Panteia
Research to Progress

Research voor Beleid | EIM | NEA | IOO | Stratus | IPM

Eindrapport

Aanpak ID-fraude in Nederland

Inventarisatie van maatregelen die bedrijven en instellingen nemen

Auteurs: John Boog, Guido Brummelkamp en Alexandra Vennekens

Zoetermeer, november 2013

Dit onderzoek is uitgevoerd in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De verantwoordelijkheid voor de inhoud van het onderzoek berust bij de auteurs. De inhoud vormt niet per definitie een weergave van het standpunt van de Minister van Binnenlandse Zaken en Koninkrijksrelaties.

Inhoudsopgave

1 Inleiding

1.1 Doel- en vraagstelling

Het succes van organisaties, of het nu gaat om private bedrijven of publieke instellingen, hangt in essentie af van de mate waarin zij in staat zijn om hun klanten (burgers) te kennen. Persoonsgegevens zijn daarom goud waard (zoals ook al door het ministerie van BZK is geconstateerd in het kader van het programma Identiteit op Orde). Deze waarde is de drijvende kracht achter de ontwikkeling van de informatiemaatschappij. De keerzijde is dat misbruik van persoonsgegevens veel schade kan veroorzaken, zowel bij bedrijven, overheden als bij individuele burgers. Het stelt overheden voor een fundamentele opgave. Zonder al te veel afbreuk te doen aan de merites van de informatiemaatschappij moet zij de ontwikkelingen in goede banen leiden. In de eerste plaats is de overheid direct verantwoordelijk voor de integriteit van publieke registraties, in de tweede plaats dient zij voorwaarden te stellen aan verzameling, opslag en koppeling van gegevens in het private domein. In de derde plaats dient zij zorg te dragen voor een effectieve handhaving van regels en aanpak van misbruik.

Dit is het verslag van een onderzoek naar de aanpak van ID-fraude door Nederlandse bedrijven en instellingen. Directe aanleiding zijn de inspanningen van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) om te komen tot een kabinetsvisie op de aanpak van ID-fraude. Eerder liet het ministerie al in beeld brengen hoe groot het probleem is. Hieruit bleek dat alleen al in 2012 600.000 mensen slachtoffer waren van deze vorm van criminaliteit en dat zij daarmee voor zo'n € 350 miljoen werden benadeeld. Daarbij is niet in beeld wat de schade voor bedrijven is. In opdracht van het ministerie van BZK heeft Panteia onderzoek gedaan naar de wijze waarop private partijen identiteitsfraude voorkomen en hoe zij in het geval van fraude hiertegen optreden. Het onderzoek heeft zich geconcentreerd op branches en bedrijven waar de risico's op ID-fraude het grootst zijn. Deze risico's hebben wij afgeleid uit de volgende indicatoren:

- Omvang cliëntenbestand: we hebben gekeken bij grote instellingen en bedrijven die zich bij hun persoonsverificatie niet kunnen baseren op een persoonlijk face to face contact met de klant (vanwege de omvang van het cliëntenbestand) en derhalve hun persoonsverificatie (slim) moeten organiseren (bijvoorbeeld telecomproviders).
- Fysieke afstand tot cliënt: we hebben voorts bedrijven in het onderzoek betrokken die geen face to face contact kunnen hebben met hun cliënten (bijvoorbeeld webwinkels).
- Prevalentie van ID-fraude: ten derde hebben we bedrijven betrokken waar ID-fraude in de afgelopen jaren vaker is voorgekomen (bijvoorbeeld banken).
- Fraudeopbrengst: ten slotte hebben wij ons op sectoren gericht waar de schade van ID-fraude groot kan zijn (bijvoorbeeld zorgverzekeraars).

Op basis van bovenstaande indicatoren zijn wij gekomen tot de volgende lijst met sectoren:

- Banken
- Financieringsmaatschappijen
- Verzekeraars
- Telecombedrijven
- Uitzendbureaus
- Ziekenhuizen
- Webwinkels
- Woningcorporaties

In elke sector hebben wij gesproken met twee bedrijven en een brancheorganisatie. Binnen de bedrijven spraken wij met mensen die verantwoordelijk zijn voor cliëntenregistratie, fraudebeheersing of de beveiliging van data- en ICT-systemen. In aanvulling daarop is gesproken met kennisinstellingen en bedrijven die een rol spelen in preventie en detectie van ID-fraude of cybercrime. De gesprekken hebben plaatsgevonden in september en oktober 2013.

1.2 Algemene bevindingen

De aanpak van ID-fraude valt vaak samen met de inspanningen die bedrijven doen om het contact met cliënten te vergemakkelijken en met hun inspanningen om cliënten beter te leren kennen (marketing-inspanningen). Kijkend naar de bedrijven en instellingen die wij hebben bezocht, vallen in dit kader drie algemene ontwikkelingen op:

Ontwikkelingen in het face to face contact
Met name grote instellingen en bedrijven investeren in de automatisering van het contact met hun cliënten. Deze investeringen hebben in de eerste plaats tot doel het contact te vergemakkelijken. Bij instellingen waar dit contact nog steeds face to face verloopt wordt in dit kader bijvoorbeeld steeds vaker gewerkt met een geautomatiseerde receptie (ontvangst). De klant meldt zich niet langer bij een balie maar bij een zuil, waar hij zich identificeert met een paspoort, ID-bewijs of cliëntenpas. Deze nieuwe praktijk is vergelijkbaar met het elektronisch inchecken bij luchtvaartmaatschappijen. Wij hebben deze ontwikkeling in het kader van dit onderzoek inmiddels gezien bij banken en ziekenhuizen.

In het geval van een ziekenhuis, meldt een patiënt voor electieve zorg (behandeling op afspraak) zich in de ontvangsthal van een ziekenhuis bij een zuil waar hij zijn ID-bewijs scant. Vervolgens ziet hij op een beeldscherm met wie en hoe laat hij een afspraak heeft. Hij kan deze informatie eventueel printen. Vergelijkbaar zijn de ontwikkelingen bij enkele grote Nederlandse banken, waar balies sinds kort zijn uitgerust met vergelijkbare ID-scanners bediend door baliepersoneel.

Zoals gezegd is deze ontwikkeling primair ingegeven door de wens om het contact met cliënten te vergemakkelijken, het biedt echter aanknopingspunten ter versterking van de persoonsverficatie. Bijvoorbeeld door de scan aan te vullen met een biometrische scan, bijvoorbeeld een irisscan of een vingerafdruk. De ervaringen met proefopstellingen zijn echter nog niet onverdeeld positief. Een pilot in de financiële wereld leverde veel mismatches op. Veel mensen werden geweigerd die niet geweigerd hadden moeten worden. Zolang biometrie niet is opgenomen in dergelijke systemen is de betrouwbaarheid van identificatie aan een balie nog steeds afhankelijk van face to face contact met een baliemedewerker, die nagaat of de persoon die zich meldt ook daadwerkelijk dezelfde is als die van het ID-bewijs.

Ontwikkelingen eID
Met de sterke ontwikkeling van het internet als verkoop- en servicekanaal, is er vrijwel geen sector meer waar persoonsverificatie op afstand (via internet) geen actueel onderwerp is. In vrijwel alle sectoren is het digitale contact tussen bedrijf en cliënt een gegeven. Afhankelijk van de aard van het product / de dienst hebben bedrijven er een kleiner of groter belang bij om de betrouwbaarheid te verifiëren van gegevens die de klant over zichzelf geeft. Zo zullen bepaalde webwinkels zich er alleen van willen verzekeren dat een klant ouder is dan 18 (omdat de wetgever dat voorschrijft, zoals bij de verkoop van tabak of drank), terwijl hypotheekverstrekkers zekerheid willen hebben over een hele brede verzameling van gegevens.

De ontwikkeling van eID is er een die direct voortkomt uit deze behoeften en waarvan de verwachtingen hoog zijn. Binnen het eID-stelsel in Nederland worden bestaande voorzieningen opgenomen, waaronder eHerkenning en DigiD. Het stelsel is in de afgelopen jaren ontwikkeld op initiatief van het ministerie van EZ en wordt nu doorontwikkeld. eID

voorziet in een behoefte aan een betrouwbare en gebruikersvriendelijkere identificatie. Sterk aan het systeem is dat de partij wiens gegevens moeten worden geverifieerd (bijvoorbeeld de consument) zelf bepaalt tot welke gegevens een bedrijf of instelling toegang krijgt. Een tweede sterke punt is dat het om een stelsel gaat waaraan meerdere partijen als provider verbonden zijn. Het systeem is daarmee niet afhankelijk van (de gezondheid) van één bedrijf.

In de afgelopen jaren hebben verschillende sectoren – vanwege het gebrek aan een eID-stelsel – zelf methoden ontwikkeld om identificatie op afstand mogelijk te maken. In de eerste plaats zijn er de webwinkels die in eigen beheer voor hun cliënten gebruikersaccounts (inlognaam en wachtwoord) aanmaken en zich vervolgens op basis van ervaringen met cliënten een beeld vormen van de betrouwbaarheid van die cliënten. In de tweede plaats zijn er sectoren waar bedrijven onderling data uitwisselen en daarmee elkaar helpen hun identificatie te versterken. Veel gebruikt in dit kader is de onderlinge identificatie of afgeleide identificatie waarbij een klant gevraagd wordt een summier bedrag over te maken. Een bedrijf maakt op deze manier gebruik van gegevens die elders over een cliënt zijn verzameld. In de derde plaats wordt hier en daar geëxperimenteerd met nieuwe methoden zoals spraakherkenning. Het biedt in de toekomst mogelijkheden om in het telefonische contact meer zekerheid te krijgen omtrent de identiteit van degene die belt.

Analyse van gedrag en voorkeuren van cliënten
Een derde algemene ontwikkeling hangt samen met de al langer lopende trend onder bedrijven en instellingen om steeds meer cliëntengegevens te verzamelen, te combineren en te verrijken teneinde meer inzicht te krijgen in het gedrag en de voorkeuren van die cliënten. Het is een ontwikkeling die vaak is ingegeven door marketingoverwegingen en nu ook steeds meer mogelijkheden biedt om ID-fraude tegen te gaan. Zo zijn banken al geruime tijd in staat om op basis van data over betaalgedrag van individuele klanten, ongebruikelijke transacties te detecteren die mogelijk wijzen op skimming of ander misbruik. Vergelijkbare data-analyses worden door telecombedrijven uitgevoerd om diefstal van telefoons (simkaarten) te detecteren.

Veel instellingen vullen hun cliëntgegevens aan met externe gegevens. Bijvoorbeeld de gegevens van VIS BV (Verificatie Informatie Systemen). Het is een systeem waarin online kan worden nagegaan of een identiteits- of reisdocument ongeldig is. Een branche waar daarnaast ook nog bedrijven onderling van elkaars informatiepositie gebruik maken is de financiële sector. Zo hebben zij een BKR stelsel en het Incidentwaarschuwingensysteem. Deze laatste is expliciet ingericht op fraudedetectie.

Door meerdere bedrijven en instellingen die actief bezig zijn met fraudedetectie via datamining is aangegeven dat deze detectie versterkt zou kunnen worden door aansluiting op de Gemeentelijke Basisadministratie Persoonsgegevens (GBA). Tevens is door enkele instellingen de wens uitgesproken om gebruik te kunnen maken van het Burger Service Nummer (BSN).

1.3 ID-fraude per branche

In navolging van het programma 'Identiteit op orde' hebben wij de volgende definitie van identiteitsfraude als uitgangspunt gebruikt: "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." Deze definitie dekt een zeer gevarieerde verzameling van

gedragingen af. Uit de gesprekken in de verschillende branches komt een gevarieerd beeld van modus operandi naar voren, dat per branche sterk verschilt.

