerde gegevens betreffen de persoonsgegevens die zijn gebruikt in de poging tot fraude. Het is mogelijk dat dit gegevens van derden betreffen die door de fraudeur worden misbruikt.

Centraal Meldpunt Identiteitsfraude en -fouten (CMI) is de sector internetwinkels met 24% de grootste sector waar burgers slachtoffer zijn geworden[23].

Zorgsector
Concrete cijfers over de omvang van identiteitsfraude in de zorgsector ontbreken. Wel zijn er signalen dat mensen gebruikmakend van de zorgpas van derden, veelal met medeweten van die persoon, zorg ontvangen. Dit betreft regelmatig onverzekerden en mensen die illegaal in Nederland verblijven. Doorgaans zijn ziekenhuizen of personen niet het slachtoffer van deze vorm van ID-fraude, de kosten voor de behandeling liggen bij de verzekeraar.

Telecomsector
Binnen de telecomsector komt ID-fraude het meest voor als gevolg van diefstal van telefoons met bijbehorende simkaart. De schade hiervan komt terecht bij de burgers. Zij dienen zelf zorg te dragen voor het melden van diefstal zodat de simkaart geblokkeerd kan worden. Het opgeven van valse adresgegevens vormt recent een probleem bij het afsluiten van contracten voor abonnementen. In korte tijd worden dan meerdere contracten afgesloten op één vals adres, maar de rekening wordt nooit betaald. De uitgegeven telefoons alsmede de verbruikte belminuten en data vormen dan een verliespost. Het is onduidelijk hoe vaak deze vorm van fraude optreedt en welke schade er mee geleden worden.

Verzekeraars
Identiteitsfraude komt voor bij verschillende soorten verzekeringen. Naast financiële schade leidt dit ook tot imagoschade voor de sector. Bij levens-, ongevallen- en arbeidsongeschiktheidsverzekeringen komt het bijvoorbeeld voor dat valse papieren worden gebruikt voor de verzekerde of de begunstigde. Bij verzuimverzekeringen wordt in geval van ziekte een duurdere medewerker opgegeven dan de feitelijke zieke medewerker. Op deze wijze ontvangt de werkgever een hogere vergoeding.

Het aanpakken van deze vormen van identiteitsfraude is lastig omdat verzekeraars geen mogelijkheden hebben om de persoonsgegevens van personen inclusief hun adresgegevens te controleren. Als gevolg hiervan wordt door de sector geschat dat 90% van de fraude ongedetecteerd blijft. Welke schade gemoeid is met identiteitsfraude bij verzekeraars is onbekend.

4.3 Burgers

Misbruik van identiteitsgegevens kan voor burgers een ingrijpende ervaring zijn en voor burgers flinke financiële schade opleveren. Uit onderzoek[24] blijkt dat aanzienlijke aantallen burgers de afgelopen jaren slachtoffer zijn geweest alsmede schade hebben geleden als gevolg van diverse vormen van identiteitsfraude.

Slachtofferschap
Op basis van een representatieve steekproef is geraamd dat in 2012 612.000 burgers slachtoffer zijn geweest van identiteitsfraude. Dit komt neer op 4-5 % van alle volwassenen in Nederland. In 2007 was sprake van 75.000 slachtoffers. Dit betekent een sterke stijging in de laatste

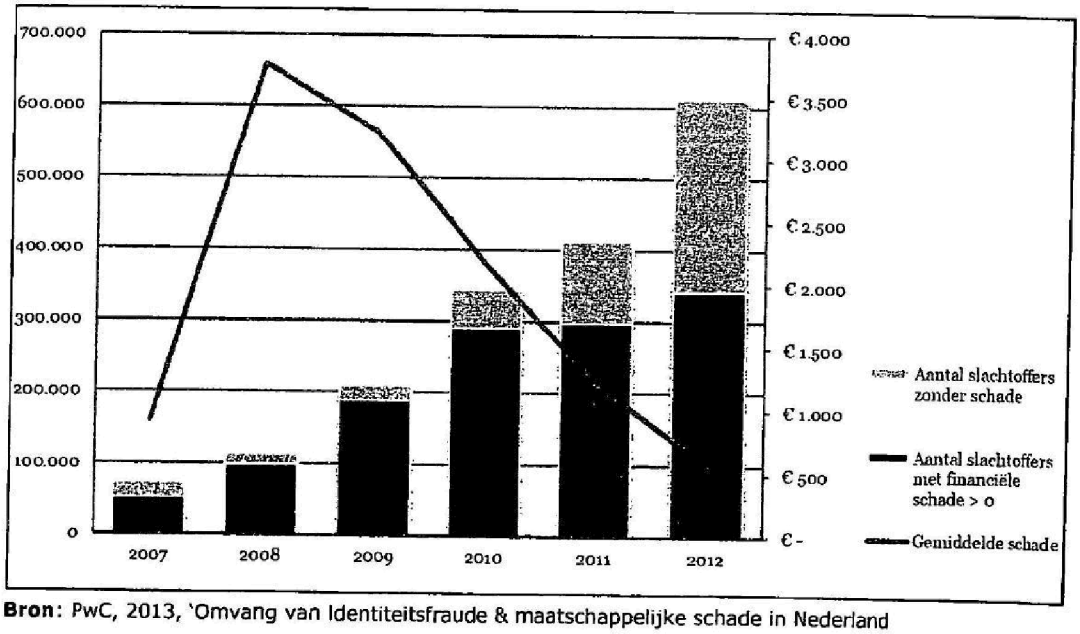
23 PwC, 2013, Analyse Meldingen CMI 2011-2012
24 PwC, 2013 Update onderzoek 'Omvang van identiteitsfraude & maatschappelijke schade in Nederland

