

HORIZONTALE FRAUDE

Verslag van een onderzoek voor het
Nationaal dreigingsbeeld 2012



Horizontale fraude

Verslag van een onderzoek voor
het Nationaal dreigingsbeeld 2012

Brigitte Bloem
Albert Harteveld

Uitgave

Dienst IPOL
Postbus 3016
2700 KX Zoetermeer

De dienst IPOL
is een onderdeel van het Korps landelijke politiediensten

Eindredactie

Iet Voorhoeve

Zoetermeer, november 2012
Copyright © 2012 KLPD–IPOL Zoetermeer

Behoudens de door de wet gestelde uitzonderingen, alsmede behoudens voorzover in deze uitgave nadrukkelijk anders is aangegeven, mag niets uit deze uitgave worden verveelvoudigd en/of openbaar worden gemaakt, in enige vorm of op enige wijze, hetzij elektronisch, mechanisch, door fotokopieën, opnamen, of op enige andere manier, zonder voorafgaande schriftelijke toestemming van het KLPD.

Aan de totstandkoming van deze uitgave is de uiterste zorg besteed. Voor informatie die nochtans onvolledig of onjuist is opgenomen, aanvaarden de auteur(s), redactie en het KLPD geen aansprakelijkheid. Voor eventuele verbeteringen van de opgenomen gegevens houden zij zich gaarne aanbevolen.

Inhoud

	Samenvatting	7
1	Inleiding	10
	1.1 Het Nationaal dreigingsbeeld	10
	1.2 Definitie	11
	1.3 Onderzoeksvragen en leeswijzer	14
	1.4 Onderzoeksmethode	14
2	Versnippering in registratie en aanpak	17
	2.1 Steekproef uit de politiesystemen	17
	2.2 Nieuw onderzoek	21
	2.3 Buitenlandse rechtshulpverzoeken	22
	2.4 Bovenregionale Recherche	23
	2.5 De Financial Intelligence Unit (FIU)	23
	2.6 De Fraudehelpdesk	24
	2.7 De Fraudemeldpunten	25
	2.8 Meldpunt Internetoplichting	26
	2.9 Overige meldpunten	28
	2.10 Nationaal Platform Criminaliteitsbeheersing	28
	2.11 Landelijk skimmingpoint	28
	2.12 Expertiseknooppunt FinEC	29
3	Analyse aangiften	30
	3.1 Fraude met online handel	33
	3.2 Fraude met betaalmiddelen	35
	3.3 Voorschotfraude	37
	3.4 Laagfrequente vormen van fraude	39
	3.4.1 Acquisitiefraude	40
	3.4.2 Hypotheekfraude	41
	3.4.3 Telecomfraude	42
	3.4.4 Verzekeringsfraude	43
	3.4.5 Faillissementsfraude	44
	3.4.6 Beleggingsfraude	45
	3.4.7 Merkfraude	45
	3.5 Conclusie	46
	3.6 Discussie	46

4	Hoofdvormen van fraude	48
4.1	Fraude met online handel	48
4.1.1	Aard	48
4.1.2	Omvang	49
4.1.3	Criminele samenwerkingsverbanden	51
4.1.4	Maatschappelijke gevolgen	52
4.1.5	Criminaliteitsrelevante factoren	52
4.1.6	Verwachtingen	53
4.1.7	Aanpak	53
4.2	Fraude met betaalmiddelen	53
4.2.1	Aard	54
4.2.2	Omvang	57
4.2.3	Criminele samenwerkingsverbanden	59
4.2.4	Maatschappelijke gevolgen	60
4.2.5	Criminaliteitsrelevante factoren	60
4.2.6	Verwachtingen	62
4.2.7	Aanpak	63
4.3	Voorschotfraude	65
4.3.1	Aard	65
4.3.2	Omvang	67
4.3.3	Criminele samenwerkingsverbanden	71
4.3.4	Maatschappelijke gevolgen	75
4.3.5	Criminaliteitsrelevante factoren	76
4.3.6	Verwachtingen	77
4.3.7	Aanpak	78
4.4	Acquisitiefraude	78
4.4.1	Aard	78
4.4.2	Omvang	81
4.4.3	Criminele samenwerkingsverbanden	83
4.4.4	Maatschappelijke gevolgen	85
4.4.5	Criminaliteitsrelevante factoren	85
4.4.6	Verwachtingen	86
4.4.7	Aanpak	86
4.5	Hypotheekfraude	87
4.5.1	Aard	88
4.5.2	Omvang	90
4.5.3	Criminele samenwerkingsverbanden	91
4.5.4	Maatschappelijke gevolgen	91
4.5.5	Criminaliteitsrelevante factoren	92
4.5.6	Verwachtingen	92
4.5.7	Aanpak	93