Financiële instellingen
Financiële instellingen lopen ten opzichte van andere branches voorop in de aanpak van ID-fraude. Het belang van een effectieve aanpak is in deze branche erg groot. De bedragen die in fraude kunnen omgaan zijn hoog. De fraude manifesteert zich met name als skimming (het kopiëren van betaalpassen) en phishing (het ontfutselen van gegevens - zoals pincodes – bij cliënten). Hoewel fraude vaak voortkomt uit onoplettendheid van klanten of beheerders van betaalsystemen (bijvoorbeeld een winkelier met een pinterminal of een betaalautomaat bij een onbemand tankstation), nemen banken de verantwoordelijkheid voor de aanpak en detectie vaak zelf direct ter hand. Zo worden patronen in betaaltransacties continu gevolgd teneinde ongebruikelijke transacties die mogelijk voortkomen uit misbruik direct na te trekken. In dit verband beheren financiële instellingen gezamenlijk een fraudealarmeringssysteem, kunnen zij toetsen bij het BKR en hebben zij toegang tot het Verificatie en Informatiesysteem aan de hand waarvan kan worden nagegaan of specifieke ID-bewijzen als vermist of gestolen zijn opgegeven.

Een vorm van ID-fraude die naast skimming en phishing in de branche is geconstateerd is het openen van rekeningen die op naam zijn gesteld van mensen van wie het ID-bewijs is misbruikt. Er zijn aanwijzingen dat in georganiseerd verband nietsvermoedende mensen een kopie van het paspoort en een loonstrook afhandig wordt gemaakt. Deze mensen zijn bijvoorbeeld in de veronderstelling dat zij van doen hebben met de verhuurder van een appartement of met een toekomstig werkgever bij sollicitatie. In dit kader bestaat er illegale handel in kopieën van ID-bewijzen. Dergelijke spookrekeningen worden met name geopend bij instellingen die geen face to face contact hebben met (nieuwe) klanten maar hun verificatie doen aan de hand van een kopie van een ID-bewijs en een afgeleide check bij een branchegenoot.

Ziekenhuizen en zorgverzekeraars
Hoewel statistieken over ID-fraude in de zorg ontbreken, is het aannemelijk dat met name ziekenhuizen en zorgverzekeraars er mee te maken hebben. Het is immers aannemelijk dat er ook onder mensen die niet verzekerd zijn voor zorgkosten, behoefte aan een behandeling zal bestaan. Voor zover deze behoefte acuut (spoedeisend) is, hebben ziekenhuizen een zorgplicht en zullen zij mensen altijd helpen. Hiervoor bestaat een regeling met verzekeraars. Voor zover de behoefte niet acuut is maar toch dringend, zal ID-fraude door menige onverzekerde als wenkend perspectief worden gezien. De gesprekken in de branche leren dat dat nogal eens met medeweten gaat van de verzekerde (wiens ID wordt misbruikt). Zoals het geval van een vrouw die vanuit het buitenland naar Nederland komt om op naam van een zus een behandeling te ondergaan. Of een illegale werknemer die na een bedrijfsongeval op naam van een collega door een arts wordt geholpen.

Kenmerkend van ID-fraude in de zorg is dat degene wiens identiteit wordt misbruikt meestal niet de financieel benadeelde partij is; dat geldt ook voor degene die de zorgdienst verleend. De benadeelde partij is vrijwel altijd de verzekeraar.

Uitzendbureaus
ID-fraude manifesteert zich onder uitzendbureaus in de eerste plaats als illegale arbeid. Met name bij ongeschoolde en laagbetaalde arbeid wordt nogal eens gebruik gemaakt van werknemers uit landen met een lager loonniveau. Onder deze werknemers bevinden zich relatief veel mensen die niet over een werkvergunning beschikken (maar wel vergunningsplichtig zijn). Sinds de Inspectie SZW strak handhaaft en de boetes voor het in dienst hebben van illegale werknemers zijn verhoogd, is er bedrijven veel aan gelegen personen goed te identificeren.

Kenmerkend voor deze vorm van fraude is dat er vaak geen concreet aanwijsbare partij is die door de illegale arbeid direct wordt benadeeld. Het is in wezen een delict waarbij zowel de illegale werknemer (hij die ID-fraude pleegt), het uitzendbureau als de inlener voordeel kunnen hebben. Het is vooral een algemeen (abstract) maatschappelijk belang dat wordt benadeeld. De grootse motivatie van werkgevers om ID-fraude te detecteren komt dan ook voort uit de verantwoordelijkheid die zij bij wet opgelegd hebben gekregen.

Webwinkels
Webwinkels hebben een ambigue houding ten opzichte van betrouwbaarheid van persoonsgegevens. Voor hen hoeft het niet zoveel uit te maken of iemand werkelijk is die hij/zij zegt te zijn. 'Mensen kunnen zich bij ons eventueel uitgeven voor Sinterklaas en zij kunnen daarbij ook een willekeurig bezorgadres opgeven, zolang de rekening maar wordt betaald'. Voor enkele webwinkels geldt dat zij maar voor specifieke persoonsgegevens zekerheid willen hebben bijvoorbeeld over de leeftijd. Voor bijvoorbeeld de verkoop van tabak en alcohol zijn winkeliers verantwoordelijk gesteld voor een goede controle. Omdat fraude bij webwinkels meestal tevens gepaard gaat met een vorm van identiteitsfraude, heeft de sector toch een groot belang bij het identificeren en tegengaan van identiteitsfraude. Zowel de klant (wiens identiteit en/of rekeningnummer wederrechtelijk is gebruikt) als de webwinkel kunnen slachtoffer zijn. Identiteitsfraude is niet gekoppeld aan specifieke productsoorten, maar komt voor bij alle soorten producten, van kleding tot bedden, van speelgoed tot televisies.

Webwinkels hebben vooralsnog vooral last van mensen die na bezorging van het product de betaling laten terugdraaien, of mensen die bestellingen die voor anderen bestemd zijn onderscheppen (de zogenaamde hengelaars). Voor zover webwinkels te maken hebben met harde ID-fraude gaat het om gevallen waarbij betalingen worden gedaan vanaf een rekening waarvan de gegevens van de oorspronkelijke houder zijn gestolen. Het zijn transacties die voortkomen uit bijvoorbeeld phishing en skimming. Ook komt het veel voor dat bestellingen worden gedaan met niet-bestaande identiteiten. Webwinkels zijn beperkt in hun mogelijkheden om de identiteit van degene die een product bestelt te verifiëren.

Telecombedrijven
ID-fraude bij telecombedrijven manifesteert zich vooral als diefstal van telefoons (en de daarin opgenomen simkaarten). Over het algemeen zijn in die gevallen niet de telecombedrijven maar vooral de cliënten gedupeerd. Het is in principe de verantwoordelijkheid van de cliënt om diefstal tijdig te signaleren en door te geven aan politie en provider opdat het account kan worden geblokkeerd.

Maar ID-fraude leidt ook in deze sector vaak tot andere vormen van fraude, zoals wanbetaling (bij contracten). Dat kan enerzijds gevolgen hebben voor het bedrijf zelf, wanneer geen betalingen worden gedaan. Anderzijds kan het gevolgen hebben voor derden, indien zij betalen voor diensten of producten die zij niet hebben ontvangen. Een recent probleem is adresfraude, waarbij de facturen voor een abonnement naar een opzettelijk "verkeerd" opgegeven adres worden gestuurd. Dit probleem komt vooral voor bij de fysieke winkels die als intermediair optreden. Dan worden bijvoorbeeld binnen korte tijd, bij verschillende winkels in totaal 10 contracten op een bepaald adres afgesloten, maar er wordt nooit betaald.

Telecombedrijven kunnen de gegevens die klanten opgeven checken tegen gegevens van Preventel, een samenwerkingsverband tussen aanbieders van telecommunicatiediensten om te voorkomen dat personen en bedrijven verplichtingen voor het gebruik van telecommunicatiediensten aangaan die zij niet kunnen dragen.

Verzekeraars

Identiteitsfraude komt voor bij verschillende soorten verzekeringen. Misbruik in de verzekeringssector is een groot probleem, financieel gezien maar ook het imago en aantal klanten lijdt eronder. Het gaat doorgaans om omvangrijke bedragen. Bij levens-, ongevallen- en arbeidsongeschiktheidsverzekeringen komt het voor dat valse papieren worden gebruikt voor de verzekerde of de begunstigde. Ook komt het voor dat schadeverzekeringen met gestolen ID-bewijzen worden afgesloten op nep-adressen. Vaak gaat het om verzekeringspolissen die tegelijkertijd worden afgesloten bij meerdere verzekeraars. Schade vanwege één autodiefstal wordt dan bij meerdere verzekeraars geclaimd. Bij verzuimverzekeringen kan een werkgever een verzekering afsluiten op basis van het aantal personeelsleden en de gemiddelde loonsom. Wanneer een werknemer ziek wordt, kan een ander personeelslid met een hoger inkomen als ziek worden opgegeven. Dit is mogelijk omdat de werkgever het contact heeft met de bedrijfsarts en de werknemer, en de verzekeraar niet. Het komt ook voor dat nepbedrijven een verzuimverzekering afsluiten voor nepwerknemers met gestolen identiteiten, waarbij de werknemers vervolgens massaal ziek worden.

De verzekeraars hebben verschillende lijsten, protocollen en samenwerkingsverbanden om identiteitsfraude en verzekeringsfraude in het algemeen tegen te gaan. Zo is er in het kader van de 'Wet ter voorkoming van witwassen en financiering van terrorisme' (Wwft) een gedragscode voor verzekeraars waarbij integriteit hoog in het vaandel staat. De verzekeraars zijn daarmee verplicht om uit te zoeken wie de echte begunstigde is: ken uw klant (Know Your Customer: KYC). Ondanks alle bestaande maatregelen wordt minstens 90 procent van de fraude in de verzekeringssector nu niet opgepikt. Een groot probleem is dat identiteitsfraude voor verzekeraars bijna niet te controleren is. Een manco daarbij is dat combinaties van persoons- en adresgegevens niet proactief (d.w.z. voordat benadeling heeft plaatsgevonden) te verifiëren zijn.

2 Maatregelen bedrijfsleven

Uit het onderzoek komen een groot aantal maatregelen van het bedrijfsleven naar voren ter bestrijding van ID-fraude. De maatregelen lopen door te keten heen van preventie, via verificatie tot opsporing en omvatten maatregelen op het terrein van publieksvoorlichting, online verificatie, face to face verificatie, bedrijfsprocessen fraudeproof maken, praktische maatregelen, informatie-uitwisseling tussen bedrijven, technische innovaties, kennisdeling binnen sectoren, ondersteuning van slachtoffers en opsporing.

De maatregelen van het bedrijfsleven zijn ingedeeld in vijf categorieën conform de indeling in de kabinetsvisie, te weten:

1. Gezonde weerstand. Verbeteren van de weerstand van burgers en organisaties tegen identiteitsfraude.
2. Betrouwbare checkups. Verstevigen van de ijkpunten van de Nederlandse identiteitsinfrastructuur door de overheid en/of het individuele bedrijfsleven.
3. Vroege diagnose. Door samenwerking daders snel op het spoor komen en liefst voor zijn.
4. Adequate behandeling. Beter begeleiden van slachtoffers van identiteitsfraude en vlot herstellen van fouten.
5. Effectieve repressie. Daders straffen en buit terugpakken.

Indeling naar deze categorieën kan bij sommige maatregelen of nader in matrixvorm als arbitrair beschouwd worden. Met name het onderscheid bij de eerste drie categorieën. Nu is er voor gekozen om in de eerste categorie alleen de preventieve maatregelen in de zin van publieksvoorlichting op te nemen. Bij de tweede categorie ligt het zwaartepunt op maatregelen vanuit de overheid ter versteviging van de infrastructuur en maatregelen die bedrijven individueel nemen. De derde categorie heeft als zwaartepunt de collectieve samenwerking tussen bedrijven om ID-fraude te beperken.

