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).

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] Kabinetsbrief aan de Tweede Kamer over eID stelsel en DigiD-kaart, verzonden 19 december 2013
[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.