4.6	Telecomfraude	94
	4.6.1 Aard	94
	4.6.2 Omvang	96
	4.6.3 Criminele samenwerkingsverbanden	98
	4.6.4 Maatschappelijke gevolgen	101
	4.6.5 Criminaliteitsrelevante factoren	102
	4.6.6 Verwachtingen	102
	4.6.7 Aanpak	103
4.7	Verzekeringsfraude	103
	4.7.1 Aard	103
	4.7.2 Omvang	104
	4.7.3 Criminele samenwerkingsverbanden	105
	4.7.4 Maatschappelijke gevolgen	106
	4.7.5 Criminaliteitsrelevante factoren	106
	4.7.6 Verwachtingen	107
	4.7.7 Aanpak	107
4.8	Faillissementsfraude	109
	4.8.1 Aard	110
	4.8.2 Omvang	112
	4.8.3 Criminele samenwerkingsverbanden	116
	4.8.4 Maatschappelijke gevolgen	117
	4.8.5 Criminaliteitsrelevante factoren	118
	4.8.6 Verwachtingen	119
	4.8.7 Aanpak	119
4.9	Beleggingsfraude	122
	4.9.1 Aard	122
	4.9.2 Omvang	126
	4.9.3 Criminele samenwerkingsverbanden	128
	4.9.4 Maatschappelijke gevolgen	130
	4.9.5 Criminaliteitsrelevante factoren	131
	4.9.6 Verwachtingen	132
	4.9.7 Aanpak	133
4.10	Merkfraude	135
	4.10.1 Aard	135
	4.10.2 Omvang	137
	4.10.3 Criminele samenwerkingsverbanden	140
	4.10.4 Maatschappelijke gevolgen	141
	4.10.5 Criminaliteitsrelevante factoren	142
	4.10.6 Verwachtingen	143
	4.10.7 Aanpak	144

5	Horizontale fraude als fenomeen	147
5.1	Aard	147
5.2	Omvang	151
5.3	Maatschappelijke gevolgen	153
5.4	Criminaliteitsrelevante factoren	154
5.5	Aanpak	154
6	Aanpak van fraude	155
6.1	Fraudebeheersstrategie	155
6.2	Achtergrond FBS	156
6.3	Werkwijze FBS	156
6.4	Voordelen FBS	157
	Literatuur	159
	Bijlage I Klankbordgroep en experts	167
	Bijlage II Lijst met afkortingen	169
	Bijlage III Overzicht hoofdvormen van horizontale fraude en hun zoekvragen in BRAINS	170
	Bijlage IV Brief Minister van Veiligheid en Justitie inzake faillissementsfraude	173

Samenvatting

In dit rapport richten we ons op verschillende vormen van horizontale fraude. Horizontale fraude gaat over fraude die gericht is tegen burgers, bedrijven en financiële instellingen. In totaal zijn tien hoofdvormen onderzocht aan de hand van de onderzoeksvragen zoals die voor alle deelprojecten voor het Nationaal dreigingsbeeld zijn geformuleerd. In hoofdstuk 2 belichten wij de gebrekkige en versnipperde informatieorganisatie: een aantal organisaties en meldpunten houdt zich bezig met het registreren van informatie, maar zij hebben alle een eigen manier van werken. De politie kent twee vormen van registratie, namelijk de buitenlandse rechtshulpverzoeken over fraude die binnenkomen bij het Landelijk Internationaal Rechtshulpcentrum (LIRC) en de binnenlandse aangiften die worden geregistreerd in de politiesystemen. Zowel in hoofdstuk 2 als in hoofdstuk 3 laten wij een analyse zien van de 30.000 aangiften die jaarlijks onder oplichting worden geregistreerd in de politiesystemen. Het doel van de analyses was om te onderzoeken welke soorten fraude zijn geregistreerd en om de bijbehorende modi operandi inzichtelijk te maken. In beide analyses blijkt fraude met online handel de meest voorkomende fraudevorm te zijn. Ook fraude met credit cards (skimmen, internetbankieren) en voorschotfraude (dating- en loterijfraude) komen veel voor.

In hoofdstuk 4 worden aan de hand van de onderzoeksvragen de tien verschillende hoofdvormen van fraude beschreven: fraude met online handel, fraude met betaalmiddelen, voorschotfraude, acquisitiefraude, hypotheekfraude, telecomfraude, verzekeringsfraude, faillissementsfraude, beleggingsfraude en merkfraude. De totale omvang is groot, zo blijkt uit onze resultaten. De schade wordt geschat op drie miljard euro per jaar. Vooral voorschotfraude, acquisitiefraude, verzekeringsfraude, faillissementsfraude en beleggingsfraude dragen daar fors aan bij. Dit zal de komende jaren naar verwachting niet minder worden. Vooral de voortgaande ontwikkelingen op het gebied van internet, waardoor fraudeurs onzichtbaar kunnen blijven en op grote schaal toe kunnen slaan, dragen hieraan bij.