2.1 Categorie 1: gezonde weerstand

Publieksvoorlichting

Banken informeren hun cliënten voortdurend via hun sites over de concrete risico's van fraude. Onder meer worden gebruikers van digitale bankportals gewezen op de risico's van phishing en skimming. Ook branchebreed zijn campagnes gevoerd zoals de advertentiecampagne 'Pas op uw persoonlijke gegevens' en is door de Nederlandse Vereniging van Banken de website geïntroduceerd 'Veilig Betalen en Bankieren'. Deze informeert consumenten over de maatregelen die de banken nemen en over de maatregelen die zij zélf kunnen nemen om veilig te bankieren.

Publieksvoorlichting	
Type maatregel:	Voorlichting
Doel:	Consumenten bewustmaken van risico's van (ID) fraude
Maatregel wordt genomen door:	Gezamenlijke Banken
Kenmerkend:	Preventieve maatregel
Uitvoerende organisatie:	NVB
Bron:	NVB

2.2 Categorie 2: betrouwbare checkups

eID en eHerkenning

We gaan steeds meer online doen, terwijl er niet goed controle mogelijk is op wie-wie is. Er zijn daarom ontwikkelingen gaande op het gebied van (Consumer) e-ID. Een concept vergelijkbaar met DigiD. Met eID zouden burgers in hun digitale contact met bedrijven, instellingen en overheden steeds gebruik kunnen maken van slechts één gebruikersnaam met een daaraan gekoppeld wachtwoord.

De ontwikkeling van eID wil men laten aansluiten op het al bestaande stelsel van eHerkenning. eHerkenning is een stelsel of platform dat is geïnitieerd door de overheid (ministerie van EZ) ter vereenvoudiging van het berichtenverkeer tussen overheid en bedrijfsleven. eHerkenning geeft bedrijven een digitale sleutel waarmee zij zich kunnen aanmelden bij overheden en (andere) bedrijven. Met deze sleutel kunnen zij inloggen, diensten afnemen, producten kopen, aanvragen doen (zoals een vergunning aanvraag), of hun status opvragen (bijvoorbeeld een verzekeringspolis inzien).

Binnen eHerkenning worden vijf typen van eHerkenningsmiddelen aangeboden, elk met een eigen betrouwbaarheidsniveau. Afhankelijk van de dienst waarvan het bedrijf gebruik wenst te maken, kiest hij een middel. Dit kan een eenvoudige gebruiksnaam met wachtwoord zijn maar ook een certificaat waarbij informatie wordt geverifieerd. De kosten van de verschillende eHerkenningsmiddelen lopen uiteen van € 6,00 tot € 90,00 per jaar.

eHerkenning is opgericht met een instellingsbesluit van het ministerie van Economische Zaken. In dit besluit is op hoofdlijnen de zeggenschap geregeld. De uitvoering is geheel in handen gelegd van private bedrijven. In het instellingsbesluit is hierover het volgende vastgelegd: 'Het Afsprakenstelsel eHerkenning wordt in opdracht van de minister beheerd door Logius, een Agentschap van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De diensten van eHerkenning worden in beginsel geleverd door marktpartijen. De afnemers van deze diensten zijn overheidsorganisaties en bedrijven die elektronische diensten aanbieden enerzijds en ondernemers die van deze diensten gebruik willen maken anderzijds. Al deze partijen krijgen zeggenschap over de inhoud en verdere ontwikkeling van de standaard eHerkenning'.

Idealiter ontstaat er op den duur een stelsel dat in de hele EU gebruikt kan worden (in plaats van een apart stelsel voor elk land). De ontwikkelingen vergen echter veel tijd.

Het stelsel zou verder versterkt kunnen worden door een verbinding te maken met het fysieke paspoort (of ID-bewijs) via de chip op dit document. Via een scanner zouden bedrijven in hun face to face contact met cliënten gegevens uit eID direct (geautomatiseerd) kunnen verifiëren met het document waarmee een cliënt zich aan de balie legitimeert.

Er zijn ook ontwikkelingen die het mogelijk kunnen maken om de chip in combinatie met de telefoon te gebruiken.

eID en eHerkenning	
Type maatregel:	Elektronische legitimatie
Doel:	Vereenvoudigen van berichtenverkeer tussen bedrijven en overheden, borgen van betrouwbaarheid van legitimatie

Maatregel wordt genomen door:	Overheid in samenwerking met bedrijven
Kenmerkend:	Publiek private samenwerking
Uitvoerende organisatie:	Welcome, Connectis, KPN, DigidentityCreaim, Gemnet
Bron:	http://www.eherkenning.nl

Onderlinge identificatie / afgeleide ID-check

In een aantal sectoren maken bedrijven gebruik van elkaars cliëntenverificatie. Dit gebeurt bijvoorbeeld bij banken. Banken zonder een fysiek kantorennetwerk (of een beperkt netwerk) vervangen dan hun face to face identificatie bij de intake van nieuwe cliënten door verificatie van cliëntgegevens bij branchegenoten. In de praktijk gebeurt dit door een cliënt een miniem bedrag (1 eurocent) te laten overmaken van zijn oude rekening naar de nieuwe (te openen) rekening. De bank haalt via deze transactie persoonsgegevens binnen aan de hand waarvan de door de nieuwe cliënt opgegeven gegevens kunnen worden geverifieerd.

Deze methoden van verificatie wordt ook veel toegepast in de telecombranche bij het afsluiten van contracten voor mobiele telefonie. Bij overmaken van gelden naar de klant wordt gebruik gemaakt van de naam, nummer controle bij Equens. Een financiële instelling is juist afgestapt van deze methode. In het verleden is voor één van de labels gebruik gemaakt van de één cent overmaakstrategie om er achter te komen dat een naam is gekoppeld aan een rekeningnummer. Dit werpt drempels op voor de klant en daarom is men daar van afgestapt. Ook nadat is gekeken naar de werkwijze van de belangrijkste concurrenten die het veelal ook niet doen. Rekeningen kunnen bij enkele banken, zoals Triodos en ASN, geopend worden op basis van een kopie legitimatiebewijs. Wat deze controle afzwakt.

Onderlinge identificatie / afgeleide ID-check	
Type maatregel:	Verificatie van persoonsgegevens bij intake
Doel:	Verificatie van gegevens die door clienten zijn verstrekt
Maatregel wordt genomen door:	Banken, financieringsinstellingen, telecombedrijven
Kenmerkend:	Lage kosten, laagdrempelig
Uitvoerende organisatie:	
Bron:	o.a. NVB, SNS, T-mobile

Lokale elektronische patiëntendossiers bij ziekenhuizen

De invoering van de identiteitsplicht in 2006 is voor ziekenhuizen een mijlpaal gebleken voor de aanpak van identiteitsfraude. Sindsdien wordt van iedere burger verwacht dat hij zich te allen tijde kan legitimeren met een paspoort of ID-bewijs. Het betekent dat iedere patiënt, of hij zich nu tot een ziekenhuis wendt voor electieve zorg (op afspraak) of voor spoedeisende hulp, gevraagd kan worden zich te legitimeren. In de praktijk van de intake voor electieve zorg geldt identificatie inmiddels als een voorwaarde. Zonder legitimatie is intake niet mogelijk[1]. Een patiënt die zich voor de eerste keer meldt moet een paspoort of ID-bewijs overleggen, vervolgens wordt voor deze patiënt een zorgpas aangemaakt. Veel ziekenhuizen maken op dit moment ook een pasfoto van de patiënt die aan het lokale elektronische dossier van de patiënt wordt toegevoegd. In een later stadium kan een behandelend arts aan de foto zien of

[1] Hierbij moet worden opgemerkt dat de coulance – jegens hen die aangeven hun ID-bewijs vergeten te zijn - per ziekenhuis verschilt.

de patiënt die de behandeling krijgt, dezelfde is als degene die zich bij de intake heeft gelegitimeerd.

Ondanks de identificatieplicht komt ID-fraude nog wel voor, vooral bij spoedeisende hulp. In de praktijk kan de identificatieplicht niet goed worden gecombineerd met de medische zorgplicht van ziekenhuizen. De ID-plicht is in een situatie waarin acuut zorg moet worden geboden niet handhaafbaar. Een patiënt in acute medisch nood moet geholpen worden of hij zich nu kan identificeren of niet.

Een aantal ziekenhuizen hebben de ontvangst van patiënten vergaand geautomatiseerd. Hier kunnen patiënten zich bij een zuil met een scanner melden. Deze scanner leest een zorgpas of paspoort uit en informeert de patiënt over zijn afspraak. Zo ziet de patiënt hoe laat en waar hij een afspraak heeft met welke arts.

Lokale elektronische patiëntendossiers bij ziekenhuizen	
Type maatregel:	Legitimatieprocedure
Doel:	Identificatie van patiënten
Maatregel wordt genomen door:	Ziekenhuizen
Kenmerkend:	
Uitvoerende organisatie:	Ziekenhuizen
Bron:	NVZ en ziekenhuizen

Vijfvoudige ID-check bij woningbouwverenigingen

Woningbouwverenigingen voeren doorgaans bij de intake van nieuwe (toekomstige) bewoners een vijfvoudige ID-check uit. Zij maken daarbij gebruik van verschillende bronnen. Een ieder die zich inschrijft moet de volgende documenten overleggen:

- inkomensverklaring
- ID-bewijs (paspoort)
- IB-60 formulier (verklaring van de Belastingdienst)
- verhuurdersverklaring (verklaring van verhuurder waar eerder is gehuurd)
- Uittreksel GBA

Wat de persoonsverificatie sterk maakt is dat deze altijd face to face aan een balie plaatsvindt.

Vijfvoudige ID-check bij woningbouwverenigingen	
Type maatregel:	Persoonsverificatie aan de balie
Doel:	Verificatie
Maatregel wordt genomen door:	Woningbouwverenigingen
Kenmerkend:	
Uitvoerende organisatie:	Woningbouwverenigingen
Bron:	Aedes

Algemene keurmerken (ISO & NEN)

Veel van de bedrijven die werken met persoonsgegevens zijn ISO 27001 gecertificeerd, voor de beveiligde opslag en verwerking van persoonsgegevens. Doelen van ISO 27001 zijn:

- Vertrouwelijkheid garanderen dat informatie alleen toegankelijk is voor daartoe geautoriseerde personen.
- Integriteit waarborgen de accuraatheid en volledigheid van informatie en informatieverwerkingsmethoden.

- Beschikbaarheid garanderen dat geautoriseerde gebruikers toegang hebben tot informatie en de daarmee verbonden middelen wanneer dit nodig is.

ISO/IEC 27001:2005, is een "information security management system" (ISMS) standaard gepubliceerd in oktober 2005 door de Internationale Organisatie voor Standardisering (ISO) en de Internationale Electrotechnische Commissie (IEC). Op 25 september 2013 is een nieuwe versie beschikbaar gekomen: ISO/IEC 27001:2013. ISO/IEC 27001 specificeert dat informatiebeveiliging formeel onder expliciete managementcontrole wordt gebracht. Een formele specificatie betekent dat voldaan moet worden aan specifieke vereisten. Organisaties die beweren aan ISO/IEC 27001 te voldoen, kunnen daarom formeel worden geaudit en gecertificeerd in overeenkomst met de standaard. De standaard beslaat in hoofdzaak 11 domeinen:

1. Beveiligingsbeleid op management niveau
2. Organisatie van en sturing op informatiebeveiliging
3. Inventarisatie en classificatie van informatie assets
4. Personeelsbeveiliging – beveiligingsaspecten ten aanzien van employees die de organisatie binnenkomen en verlaten, en die binnen de organisatie van plaats veranderen
5. Fysieke en omgevingsbeveiliging – bescherming van computer faciliteiten
6. Communicatie and operationeel management - management van technische beveligingscontroles in systemen en netwerken
7. Toegangscontrole – Restrictie van toegangsrechten op netwerken, systemen, applicaties, functies en gegevens
8. Information systemen: aanschaf, ontwikkeling en onderhoud – het inbouwen van beveiliging in applicaties
9. Management van incidenten – Anticiperen en reageren op lekken / gaten in informatie beveiliging
10. Management van bedrijfscontinuiteit - bescherming, onderhoud en terughalen van bedrijfskritieke processen en systemen
11. Compliance - ensuring conformance with information security policies, standards, laws and regulations

De NEN 7510-norm is afgeleid van ISO 27001, gericht op informatiebeveiliging binnen de gezondheidszorg. Het geeft zorginstellingen handvatten voor het inrichten van adequate ICT-systemen Doel is het waarborgen van de beschikbaarheid, integriteit en vertrouwelijkheid van alle informatie ten behoeve van verantwoorde zorg voor patiënten. Naast het borgen van kwaliteit moeten de informatiebeveiligingsmaatregelen volgens de norm zo zijn ingericht dat ze zijn te controleren.. De NEN 7510 dekt het hele gebied van informatiebeveiliging, van technische specificaties tot richting geven aan de organisatie en het menselijk handelen.
De audits op ISO en NEN-standaarden worden uitgevoerd door commerciële partijen. Doorgaans wordt 1x per jaar een controle uitgevoerd of het bedrijf veilig omgaat met de gegevens, waarbij tevens een toets op naleving van de WBP (Wet Bescherming Persoonsgegevens) wordt gedaan.