jaren. Steeds meer mensen zijn jaarlijks slachtoffer. Cumulatief gezien blijkt uit het onderzoek dat circa 16,3% van de Nederlandse bevolking ooit slachtoffer is geweest van enige vorm van identiteitsfraude.

In bijna de helft van de gevallen gaat het om financiële identiteitsfraude, onder andere door het skimmen van een bankpas (zie ook alinea bankensector onder 4.2). Bijna 20 procent van de slachtoffers kreeg te maken met ID-fraude via het internet. Bij 10 procent was sprake van het gebruik van andermans identiteit om straffeloos een overtreding of misdrijf te begaan. Ook in zo'n 10 procent van de gevallen werd een burgerservicenummer van een ander gebruikt bij een huisarts of in een ziekenhuis.

Slachtofferschap komt vaker voor bij jongeren, mannen en hoog opgeleiden. Onder de Nederlanders in de leeftijdscategorie 18 tot 34 jaar is één op de vijf ooit slachtoffer geweest van enige vorm van identiteitsfraude. Bij mensen van 65 jaar of ouder is dat iets meer dan één op de tien. Van de Nederlandse mannen is bijna één op de vijf ooit slachtoffer geweest van identiteitsfraude. Onder vrouwen ligt het slachtofferschap iets lager: ongeveer één op de zeven. Onder hoog opgeleide Nederlanders is ruim één op de vijf wel eens slachtoffer geweest van identiteitsfraude, terwijl dat bij middelbaar opgeleide Nederlanders op ruim één op de tien ligt. Voor laag opgeleide Nederlanders ligt het er ongeveer tussenin: bijna één op de zes.

Figuur 1Schatting slachtoffers identiteitsfraude Nederland en gemiddeld schadebedrag



Bron: PwC, 2013, 'Omvang van Identiteitsfraude & maatschappelijke schade in Nederland

Schade
Niet alle burgers lijden financiële schade als gevolg van het slachtofferschap van identiteitsfraude. De fraude kan ontdekt zijn voordat schade is berokkend of de burger is schadeloos gesteld door bijvoorbeeld de bank. In het geval van schadeloosstelling, is er nog altijd wel sprake van schade voor de maatschappij, maar die wordt dan niet direct door de burger gedragen. Naar schatting heeft tussen de 9 en de 11 % van de Nederlandse bevolking daadwerkelijke financiële schade ondervonden als gevolg van identiteitsfraude. In 2012 bedroeg deze schade 355 miljoen (met een betrouwbaarheidsmarge van 207-504 miljoen). Het gemiddelde schadebedrag bedroeg in 2012 €600,- per slachtoffer. Over de jaren heen is dit bedrag is gedaald.

4.4 Beschouwing

Over de volle breedte van de maatschappij komt identiteitsfraude voor en wordt aanzienlijke (financiële) schade geleden als gevolg daarvan. Bovendien kost het aanpakken van deze fraude ook geld, waardoor publieke en private organisaties dubbel geraakt worden.

Een uitspraak over de totale omvang en schade van identiteitsfraude is (nog) niet te geven. Daarvoor ontbreekt het op dit moment nog aan een volledig en precies overzicht. Duidelijk is dat de jaarlijkse omvang van de schade substantieel is, hetgeen een gecoördineerde en gezamenlijke aanpak van het probleem rechtvaardigt. Helder is ook dat de daadwerkelijke schade waarschijnlijk groter is dan in deze editie van de monitor is gepresenteerd.

Een eerste stap in de aanpak van identiteitsfraude is het onderkennen dat identiteitsfraude zich op vele domeinen voordoet en hand in hand gaat met andere fraudevormen. Identiteitsfraude is vaak het middel om te komen tot andere vormen van fraude en andere vormen van criminaliteit. Een nadere analyse op overige regelingen en voorzieningen waarbij sprake is van fraude en mogelijk identiteitsfraude zou het zicht op de problematiek vanuit overheidsperspectief kunnen vergroten. Meer zicht op de omvang en precieze vormen waarop identiteitsgegevens worden misbruikt om voordeel te behalen binnen regelingen en voorzieningen biedt ook aanknopingspunten voor het bestrijden van identiteitsfraude en draagt bij aan het bestrijden van andere vormen van fraude.

1910888 01409