In hoofdstuk 5 worden de gemeenschappelijke kenmerken van de diverse vormen van fraude beschreven, ook aan de hand van de onderzoeksvragen. Bij het wegen van het fenomeen horizontale fraude pleiten wij ervoor om de hoofdvormen niet alleen afzonderlijk te wegen, maar ook gezamenlijk in samenhang te beschouwen. Zes van de tien hoofdvormen zijn vormen van massmarketingfraude, dat vooral individuen en kleine bedrijven treft. Het gaat

hier om een modus operandi waarbij potentiële slachtoffers grootschalig worden benaderd, bijvoorbeeld via e-mail, online handelssites, post of telefoon. Globaal gaat het om twee verschillende tactieken. Bij de eerste worden zo veel mogelijk slachtoffers gemaakt voor relatief kleine bedragen (bijvoorbeeld bij fraude met online handel of acquisitiefraude). Bij de tweede tactiek richt men zich op specifieke slachtoffers met wie een relatie wordt opgebouwd, waarbij soms grote bedragen afhandig worden gemaakt en veel emotionele schade wordt aangericht (bijvoorbeeld bij datingfraude en beleggingsfraude). De fraudeurs richten zich hierbij op kwetsbare groepen, zoals ouderen, of ze geven lijsten van eerdere slachtoffers aan elkaar door (*suckerlists*). Ze blijken hierbij gebruik te maken van een ingewikkelde combinatie van beïnvloedings-technieken die te vergelijken zijn met de marketingmethoden die een verkoper hanteert om zijn producten aan de man te brengen. Kennis van dergelijke technieken is om twee redenen belangrijk: het maakt duidelijk dat het niet terecht is om slachtoffers weg te zetten als hebzuchtig, dom of naïef, ze handelen namelijk vaak in goed vertrouwen. Ook kan de kennis van de beïnvloedingstechnieken worden gebruikt om mensen voor te lichten zodat ze deze beter herkennen.

Naast individuen en kleine bedrijven die de dupe worden, ondervinden de private partijen en grote bedrijven, zoals banken, de telecomsector, creditcardmaatschappijen en verzekeraars veel last van fraude. Zij zijn in een voortdurende wedloop met de fraudeurs om hun systemen, gegevens en eigendommen te beveiligen, en hun klanten tegen aanvallen van fraudeurs te beschermen. Niet alleen lijden deze partijen soms grote verliezen en reputatieschade als gevolg van de fraude, het gaat ook gepaard met grote (financiële) inspanningen om de fraudeurs voor te blijven. Desondanks blijken de aanvallen van fraudeurs steeds weer succesvol te zijn. Ze kunnen eindeloos hun gang gaan door het uitblijven van een gerichte aanpak. De impact van deze delicten wordt verergerd doordat in toenemende mate katvangers worden gerekruteerd om bank- of pinpasgegevens tegen een gering bedrag ter beschikking te stellen. Deze katvangers, voornamelijk jonge scholieren, ondervinden nadien nog lang de financiële gevolgen van hun daden.

Bij nagenoeg alle vormen van fraude is ook sprake van identiteitsfraude die wordt gebruikt om de fraude uit te kunnen voeren. Wij zagen identiteitsfraude terug bij acht van de tien hoofdvormen van fraude; bij de overige twee vormen was het niet bekend. Fraudeurs maken misbruik van valse of vervalste persoonsgegevens bij het uitvoeren van de delicten. Daarnaast worden rechtspersonen misbruikt, die ook op naam van katvangers worden gezet: allerlei goederen worden besteld en niet betaald, waarna men de rechtspersoon laat 'ploffen'.

Doordat de beschikbare informatie gebrekkig en versnipperd is vastgelegd, zijn delen van de onderzoeksvragen onderbelicht gebleven. Vooral gedetailleerde informatie over criminele samenwerkingsverbanden ontbreekt. Op grond van de onderzoeksresultaten pleiten we dan ook voor verbetering van de informatieorganisatie rond horizontale fraude, met nadruk op een centraal punt en/of loket waar gedupeerden hun meldingen en aangiften laagdrempelig kunnen doen. Door een centrale analyse, veredeling en clustering van informatie kan een goed inzicht in de aard, omvang en trends worden verkregen, op basis waarvan een gerichte aanpak kan worden bepaald. Die aanpak hoeft niet noodzakelijkerwijs repressief te zijn, maar kan ook preventief zijn en gericht op barrières. Een voorstel voor een aanpak staat in hoofdstuk 6 omschreven.