Algemene keurmerken	
Type maatregel:	Organisatorisch
Doel:	Borgen van kwaliteit rond opslag en verwerking van persoonsgegevens
Maatregel wordt genomen door:	Bedrijven

Kenmerkend:	Zelfregulering
Uitvoerende organisatie:	Audit bedrijven
Bron:	Verzekeraars, telecombedrijven, uitvoerder van controle van ID-bewijzen, www.dnvba.com, *www.bsigroup.nl*

Automatisch watermerken van kopieën van ID-bewijzen

In de financiële sector komt het regelmatig voor dat kopieën van ID-bewijzen worden misbruikt. Er zijn signalen van een illegale handel in kopieën, bijvoorbeeld door ex-werknemers van instellingen die dergelijke kopieën verzamelen van klanten. Dergelijke handel zou in de toekomst enigszins kunnen worden beperkt wanneer kopieën slechts voor één doeleinde kunnen worden gebruikt. Wanneer er bijvoorbeeld in een belwinkel een kopie wordt gemaakt van een paspoort dan zou op die kopie automatisch een watermerk moeten komen te staan van de betreffende belwinkel. De kopie kan dan later minder makkelijk opnieuw worden gebruikt voor bijvoorbeeld het openen van een bankrekening.
De omgang met kopieën van ID-bewijzen binnen bedrijven zou onderdeel kunnen worden van kwaliteitsmanagementsystemen. Het zou bijvoorbeeld geintegreerd kunnen worden met ISO-certificering.

Automatisch watermerken van kopieën van ID-bewijzen	
Type maatregel:	Technisch & organisatorisch
Doel:	Preventie handel in kopieën van ID-bewijzen
Maatregel wordt genomen door:	
Kenmerkend:	Wordt nog niet uitgevoerd, wel wordt aanbevolen om met pen of anderszins de datum en het doel op de kopie te schrijven
Uitvoerende organisatie:	
Bron:	Interviews

Casemanagement aan de hand van modus operandi

Een eigen onderzoeksteam doet onderzoek naar identiteitsfraude. De ervaringen uit onderzoeken worden gebruikt om bestaande processen daar waar nodig aan te passen om fraude verder te voorkomen. Een simpele maatregel is bijvoorbeeld om een werkgever na te bellen op een vast telefoonnummer. Verder wordt de ervaring uit die onderzoeken gebruikt om het monitoringsysteem te finetunen. In zijn algemeenheid worden de gegevens opgenomen in een monitoringsysteem, zodat historische data wordt opgebouwd. Bij calamiteiten wordt nagegaan wat men kan leren uit de wijze waarop de dader te werk is gegaan en vervolgens hoe men dat kan herkennen respectievelijk kan voorkomen. Aan de hand van de modus operandi wordt herleid hoe de crimineel er voor zorgt dat de misdaad lukt en hoe de identificatie van de dader wordt tegengegaan zodat men “buiten schot” blijft. Door dit in kaart te brengen komt men op mogelijkheden om misbruik te voorkomen.

Casemanagement aan de hand van modus operandi	
Type maatregel:	Monitoring
Doel:	Verificatie van betrouwbaarheid cliënten
Maatregel wordt genomen door:	Financiële instellingen
Kenmerkend:	Verificatie via technologie

Uitvoerende organisatie:	Financiële instellingen
Bron:	Interviews

Scanningsapparatuur ID-documenten aan de balie

Onlangs heeft een uitrol plaatsgevonden van scanners op de kantoren van de grotere banken. Met deze scanners kunnen verblijfsvergunningen, paspoorten en ID-bewijzen op creditcardformaat gescand worden van over de hele wereld (dus geen papieren rijbewijzen, maar aangezien deze sinds oktober 2006 niet meer worden uitgegeven wordt dat steeds minder een probleem). Vooral de fraude met valse rijbewijzen kan hierdoor voorkomen worden. De scanner maakt een PDF en kan handmatig gekoppeld worden met een systeem van Customer Relationship Management (CRM). In de nabije toekomst is er de mogelijkheid om de koppeling elektronisch te laten plaatsvinden geïntegreerd in het CRM-systeem, waarbij automatisch velden worden gevuld. In de verre toekomst is biometrische scanning een overweging.
Indien er twijfel is over het ID-bewijs zal de baliemedewerker daar overleg over voeren op de locatie. Als de aanvrager kwaad in de zin heeft en dit merkt dan zal dat meestal het signaal zijn om zo snel mogelijk de deur uit te lopen.

Scanningsapparatuur ID-documenten aan de balie	
Type maatregel:	Verificatie persoonsgegevens bij intake
Doel:	Verificatie van gegevens die door cliënten zijn verstrekt
Maatregel wordt genomen door:	Financiële instellingen
Kenmerkend:	Verificatie via technologie
Uitvoerende organisatie:	Financiële instellingen
Bron:	Interviews

Foto-op-foto vergelijking

Werkgevers zijn verplicht om hun werknemers te identificeren. Met de Wet Ketenaansprakelijkheid zijn zij ook verantwoordelijk voor identificatie van personeel dat zij via een derde partij (zoals een uitzendbureau) inhuren. Dit moet voorkomen dat werkgevers personeel zonder werkvergunning in dienst hebben. De boetes die kunnen worden opgelegd zijn fors (€ 8.000 per werknemer). Het heeft geleid tot een toename van inspanningen onder werkgevers om ID-fraude tegen te gaan.

In sectoren waar veelvuldig via uitzendbureaus gebruik wordt gemaakt van flexibel inzetbaar buitenlands personeel, is de kans op lookalike-fraude groot. De identiteit is voor het ongeoefende oog van veel werkgevers lastig te verifiëren aan de hand van een pasfoto in een paspoort of ID-bewijs.

Bedrijven met een groot risico op lookalike-fraude zoals slachterijen en tuinderijen geven daarom soms zelf werknemerspassen uit, en controleren dagelijks aan de poort. Afhankelijk van de herkomst van het personeel houdt deze controle onder meer een foto-op-foto vergelijking in. Hierbij wordt ter plekke van de werknemer een pasfoto gemaakt welke vervolgens wordt vergeleken met de foto op de werknemerspas of de foto op het paspoort/identiteitsbewijs.

Foto-op-foto vergelijking	
Type maatregel:	Organisatorisch
Doel:	Detectie van lookalike-fraude
Maatregel wordt genomen door:	Bedrijven met flexwerkers

Kenmerkend:	
Uitvoerende organisatie:	Bedrijven met flexwerkers
Bron:	Uitzendbureau

Training van personeel t.b.v. preventie van ID-fraude

In Nederland bestaat een tiental bedrijven dat op commerciële basis trainingen aanbiedt op het terrein van preventie van ID-fraude (waaronder de detectie van valse identiteitsbewijzen). De sectoren die door deze trainingsbureaus worden bediend lopen uiteen van ziekenhuizen, banken, woningcorporaties tot gemeenten. Een dergelijk training beslaat doorgaans een of twee dagdelen. Onderwerpen die aan de orde komen zijn:

- Controleren van ID-documenten aan de hand van echtheidskenmerken
- Omgaan met verificatiesystemen
- Kennis over vervalsingen en veelgebruikte vervalsingsmethoden
- Vaardigheden m.b.t. het herkennen van mensen met een verhoogd risico op ID-fraude
- Wetgeving
- Handhaving (wat te doen in een concreet geval van ID-fraude?)

Een aantal bureaus biedt online trainingen aan (e-learning).

Training van personeel t.b.v. ID-fraude	
Type maatregel:	Organisatorisch
Doel:	Verificatie van ID-bewijzen
Maatregel wordt genomen door:	Bedrijven en overheden
Kenmerkend:	
Uitvoerende organisatie:	Diverse private partijen en de Marechaussee
Bron:	Diverse aanbieders van trainingen

Handboeken voor herkenning van (buitenlandse) identiteitsdocumenten

Er zijn verschillende verificatienaslagwerken en referentieboeken beschikbaar voor werkgevers, overheden en uitvoeringsinstellingen en voor meer specifieke sectoren als de advocatuur, gezondheidszorg en banken. Een voorbeeld hiervan is WIDboek.nl® (uitgegeven door PG-Support), een verificatieboek met kleurechte voorbeelden en beschrijvingen van paspoorten, identiteitskaarten, Nederlandse verblijfsvergunningen en -aantekeningen, visa en rijbewijzen in boekvorm op A5-formaat. Een ander voorbeeld is de Keesing Identity Checker. Dergelijke handboeken helpen de ruim 220 verschillende modellen te herkennen die in Nederland gebruikt mogen worden als geldig identiteitsbewijs bij arbeid.
De naslagwerken zijn in te zetten in combinatie met training in documentherkenning en gebruik van digitale MRZ (Machine Readable Zone) - readers.

Handboeken	
Type maatregel:	Off-line verificatie van identiteitsdocumenten
Doel:	Vervalste / gestolen / ongeldige identiteitsdocumenten herkennen
Maatregel wordt genomen door:	Bedrijven (waaronder specifieke beroepsgroepen en sectoren)
Kenmerkend:	
Uitvoerende organisatie:	Diverse private partijen
Bron:	www.pgsupport.nl, https://keesingreferencesystems.com, uitzendbureaus en -brancheorganisatie

Online verificatie van identiteitsdocumenten

Omdat het opslaan en controleren van kopieën van identiteitsdocumenten onder andere in de uitzendbranche steeds belangrijker is geworden, bieden een aantal bedrijven een online controle aan van identiteitsdocumenten. Dit gebeurt bijvoorbeeld door middel van een communicerend kastje (paspoort of document reader op locatie) waarin het identiteitsdocument moet worden geplaatst, of op basis van een digitaal opgestuurde scan of foto van het identiteitsdocument. Met behulp van OCR-technologie wordt de Machine Readable Zone (MRZ) uitgelezen en kan binnen tien seconden worden vastgesteld of het document echt, vals of onverwerkbaar is. De codecombinaties van het document worden vergeleken met een referentiedatabase. Het computerprogramma Edison Travel Documents (Edison TD) bevat meer dan 2500 verschillende soorten reisdocumenten uit ongeveer tweehonderd verschillende landen.

Zo is te controleren of de MRZ-gegevens op het legitimatiebewijs aan de ICAO-standaard voldoen. De klant ontvangt digitaal alle informatie die in het document staat en een digitaal rapport met de bevindingen, hetgeen de klant ook aan de inlener kan doorsturen. Alle gegevens van het document kunnen worden verwerkt en aan de klant teruggeleverd worden, zodat dossiers up-to-date kunnen worden gehouden. De digitale kopieën en rapporten worden in een beveiligde archiefomgeving opgeslagen.

Bovenop de MRZ-controle is een uitgebreidere controle op falsificatie of diefstal van het identiteitsdocument mogelijk. De digitale kopie van het document wordt dan tevens gecontroleerd op pasfotovervanging en gebruikte lettertypes. Ook kan deze door ID-experts (met marechaussee-ervaring) handmatig nader bekeken en gecontroleerd worden op kenmerken als achtergrondbedrukking, stempels, image, microtekst, etc. Aanvullend kan gecheckt worden of het document als vermist of gestolen is opgegeven.

Digitale ID-documentverificatie kan worden ingezet voor bijvoorbeeld screenen van toekomstige werknemers of uitzendkrachten, tewerkstellingsvergunningen, in het kader van Know Your Customer programs en de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). Online ID-verificatie lijkt effectief en gebruiksvriendelijk, bedrijven hoeven minder gebruik te maken van handboeken, blauwe lampen etc. Bij een volledige check kan het controlerende bedrijf de verantwoordelijkheid op zich nemen voor een eventuele boete in geval van bijv. vervalsing.

Lookalike-fraude kan digitaal nog niet worden geïdentificeerd. Hiervoor zijn wel ontwikkelingen in gang (o.a. gezichtsherkenning, vingerafdrukken).

Online verificatie van identiteitsdocumenten	
Type maatregel:	Online verificatie van identiteitsdocumenten
Doel:	Vervalste / gestolen / ongeldige identiteitsdocumenten herkennen
Maatregel wordt genomen door:	Bedrijven (waaronder specifieke beroepsgroepen en sectoren)
Kenmerkend:	
Uitvoerende organisatie:	Diverse private partijen
Bron:	www.id-checker.com , www.keesingdocumentscan.com, ID-Checker, uitzendbureaus

On-site verificatie van identiteitsdocument (DVD)

Een variant op de online verificatie is de on-site verificatie. Voor deze verificatie is geen internetverbinding nodig. Bij deze variant worden documenten gecontroleerd aan de hand van een database op DVD of Intranet.

On-site verificatie van identiteitsdocumenten	
Type maatregel:	On site verificatie van identiteitsdocumenten
Doel:	Vervalste / gestolen / ongeldige identiteitsdocumenten herkennen
Maatregel wordt genomen door:	Bedrijven (waaronder specifieke beroepsgroepen en sectoren)
Kenmerkend:	
Uitvoerende organisatie:	Diverse private partijen
Bron:	www.id-checker.com , www.keesingdocumentscan.com, ID-Checker, uitzendbureaus

Kopen en delen van adresgegevens

In Nederland zijn enkele bedrijven actief op het gebied van beheersing van kwaliteit van data (waaronder cliëntgegevens). Een voorbeeld is: 'Communicatie Data Diensten Nederland' (CDDN). Dit bedrijf beheert onder meer een platform waarbij persoonsgegevens uit verschillende bronnen worden gecombineerd. Daarmee verschaffen zij onder andere aan bedrijven inzicht in de verblijfplaats van hun klanten en of hun gegevens nog correct zijn. Andere voorbeelden van bedrijven die dergelijke diensten bieden zijn Experian, Risk Solutions – Focum en Cendris.

Kopen en delen van adresgegevens	
Type maatregel:	Kopen en delen van adresgegevens
Doel:	Onderhoud van cliëntenbestanden
Maatregel wordt genomen door:	
Kenmerkend:	Geheel privaat initiatief
Uitvoerende organisatie:	Private dataleveranciers
Bron:	o.a. CDDN

Mobiele verificatie aan de deur

Een aantal bedrijven waarbij het contact met cliënten vooral online verloopt, voert identiteitsverificatie via een terminalverbinding aan de deur van de cliënt uit. Zij maken hiervoor gebruik van koeriers die zijn uitgerust met een apparaat waarmee ID-bewijzen kunnen worden gecheckt. Deze koeriers zijn vaak ook getraind op persoonsidentificatie en verificatie van documenten. Dergelijke identificatie door de koerier wordt bijvoorbeeld toegepast bij de aflevering van decoders voor telecomdiensten of bij de aflevering van duurdere producten.

Mobiele verificatie aan de deur	
Type maatregel:	Online verificatie

Doel:	Verificatie van ID-bewijs en identificatie
Maatregel wordt genomen door:	Online retail bedrijven (waaronder telecombedrijven)
Kenmerkend:	Geheel privaat initiatief
Uitvoerende organisatie:	Private koeriersbedrijven
Bron:	Webwinkel

Controle op telefonische betrouwbaarheid

Bij twijfel van de identiteit van de persoon wordt aanvullend gebruik gemaakt van Experian en Autotrace. Bij bepaalde leningen is het mogelijk om na aflossing heropnames te doen. Controle op telefonische betrouwbaarheid (identiteit) geschiedt aan de hand van controlevragen. In geval van twijfel wordt de persoon ter verificatie teruggebeld.

Controle op telefonische betrouwbaarheid	
Type maatregel:	Telefonische verificatie
Doel:	Identiteit klant verifiëren aan de hand controlevragen
Maatregel wordt genomen door:	Financiële instellingen
Kenmerkend:	Alleen bij twijfel identiteit uitgevoerd
Uitvoerende organisatie:	Financiële instellingen
Bron:	Interviews

Geautomatiseerde herinnering

Bij veel ziekenhuizen hoeft een patiënt zich niet voor elke opname te legitimeren maar geldt een legitimatietermijn. Doorgaans is dat een periode van twee jaar. Dit betekent dat een patiënt die eenmaal een zorgpas heeft, daar twee jaar mee terecht kan. Na deze periode moet hij zich opnieuw legitimeren met een paspoort of ID-bewijs. De meeste ziekenhuizen hebben een geautomatiseerd herinneringssysteem.

Geautomatiseerde herinnering	
Type maatregel:	Automatisering
Doel:	Borgen van betrouwbaarheid van legitimatie van burgers
Maatregel wordt genomen door:	Ziekenhuizen
Kenmerkend:	
Uitvoerende organisatie:	Ziekenhuizen
Bron:	Ziekenhuizen, Vereniging van Ziekenhuizen

Stemherkenning

Sommige banken zijn bezig met een pilot Stemherkenning, waarbij telefonisch kan worden herkend of men al of niet te goeder trouw is. Enkele banken werken daar al mee. Een groeiend aantal banken onderzoekt de mogelijkheden van biometrie als beveiligingsmiddel. De overheid zal eerst moeten vastleggen hoe deze mogelijkheden kunnen worden ingezet. Momenteel worden ze nog niet gebruikt. Het is ook telkens een kostenafweging versus het risico dat men loopt als bedrijf en als maatschappij. Het zou een substantiële kostenpost zijn om bij alle balies biometrische scanapparatuur te plaatsen, terwijl de schadeomvang dat momenteel niet rechtvaardigt.

Stemherkenning	
Type maatregel:	Opsporing

Doel:	Verzamelen bewijsmateriaal tegen verdachten
Maatregel wordt genomen door:	Enkele financiële instellingen
Kenmerkend:	In beginstadium
Uitvoerende organisatie:	Enkele financiële instellingen
Bron:	Interviews

Controle en monitoring aanvraagproces

Bij aanvragen via een papieren aanvraagformulier of via het internet wordt gevraagd een kopie van het legitimatiebewijs, bankrekeningnummer en salarisstrook op te sturen. Aan de hand daarvan vinden checks plaats bij bijvoorbeeld BKR. Op het aanvraagsysteem wordt gemonitord met een geavanceerd rule based monitoringsysteem, waarbij op basis van een substantieel aantal indicatoren alerts worden afgegeven. Combinaties van historische data (datamining) kan met een rule tot een fraudealert leiden om extra onderzoek te verrichten en dieper te graven. Voorbeeld van indicatoren zijn een gratis e-mail extension (gmail of hotmail), adressen met hoogbouw etc. Daarbij maakt men gebruik van hoogbouwdata van Cendris. Fraudeurs maken gebruik van hoogbouw c.q. portieken met brievenbussen, omdat ze controle kunnen uitoefenen op de poststroom in het geval van een valse aanvraag.
Het komt ook voor dat bij aanvraag van een laag krediet onder de € 2.500 alleen een kopie van het legitimatiebewijs wordt verlangd en een natte handtekening op de overeenkomst en bij hogere kredietaanvragen dat men ook een recente salarisstrook en bankafschrift moet meesturen. Teams van underwriters zijn vaak goed getraind. Er wordt daarbij gebruik gemaakt van Experian en Datachecker / Focum. Per raadpleging kost dat enkele euro's. Via Datachecker kan het legitimatiebewijs geautomatiseerd verder gecontroleerd worden (een paspoort, een identiteitskaart, een verblijfsvergunning, een rijbewijs). De rapportages kunnen in een beveiligde database opgeslagen worden en zijn altijd oproepbaar. Ook kan men met adresonderzoek een adres en de persoonsgegevens in relatie tot het adres verifiëren. Ook kan men het betalingsrisico inschatten via een kredietwaardigheidscontrole op basis van informatie van het incassobureau. Bij hoge kredieten wordt tegenwoordig ook de werkgever gebeld of de persoon daadwerkelijk in dienst is tegen het opgegeven salaris. Bij een ID-overname doet men vaak aanvragen bij meerdere financiële partijen. Het komt voor dat meerdere financiële instellingen vervalsingen ongeveer op hetzelfde moment signaleren.

Het beleid is aangifte te doen bij strafbare feiten, tenzij er zwaarwegende argumenten zijn om dat niet te doen. Dit soort zaken wordt aan een interne Commissie voorgelegd ter beoordeling. Zelfs als de leesfunctie van Outlook openstaat kan een besmetting optreden waardoor een "trojan" op de computer kan worden geplaatst. Deze trojan kan dan cruciale informatie van de klant doorsturen naar de crimineel, of tijdens een internetsessie een extra betaling toevoegen.
De politie loopt minder hard als het om één individu gaat, maar als het om een cluster van individuen gaat zal de inspanning van de politie groter zijn. De Electronic Crime Task Force Driebergen kan hier dan op ingezet worden: http://www.cpni.nl/projecten/electronic-crimes-taskforce-ectf . Oplichting kan ook gemeld worden bij het Landelijk Meldpunt Internetoplichting in Heemskerk in samenwerking met Marktplaats: https://www.mijnpolitie.nl/if.shtml en het Landelijk Meldpunt Skimmen in Den Bosch samen met Equens http://www.politie.nl/onderwerpen/skimming.html

Controle en monitoring aanvraagproces

Type maatregel:	Verificatie persoonsgegevens bij intake
Doel:	Verificatie van gegevens die door cliënten zijn verstrekt
Maatregel wordt genomen door:	Financiële instellingen
Kenmerkend:	Verificatie via aanvullende bronnen
Uitvoerende organisatie:	Financiële instellingen
Bron:	Interviews

Monitoring op verdachte transacties

Met een rule based systeem kan worden ingebroken in het autorisatieproces. Stel er zijn meerdere valse aanvragen (identiteitsfraude) in een bepaald gebied, dan kan het postcodegebied worden gecombineerd met Automatic Teller Machine (ATM)-autorisaties in een bepaalde rule en daarmee een alert of een decline genereren bij een poging geld op te nemen bij een geldautomaat. Een ander voorbeeld is als kaarthouders geïdentificeerd kunnen worden en met name via welke IP-adressen en welke devices eerdere betrouwbare / rechtmatige transacties zijn uitgevoerd dan kan dat geauthentiseerd bijgehouden worden in een riskbased geautomatiseerd systeem.

Monitoring op verdachte transacties	
Type maatregel:	Monitoring
Doel:	Verificatie van betrouwbaarheid cliënten
Maatregel wordt genomen door:	Financiële instellingen
Kenmerkend:	Verificatie via technologie
Uitvoerende organisatie:	Financiële instellingen
Bron:	Interviews

2.3 Categorie 3: vroege diagnose

Branchespecifieke keurmerken voor ID-controle

De uitzendbranche heeft een SNA keurmerk (Stichting Normering Arbeid). Dit keurmerk stelt eisen aan het proces van opslag en controle van identiteitsgegevens door uitzendbureaus. Op de SNA website is een register opgenomen met gecertificeerde bedrijven. Lidmaatschap van ABU vereist registratie bij SNA.

Branchespecifieke keurmerken voor ID-controle	
Type maatregel:	Organisatorisch
Doel:	Borgen van kwaliteit rond opslag en verwerking van persoonsgegevens
Maatregel wordt genomen door:	Bedrijven
Kenmerkend:	Zelfregulering
Uitvoerende organisatie:	Audit bedrijven
Bron:	ABU, www.normeringarbeid.nl/

Fraude-overleg binnen de sector

De zes grootste telecomaanbieders van Nederland voeren periodiek "operationeel fraude-overleg" waarin mogelijke maatregelen worden besproken om fraude te beperken. Vergelijkbaar fraudeoverleg wordt gevoerd binnen de branche van financieringsondernemingen. In het overleg worden nieuwe ontwikkelingen met betrekking tot modus operandi van fraudeurs uitgewisseld.

Fraude-overleg binnen de sector

Type maatregel:	Organisatorisch
Doel:	Kennisuitwisseling
Maatregel wordt genomen door:	Telecombedrijven, financieringsinstellingen en banken
Kenmerkend:	Geheel privaat initiatief
Uitvoerende organisatie:	Brancheorganisaties
Bron:	interviews

Incidentenwaarschuwingssysteem financiële instellingen

Banken, financieringsondernemingen, en verzekeraars zijn gezamenlijk gekomen tot het 'Protocol Incidentenwaarschuwingssteem Financiële instellingen' (PIFI). Dit protocol is een register waarin malafide cliënten worden opgenomen. Dit register wordt aangeduid als het Incidentenregister.

Het protocol is er op gericht om (rechts)personen die een financiële instelling willen schaden of op oneigenlijke gronden gebruik maken van diensten van de financiële instelling zoveel mogelijk te bestrijden. Dit betreft tevens een wettelijke verplichting op basis van de Wet op het financieel toezicht (Wft) of de Wet ter voorkoming van witwassen en financieren terrorisme (Wwft). Een van de door financiële instellingen genomen maatregelen is het vastleggen van gedragingen van (rechts)personen die hebben geleid of kunnen leiden tot benadeling van financiële instellingen. Deze gegevens worden door de financiële instellingen vastgelegd in een Incidentenregister. Aan het Incidentenregister is een Extern Verwijzingsregister gekoppeld. Dit Extern Verwijzingsregister bevat uitsluitend Verwijzingsgegevens (bijvoorbeeld een naam en geboortedatum of KvK-nummer) die onder strikte voorwaarden mogen worden opgenomen. Iedere Deelnemer heeft afhankelijk van het lidmaatschap van de betreffende brancheverenigingtoegang tot een deel of meerdere delen van het Externe Verwijzingsregister. De banken die lid zijn van de Nederlandse Vereniging van Banken (NVB), evenals de financieringsinstellingen, die lid zijn van de Vereniging van Financieringsinstellingen in Nederland (VFN), hebben de mogelijkheid om via een Verwijzingsapplicatie te toetsen of een (rechts)persoon in het Extern Verwijzingsregister (EVR) van respectievelijk de financieringsmaatschappijen of de banken voorkomt. Ook leden van het Verbond van Verzekeraars hebben toegang.

Om er voor zorg te dragen dat de belangen van de betrokkenen op goede wijze worden beschermd, is opname in en raadpleging van het Incidentenregister en Extern Verwijzingsregister alleen toegestaan onder de voorwaarden van het Protocol met de daarbij horende Annex. Het CBP heeft vastgesteld dat de Verwerking van Persoonsgegevens zoals omschreven in het Protocol rechtmatig is. Het CBP heeft daartoe een voorafgaand en een nader onderzoek uitgevoerd. Het Protocol is geen Gedragscode zoals omschreven in artikel 25 WBP. Personen blijven acht jaar in de registratie.

Alle deelnemers aan het Waarschuwingssysteem beschikken over een Incidentenregister waarin onder strikte voorwaarden incidenten worden vastgelegd. Deze voorwaarden zijn vastgelegd in het Protocol. Als incidenten kunnen bijvoorbeeld voorkomen het falsificeren van nota"s, identiteitsfraude, skimming, verduistering in dienstbetrekking, phishing en opzettelijke misleiding. In het Incidentenregister worden karakteristieken van het incident vastgelegd en kenmerken van de daarbij betrokken personen, evenals handelingen die naar aanleiding van het incident hebben plaatsgevonden.

Als bij controles blijkt dat er een vermoeden is van ID-fraude (ID Theft of ID Take Over) dan kan de persoon waarvan de ID-gegevens worden misbruikt als alias gemeld worden via de Externe Verwijzingsapplicatie (EVA). Dit wordt alleen gedaan als de betrokken persoon de consequenties van de registratie accepteert. Bij registratie als alias wordt de persoon waarvan de ID-gegevens zijn misbruikt per brief geïnformeerd. Als de identiteit van de vermoedelijke fraudeur bekend is, zal tegen de vermoedelijke fraudeur aangifte worden gedaan en zal de vermoedelijke fraudeur EVA worden gemeld. Conform het PIFI zal ook de vermoedelijke frauderende partij worden geïnformeerd.

De gegevens in het Incidentenregister worden door de veiligheidsafdelingen of de fraudecoördinatoren van de financiële instellingen geraadpleegd als dat noodzakelijk is voor de uitvoering van hun werkzaamheden. Daarbij kan gedacht worden aan trendanalyses, het ontwikkelen van fraudepreventiestrategieën, pre-employmentscreening en integriteittoetsing, schadeverhaal en Customer Due Diligence.

Incidentenwaarschuwingssysteem door financiële instellingen	
Type maatregel:	Gegevensuitwisseling tussen bedrijven
Doel:	Detectie van fraude
Maatregel wordt genomen door:	Financiële instellingen
Kenmerkend:	Hoge effectiviteit
Uitvoerende organisatie:	NVB, Verbond van Verzekeraars, VFN, SFH, ZN, FOV
Bron:	o.a. www.verzekeraars.nl

Landelijk Schakelpunt Elektronisch Patiëntendossier (EPD)

Ieder ziekenhuis in Nederland houdt van haar patiënten een digitaal dossier bij. In een toenemend aantal ziekenhuizen is aan dit digitale dossier een digitale pasfoto toegevoegd waarmee de behandelend arts kan zien of degene die hij face to face voor zich heeft overeenkomt met het digitale dossier.

Enkele jaren geleden is een stelsel ontwikkeld waarmee ziekenhuizen en andere zorgverleners patiëntengegevens onderling kunnen uitwisselen: het Elektronisch Patiëntendossier. Hoewel het Elektronisch Patiëntendossier nooit in gebruik is genomen, bestaat de infrastructuur die uitwisseling van patiëntengegevens mogelijk zou kunnen maken nog wel. Dit is het landelijk schakelpunt.

De ontwikkeling van het Elektronisch Patiëntendossier (EPD) zou een veelbelovende aanvulling zijn geweest op de aanpak van ID-fraude. Zorginstellingen waaronder ziekenhuizen zouden beter in staat zijn onderling informatie uit te wisselen.

Landelijke Schakelpunt Elektronisch Patiëntendossier	
Type maatregel:	Gegevensuitwisseling/ - koppeling
Doel:	Gegevensuitwisseling tussen zorgaanbieders
Maatregel wordt genomen door:	Zorgaanbieders
Kenmerkend:	EPD afgeblazen, LSP bestaat nog
Uitvoerende organisatie:	Ministerie van VWS
Bron:	Ministerie van VWS

Verificatie Informatie Systeem (VIS)

De meeste Nederlandse financiële instellingen zijn aangesloten op het Verificatie Informatie Systeem (VIS), hiermee kunnen zij nagaan of een Nederlands document gestolen, vermist of om een andere reden ongeldig verklaard is. Hieronder vallen onder meer paspoorten, visa en de Nederlandse op naam gestelde rijbewijzen. VIS is een 100% dochteronderneming van BKR. VIS heeft als doel "het voorkomen van schade bij het bedrijfsleven en de overheid door frauduleus handelen met ongeldige reis- en identiteitsdocumenten".

Men tikt de documentsoort, het documentnummer en het land van herkomst in. Binnen enkele seconden is bekend of het document in VIS voorkomt. Herkent VIS het document niet? Dan staat het document niet als ongeldig te boek. Komt het wel in VIS voor? Dan staat het getoonde document wel als ongeldig te boek. Er is dan sprake van een hit. Zo kan men via VIS binnen enkele seconden via één distributiekanaal de geldigheid van een bepaald document verifiëren, ongeacht het soort of de herkomst van het document.

VIS is raadpleegbaar via documentscanners, via software die een koppeling maakt met eigen programmatuur van instellingen/bedrijven of via het beveiligde klantportal van BKR. De informatie uit VIS is afkomstig van drie bronleveranciers:

- De Rijksdienst voor het Wegverkeer (RDW),
- Het agentschap Basisadministratie Persoonsgegevens, Reisdocumenten (BPR) en
- Korps Landelijke Politiediensten (KLPD).

In 2011 heeft BKR met diverse externe partijen gesprekken gevoerd over productwensen met betrekking tot identificatie en fraudebestrijding. Om binnen de gemeentelijke markt identiteitsfraude beter tegen te kunnen gaan, is een samenwerkingsovereenkomst met Centric gesloten.

Volgens enkele respondenten heeft VIS een groot nadeel en dat is dat een bank of verzekeraar handmatig de documentgegevens moet insturen, waarna het verificatieresultaat volgt. Met een groot klantenbestand is dit een onhandig proces. Een ander nadeel van VIS is dat nogal wat gestolen ID-bewijzen niet meteen in het systeem worden geregistreerd. Veel mensen doen in geval van ID-bewijsdiefstal wel aangifte bij de politie, maar melden dit soms pas veel later bij hun gemeente met als gevolg dat de vermissing/diefstal niet in VIS is geregistreerd.

Verificatie Informatie Systeem (VIS)	
Type maatregel:	Database
Doel:	Controleren van ID-bewijzen op diefstal en vermissing
Maatregel wordt genomen door:	Ten behoeve van financiële instellingen
Kenmerkend:	Publiek-private samenwerking
Uitvoerende organisatie:	BKR
Bron:	www.bkr.nl

Fraude en Informatie Systeem Holland (FISH)

In opdracht van de stichting CIS (een stichting t.b.v. Nederlandse verzekeringsmaatschappijen) beheert het ICT-bedrijf ABZ een databank met (historische) gegevens over verzekerden van Nederlandse verzekeringsmaatschappijen. Deze databank wordt FISH (Fraude en Informatie Systeem Holland) genoemd. 'De verwerking van de informatie heeft tot doel het

leveren van een bijdrage aan de behartiging van de gemeenschappelijke belangen van de deelnemers inzake':

- het inschatten en beheersen van risico's in het algemeen;
- schadelastbeperking, in het bijzonder door een verantwoord acceptatiebeleid;
- het ontdekken, voorkomen en bestrijden van verzekeringsfraude;
- het uitwisselen van feitelijke gegevens tussen deelnemers onderling, tussen verzekeraars en politie/justitie en andere door de verantwoordelijken erkende instellingen.

Fraude en Informatie Systeem Holland (FISH)	
Type maatregel:	Database
Doel:	Detectie onrechtmatigheden onder verzekerden
Maatregel wordt genomen door:	Ten behoeve van verzekeraars
Kenmerkend:	Samenwerking tussen branchegenoten
Uitvoerende organisatie:	CIS & AMZ
Bron:	Stichting CIS

Preventel

De stichting Preventel is een samenwerkingsverband tussen aanbieders van telecommunicatiediensten. Preventel houdt een register bij van cliënten van telecombedrijven die rekeningen niet hebben betaald. Hoewel de dienst niet primair tot doel heeft ID-fraude tegen te gaan, komt via het systeem fraude wel geregeld aan het licht. Het gaat dan met name om mensen wiens naam en gegevens zijn misbruikt.

Preventel	
Type maatregel:	Datavergelijking
Doel:	Kennisuitwisseling
Maatregel wordt genomen door:	Telecombedrijven
Kenmerkend:	Geheel privaat initiatief
Uitvoerende organisatie:	Private partij
Bron:	www.preventel.nl

Intermediaire controles / point of sale-controles

Indien een financieel product in eerste instantie via een intermediair verloopt, vindt aldaar de fysieke toets van documenten en de persoon plaats. Bij particulieren vindt bij het eerste contact met de intermediair / financieel adviseur controle plaats aan de hand van originele identiteitsdocumenten en indien van toepassing een geldige verblijfsvergunning. In de back-office worden kopieën van de identiteitsdocumenten gecontroleerd. Daarbij wordt bij twijfel gebruik gemaakt van de ID DocumentScan van Keesing https://keesingreferencesystems.com/products/for_checking_id/id_documentscan. In incidentele gevallen kan contact op worden genomen met het systeem van het Expertisecentrum Identiteitsfraude en Documenten van de Koninklijke Marechaussee http://www.defensie.nl/marechaussee/service/expertisecentra/expertisecentrum_identiteitsfraude_en_documenten/documentcontrole_ten_behoeve_van_het_bedrijfsleven

Intermediaire controles	
Type maatregel:	Verificatie persoonsgegevens bij intake
Doel:	Verificatie van gegevens die door cliënten zijn verstrekt
Maatregel wordt	Financiële instellingen

genomen door:	
Kenmerkend:	Verificatie via aanvullende bronnen
Uitvoerende organisatie:	Financiële instellingen
Bron:	Interviews

2.4 Categorie 4: adequate behandeling

Fraudehelpdesk

De fraudehelpdesk is een meldpunt voor zowel burgers als bedrijven die slachtoffer zijn geworden van fraude (zoals ID-fraude). Het is een publiek-privaat initiatief. Doel van de fraudehelpdesk is om door te verwijzen en eventueel te ondersteunen bij het doen van aangifte van fraude. Daarnaast analyseert de helpdesk de binnengekomen meldingen om er trends uit af te leiden.

De helpdesk wordt vooral benaderd door bedrijven en burgers die zich onvoldoende gehoord voelen door de politie. Onder slachtoffers bestaat het idee dat de politie weinig doet met aangiften.

Fraudehelpdesk	
Type maatregel:	Organisatorisch
Doel:	Adviseren slachtoffers van fraude
Maatregel wordt genomen door:	Doelgroep zijn bedrijven en burgers
Kenmerkend:	Publiek privaat initiatief
Uitvoerende organisatie:	Fraudehelpdesk
Bron:	www.fraudehelpdesk.nl

Fraude-alarmering

De fraudehelpdesk voorziet tevens in een alarmeringssysteem. Met dit systeem worden bedrijven gewaarschuwd indien zich bepaalde typen van fraude of oplichting voordoen. Deze waarschuwing gebeurt in passieve vorm op de website en in actieve vorm via mailing van aangesloten bedrijven.

Of de maatregel effectief is, is niet bekend. De effectiviteit wordt wellicht groter wanneer de maatregel zich richt op een specifieke branche. Bedrijven voelen zich dan wellicht directer aangesproken. Een voorbeeld van een gerichte (effectieve) uitwisseling is het Incidentenwaarschuwingssysteem Financiële Instellingen.

Fraude-alarmering	
Type maatregel:	Organisatorisch
Doel:	Waarschuwen van potentiële slachtoffers van fraude
Maatregel wordt genomen door:	Doelgroep zijn bedrijven en burgers
Kenmerkend:	Publiek privaat initiatief
Uitvoerende organisatie:	Fraudehelpdesk
Bron:	www.fraudehelpdesk.nl

2.5 Categorie 5: opsporing

Particuliere recherche

Alle bedrijven en instellingen die in het kader van dit onderzoek zijn bezocht hebben medewerkers die een taak toebedeeld hebben gekregen ten behoeve van het voorkomen van ID-fraude. Enkele bedrijven hadden daarnaast een afdeling die meer deed dan alleen fraudedetectie en op basis van fraudesignalen recherchewerk uitvoeren. Hierbij kan gedacht worden aan het observeren van verdachten en het inwinnen van gegevens via of bij private partijen.

Bij één bedrijf gold een opschalingsbeleid. Fraude onder de € 10.000 wordt daar afgedaan door de afdeling crediteurenbeheer; boven de € 10.000 wordt de zaak overgedragen aan de afdeling security.

Particuliere recherche	
Type maatregel:	Opsporing
Doel:	Verzamelen bewijsmateriaal tegen verdachten
Maatregel wordt genomen door:	Enkele financiële instellingen
Kenmerkend:	Kostbaar
Uitvoerende organisatie:	Enkele financiële instellingen
Bron:	Interviews

Heterdaadmeldingen

Het beleid is aangifte te doen bij strafbare feiten en een bekende verdachte. De politie geeft echter niet altijd prioriteit en heeft niet altijd capaciteit. Als men ernstige verdenkingen en aanwijzingen heeft dat georganiseerd geprobeerd wordt op andermans naam financiële producten te verkrijgen dan creëert men soms "heterdaadsituaties". Stukken worden naar het aangegeven postadres gestuurd, waarna gepost wordt en zodra de post wordt opgehaald wordt deze persoon "in de kraag gevat" en aan de politie overgedragen. E.e.a. altijd in overleg met het wijkteam van het betrokken gebied. Pro-activiteit is het credo en de bedoeling is een signaal af te geven aan de fraudeur dat er wordt gemonitord en er actief wordt opgespoord. De bedoeling is dat hier ook een voorbeeldfunctie vanuit gaat die malafide aanvragers moet afschrikken.

Heterdaadmeldingen	
Type maatregel:	Opsporing
Doel:	Op heterdaad betrappen fraudeurs / voorbeeld stellen
Maatregel wordt genomen door:	Financiële instellingen
Kenmerkend:	In overleg met de politie
Uitvoerende organisatie:	Financiële instellingen
Bron:	Interviews

3 Suggesties voor beleid

In het voorgaande hoofdstuk zijn een groot aantal maatregelen weergegeven die het bedrijfsleven toepast om identiteitsfraude te voorkomen en te bestrijden. In dit hoofdstuk beschrijven wij de suggesties voor beleid die in de gesprekken zijn gedaan ten behoeve van wetgeving, beleid en handhaving.

Wie met beveiligings- en fraudedeskundigen van bedrijven en instellingen spreekt over ID-fraude en de maatregelen die zij zelf nemen, ontvangt al snel veel suggesties ten aanzien van wetgeving, beleid en handhaving. Uit de gesprekken komt ID-fraude in de eerste plaats naar voren als een maatschappelijk probleem dat vooral ook op bedrijfs- en branche-overschrijdend niveau moet worden aangepakt. Een voorbeeld was een gesprek met een stadsziekenhuis waar het probleem van ID-fraude direct voortkwam uit de aanwezigheid van mensen zonder verblijfs- en werkvergunning. Hun zorgbehoefte (en pogingen om toegang te krijgen tot zorg) kan niet worden weggenomen door ID-verificatie aan de balie van dat ene ziekenhuis te verbeteren. Hetzelfde geldt voor het probleem van skimming. Een individuele bank kan slechts symptomen bestrijden. De aanpak van de achterliggende – vaak internationaal opererende – bendes vereist meer dan een goed beveiligde bankpas of internetportal. Burgers moeten bewust worden gemaakt net als de beheerders van pinterminals (de winkeliers) en er moet vooral ook een opsporingsapparaat klaar staan op het moment dat een dader in beeld is. Dit betekent dat individuele bedrijven weliswaar maatregelen kunnen nemen, maar ook dat collectieve actie vereist is. In meerdere gesprekken komt het beeld naar voren van een bedrijfsketen waarin criminelen op zoek gaan naar de zwakste schakel. In dit licht is meerdere malen benadrukt dat overheden (zowel beleidsdirecties als de handhavende instellingen) ontwikkelingen goed moeten volgen, zich een beeld moeten volgen van de sterkte van de schakels en daarop moeten anticiperen onder ander ook door bedrijven collectief te stimuleren en helpen om hun verantwoordelijkheid te nemen.

Verhoog capaciteit, deskundigheid en prioriteit van handhaving

De aanpak van ID-fraude en andere vormen van fraude die in het digitale domein worden gepleegd, verdient meer aandacht. De ontwikkelingen binnen de politie en het openbaar ministerie met betrekking tot de aanpak van cybercrime worden als gunstig gezien maar lopen nog steeds achter op het probleem. Bedrijven constateren nog steeds onvoldoende capaciteit, expertise en prioriteit.

> "Het komt voor dat wij een compleet dossier bij de politie aanleveren, maar dat het toch niet wordt opgepakt. Het ligt niet zozeer aan de politie – wij hebben daar goede contacten – het is vooral het openbaar ministerie waar het aan capaciteit ontbreekt. Je ziet hier overigens verschillen tussen arrondissementen. In Groningen is de kans groter dat een zaak wordt opgepakt dan in de Randstad." (respondent financiële instelling)

> "Bedrijven die aangifte doen bij de politie hebben vaak het idee dat er niets met de melding wordt gedaan. Het is een administratieve handeling die gedaan wordt bijvoorbeeld omdat een bedrijfsproces dat voorschrijft. Men verwacht eigenlijk van zo'n aangifte bij voorbaat niet veel" (respondent brancheverenigingen)

Om ID-fraude aan te pakken zijn bedrijven en branches nu nog veelal op zichzelf aangewezen. Maar kunnen in de praktijk niet meer doen dan de symptomen bestrijden, achterliggende problemen liggen buiten hun bereik. Een voorbeeld dat in dit verband meerdere malen is aangehaald is de aanpak van skimming. Over het algemeen wordt hier de identiteit van nietsvermoedende rekeninghouders misbruikt. De betrokken rekeningen kunnen door een bank worden geblokkeerd, transacties kunnen soms worden teruggedraaid maar de opsporing van bendes ligt buiten het bereik van de mogelijkheden die banken hebben.

Voor zover ID-fraude zich manifesteert in het digitale domein (bijvoorbeeld in combinatie met hacking) zijn bedrijven in de praktijk vooral aangewezen op private ICT-beveiligingsbedrijven. Het is een veld waar het de overheid (o.a. politie) nog aan kennis en capaciteit ontbreekt. Deze achterstand moet snel worden ingelopen aangezien nogal wat conventionele criminaliteit zich snel aan het verplaatsen is naar het digitale domein.

> "Voor een gewapende overval op een bankfiliaal is de politie goed toegerust, ze zijn doorgaans snel ter plaatse en weten hoe een forensisch onderzoek moet worden uitgevoerd. Deze bankovervallen hebben echter hun langste tijd gehad, het verplaatst zich nu snel naar het digitale domein. De politie moet daarin meegaan." (respondent kennisinstelling)

Autoriteiten waar van oudsher van wordt verwacht dat zij meldingen van criminaliteit oppakken (politie, OM), blijken nu vaak niet in staat ID-fraude (en andere vormen van digitale criminaliteit) te registreren of te onderzoeken laat staan op te sporen. Deze omissie heeft inmiddels geleid tot twee meldpunten. Deze meldpunten zijn echter niet het fundamentele antwoord op de behoeften van burgers en bedrijven die zich er melden.

Ketenbeheersing en verantwoordelijkheidstoedeling

In het verlengde van bovenstaande wordt gepleit voor een ketenbenadering. Criminelen zoeken uiteindelijk altijd de plek waar de kans op succes het grootst is. Een versterking van de beveiliging op het ene punt zal vrijwel altijd leiden tot verschuiving van problemen naar andere (zwakkere) punten (het waterbedeffect). Aanpak van identiteitsfraude moet daarom altijd breed zijn opgezet. In de preventieve sfeer betekent dit dat de verschillende partijen zich bewust moeten zijn van risico's. Op dit moment worden de inspanningen nog te veel beperkt tot de plekken waar de schade wordt gevoeld. Dit geldt bijvoorbeeld voor zorgfraude. Hier landt de schade vrijwel altijd bij de zorgverzekeraars. Deze zijn dan ook het meest actief met de bestrijding van fraude. In dit domein zouden ook zorginstellingen en de burger tot een grotere alertheid moeten worden aangezet. Het geldt bijvoorbeeld ook voor skimmen (kopiëren van bankpassen). De inspanningen van banken laten onverlet dat ook rekeninghouders en beheerders van pinterminals (winkeliers) een cruciale rol hebben te spelen in de beheersing van de risico's. De overheid heeft een rol te spelen in het activeren van al deze partijen (dus ook de partijen waar de schade van ID-fraude uiteindelijk niet landt). Dit kan door voorlichting maar ook door het stellen van voorwaarden.

Als het gaat om ID-fraude is er altijd een rol en verantwoordelijkheid weggelegd voor de burger. Hij dient zich bewust te zijn van de waarde van zijn identiteit en de mogelijkheden die er zijn om die te misbruiken. Dat de burger op dit punt onwetend is blijkt uit bijna alle fraudecases die onze respondenten onder ogen hebben gehad. Te

denken valt aan kopieën van paspoorten die zonder verder door vragen worden afgegeven, of persoonsgebonden informatie die men zomaar geeft aan anonieme bellers, of mensen die als vriendendienst hun ID-bewijs uitlenen voor een doktersbezoek.

Ontwikkeling van het digitale paspoort (eID)

De ontwikkeling van een eHerkenningsstelsel voor zowel burgers als bedrijven wordt door alle respondenten als belangrijk gezien. Er bestaat grote behoefte aan een stelsel waarmee burgers en bedrijven zich op afstand via het internet kunnen identificeren. De ontwikkeling van het bestaande stelsel van eHerkenning (voor bedrijven) tot een eID-stelsel waar ook burgers gebruik van kunnen maken wordt door alle respondenten als veelbelovend gezien. Hoewel de overheid een initiërende rol heeft gespeeld bij de totstandkoming van het stelsel, wordt de uitvoering ervan grotendeels overgelaten aan private partijen. Naast de initiërende rol zijn er de volgende verwachtingen geuit met betrekking tot de rol van de overheid:

- Men verwacht een aanjagende en faciliterende rol van de overheid.
- De overheid dient zich dermate aan het stelsel te verbinden, dat het de burger vertrouwen geeft. Vertrouwen is immers een cruciale voorwaarde voor het stelsel. Een actieve rol van de overheid versterkt dit vertrouwen. Van ouds is de overheid verantwoordelijk voor het verstrekken van identiteitsdocumenten, zij dient die verantwoordelijkheid ook te nemen in de onlinewereld.
- De overheid dient de burger voor te lichten over het stelsel (of dient daar een belangrijke rol in te spelen). Omdat het gaat om abstracte diensten is communicatie belangrijk.
- De overheid dient randvoorwaarden te stellen. Enerzijds met betrekking tot de beveiliging en duurzaamheid van het stelsel. Het moet beveiligd zijn tegen bijvoorbeeld hacking en het moet overeind blijven staan als een van de private partijen mocht omvallen (zoals met Diginotar gebeurde). Anderzijds met betrekking tot het gebruik van persoonsgegevens door bedrijven die van het stelsel gebruik maken.

Wetgeving belemmerend

De Wet Bescherming Persoonsgegevens werkt belemmerend. Het herziene Pifi-protocol is strikter. Er moet een verplichte aangifte komen, maar de effectiviteit is vrijwel nihil. De prioriteit bij de politie is minimaal, omdat er onvoldoende middelen zijn en zaken worden daardoor geseponeerd. Daarnaast wordt de toegevoegde waarde van een aangifte als er geen schade is geleden door sommige politieregio's als nihil gezien. De maatregel om aangifte te doen op basis van CBP-eisen kost veel tijd en werk maar de politie kan te weinig doen. Dit moet effectief opgepakt worden.

Meldplichtige instellingen melden ongebruikelijke transacties bij de Financial Intelligence Unit – Nederland (FIU) op basis van de Wet ter voorkoming van witwassen en financieren van terrorisme (Wwft). Het FIU zoekt naar samenwerking, maar is niet verplicht feedback te geven over de aanpak van de meldingen. Bedrijven vinden dit minder transparant en stimulerend.

Extra regelgeving moet in de toekomst getoetst worden op pro-cycliciteit, doelmatigheid en (praktische) haalbaarheid. Veel goed bedoeld beleid heeft nu op korte termijn een averechts effect. Zo werkt het aanscherpen van de normen voor kredietverlening extra negatief uit voor consumptie tijdens een periode van een grote crisis. Daarnaast is er het effect van financiële uitsluiting: de maatregelen zijn bedoeld voor de consumenten met een hoog risico op betalingsachterstanden, maar zorgen er ook voor dat grote aantallen huishoudens lastiger krediet kunnen krijgen terwijl zij prima hun financiële huishouden op orde hebben. Extra beleid kan effect hebben op

bijvoorbeeld kosten (en prijs) van krediet en op de complexiteit voor het verkrijgen van krediet. Zie ook het onderzoek van de Universiteit van Tilburg in opdracht van de VFN:
http://www.vfn.nl/assets/uploads/files/Onderzoek%20naar%20Consumentenkrediet%20in%20Nederland.pdf

Op basis van Wft en Wwft zijn diploma's geëist. Het zogenaamde fingerspitzengefühl wat men nodig heeft om witwassen of fraude te herkennen leert men niet op een cursus. Daar is affiniteit met de business voor nodig en gevoel voor niet-reguliere afwijking in patronen.

Toegang tot GBA
Met name financiële instellingen hebben aangegeven dat toegang tot het GBA de verificatie aanzienlijk zou kunnen verbeteren. Bij nogal wat fraudegevallen wordt gebruik gemaakt van een geldig paspoort (dat gestolen is) waarbij adresgegevens worden opgegeven die anders zijn dan die van de houder van het paspoort. Op deze manier kan de post voor de formele rekeninghouder worden onderschept. Wanneer banken direct toegang zouden hebben tot het GBA zijn zij beter in staat om het adres van degene op wiens naam een rekening wordt geopend te verifiëren. Door andere branches wordt de noodzaak van toegang tot het GBA overigens gerelativeerd. Adresgegevens zijn lang niet in alle branches even relevant.

Het zou ook al veel schelen als via de interne banksystemen gebruik kan worden gemaakt van RDW-gegevens (Rijbewijsnummer) in combinatie met de geboortedatum. Dit is technisch nog niet mogelijk. Daarnaast zou het veel schelen als de RDW bij aanlevering aan het VIS-systeem een codering zou meegeven zodat voor de financiële instelling alleen de vermiste/gestolen documenten tot een hit leiden. De overige redenen waarom een rijbewijs ongeldig zijn verklaard zijn voor de financiële instellingen niet echt relevant.

Gebruik van BSN
Veel bedrijven beschikken over het BSN van hun cliënten. De meesten mogen dit nummer echter niet gebruiken in hun berichtenverkeer of gegevensuitwisseling met branchegenoten. Gebruik van BSN zou het berichtenverkeer kunnen vergemakkelijken omdat het persoonsverwisselingen voorkomt.
'Wij hebben laatst een brief gestuurd naar een patiënt in verband met een bevalling. Degene die de brief ontving bleek nog nooit een kind te hebben gehad. Zij bleek wel dezelfde naam en geboortedatum te hebben van degene waar de brief wel naar toe had gemoeten'

BSN zou kunnen helpen bij de controle of de klant ook daadwerkelijk de klant is. Gebruik van BSN als koppelingsgegeven is niet toegestaan. Het mag niet als zoeksleutel gebruikt worden. Wel kan de elfproef gedaan worden als eerste check. Bij gebruik van BSN zou het aantal ID takeovers verminderd kunnen worden. Het wordt inconsequent gevonden dat bedrijven het BSN wel mogen gebruiken om gegevens van personen te renseigneren naar de Belastingdienst, maar dat het niet mag worden benut om te helpen identiteitsfraude te voorkomen. Hierbij zij verder verwezen naar de voorhangprocedure bij het Ontwerpbesluit Wet Basisregistratie Personen, waarin deze problematiek is weergegeven in relatie tot financieringsmaatschappijen. Er zijn vragen van de brancheorganisatie VFN naar voren gekomen en beantwoord om extra mogelijkheden te realiseren via verificatie van het GBA voor niet matchende gegevens.

Mogelijke problemen door wetgeving rond naamgeving voorkomen/oplossen

Een groeiend probleem en een potentiële fraudeveroorzaker kan de eventuele nieuwe wet- en regelgeving rondom naamgeving van ouders en kinderen zijn. De werkgroep liberalisering naamrecht heeft daar rapport over uitgebracht[2]. De kans op "stroman"-rekeningen groeit zeker bij minderjarigen. Het is heel lastig te beoordelen straks wie nog bij welke vader en/of moeder hoort. Als wordt besloten tot registratie van dubbele achternamen dan zal in de GBA een wirwar aan namen ontstaan: dubbele achternamen van de pasgeborenen, ouders die eigen achternaam of de achternaam van de echtgenoot hebben, kinderen met de achternaam van dan wel de vader, dan wel van de moeder. Dit zou kunnen leiden tot grotere identiteitsfraude omdat de wirwar aan namen onduidelijkheid schept. De staatssecretaris van Veiligheid en Justitie heeft daarover overigens in 2012 opgemerkt dat niet is gebleken dat er sprake is van zodanige grote en urgente problemen op het gebied van het naamrecht dat thans een wetswijziging noodzakelijk is. Identiteitsfraude zou niet groter zijn, zolang de desbetreffende keten (bijvoorbeeld: geboorteakte-GBA-paspoort) goed georganiseerd blijft.

Biometrie

In meerdere sectoren zou het gebruik van biometrische gegevens de identiteitsverificatie kunnen versterken. Dit geldt bijvoorbeeld voor identificatie aan de balie van een ziekenhuis of bank en op termijn mogelijk ook voor identificatie op afstand (zoals online). Zo'n verificatie kan ID-fraude tegengaan maar bijvoorbeeld ook voorkomen dat na een jaar een klant ontkent ooit een contract te hebben afgesloten. Ondanks de hardheid die biometrie kan brengen in persoonsidentificatie zijn veel respondenten terughoudend in hun pleidooi voor deze aanvulling. Mogelijk schrikt het klanten af. Daarnaast zijn ervaringen met een proef bij een financiële instelling niet onverdeeld positief.

Voorkomen fraude via postbedrijven

Privatisering heeft er toe geleid dat postbedrijven goedkope arbeidskrachten zijn gaan inhuren, steeds vaker worden ZZP-ers ingezet. De druk op de marges van deze nieuwe postbezorgers kan fraude in de hand werken. Postbestellers kennen de waarde van financiële bescheiden als bankafschriften en salarisstroken. Door deze financiële bescheiden uit de poststroom weg te nemen of te kopiëren kunnen zij er misbruik van maken, bijvoorbeeld door met die bescheiden financiële producten aan te vragen. In de afgelopen tijd is al vaak vastgesteld dat de postbesteller ook degene is die de financiële bescheiden/producten heeft weggenomen. In nogal wat gevallen bestaat het idee dat de betreffende fraudeur bewust een baan als postbesteller heeft genomen om te frauderen. In het aannamebeleid van postbedrijven is er te weinig controle door postbedrijven op wie er solliciteert.

Overheidssteun voor slachtoffers identiteitsfraude

Meerdere instellingen hebben tenslotte aangegeven dat er meer gedaan moet worden ten behoeve van de slachtoffers van ID-fraude. Vaak wordt daarbij in het midden gelaten hoe verantwoordelijkheden tussen bedrijven en overheid precies verdeeld moeten worden. Het zou in veel gevallen voor slachtoffers erg lastig zijn om zich uit alle negatieve registraties te laten verwijderen. Als de onschuld van een slachtoffer overduidelijk is dan zou afmelding / uitschrijving uit de registratie eerder en makkelijker moeten kunnen.

[2] http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2012/12/18/rapport-werkgroep-liberalisering-naamrecht.html