Fraude van deze omvang en het gegeven dat het al jaren doorwoekert zonder effectieve aanpak, ondermijnt het vertrouwen in een rechtvaardige samenleving. Het leidt niet alleen tot wantrouwen in het functioneren van het financieel-economische stelsel, doordat illegale gelden in omloop komen die worden witgewassen of gebruikt voor andere criminaliteitsvormen (hennepsteelt, mensenhandel), maar het schendt ook het vertrouwen in elkaar, in medemensen. Daarnaast ondermijnt het de positie van organisaties, waaronder de opsporing, die in het leven zijn geroepen om de samenleving tegen criminaliteit in het algemeen, en fraude in het bijzonder, te beschermen. Tot slot leidt het achterblijven van een adequate (strafrechtelijke) aanpak tot normvervaging bij burgers, tot vermindering van het zelfreinigend vermogen van (financiële) ondernemingen, tot ontduiking van regels en (betalings)verplichtingen en tot een lage publieke moraal in het algemeen.

De politie staat ten tijde van het schrijven van dit rapport aan de vooravond van een ingrijpende reorganisatie. Fraude krijgt op diverse plekken een plaats binnen de nieuwe organisatie, zoals bij de Landelijke Recherche en de nieuwe regionale informatie- en opsporingsknooppunten. Fraude is tot speerpunt benoemd binnen de *Nationale Intelligence Agenda* (NIA), samen met witwassen en ontnemen. Met een brede aanpak, gericht op verbetering van het informatieproces en samenwerking tussen private en publieke partijen onder auspiciën van, bijvoorbeeld, een coördinerende fraudeautoriteit valt veel te winnen. Recentelijk werd in een onderzoek becijferd dat Nederland hierdoor vier miljard euro kan besparen, en wellicht nog meer aangezien in dat onderzoek bij lange na niet alle fraudevormen zijn meegenomen (Van Geldrop & De Vries, 2012).

1

Inleiding

1.1 Het Nationaal dreigingsbeeld

Elke vier jaar wordt door de Dienst IPOL van het Korps landelijke politiediensten (KLPD) in samenwerking met de Dienst Nationale Recherche van hetzelfde korps, het Nationaal dreigingsbeeld (NDB) georganiseerde criminaliteit vervaardigd. Het eerste verscheen in 2004. In opdracht van het College van procureurs-generaal wordt telkens een zo breed mogelijk overzicht gepresenteerd van de stand van zaken rond de georganiseerde criminaliteit in Nederland. Centraal staan daarbij de criminele hoofdactiviteiten. Dat wil zeggen dat vooral de daarop betrekking hebbende strafrechtelijke delictcategorieën onderwerp van onderzoek zijn. Het gaat dan niet alleen om de meer traditionele vormen van georganiseerde criminaliteit zoals drugshandel, witwassen, mensenhandel en –smokkel, maar ook om minder bekende vormen zoals wapenhandel, skimmen, kinderporno-graphie, vals geld en allerlei vormen van cybercrime en vermogenscriminaliteit.

Deze vormen van georganiseerde criminaliteit worden –aan de hand van uniforme onderzoeksvragen- in afzonderlijke projecten onderzocht. In het eindrapport NDB worden de resultaten van deze projecten samengevat en voorzien van wat wij ‘een kwalificatie van dreiging’ noemen. Hiermee wordt aangegeven of de betrokken vorm van georganiseerde criminaliteit voor de komende vier jaar als een bedreiging voor de Nederlandse samenleving moet worden gezien. Mede op grond van deze kwalificaties worden de landelijke beleidsprioriteiten voor de middellange termijn vastgesteld.

Dit rapport over georganiseerde horizontale fraude is een van de deelrapporten die de bouwstenen voor het Nationaal dreigingsbeeld (NDB2012) vormen. Behalve als bouwsteen, hebben deze rapportages natuurlijk ook zelfstandige betekenis. Ze worden daarom ook separaat gepubliceerd.

Voordat we de onderzoeksvragen beantwoorden, gaan we in op de afbakening van het onderwerp en op de doelstelling van het onderzoek, zetten we de onderzoeksvragen uiteen en schenken we aandacht aan de onderzoeksmethode.

1.2 Definitie

Van fraude bestaat geen eenduidige of duidelijke definitie; er moet sprake zijn van:

- een benadeelde;
- opzettelijk handelen;
- onrechtmatig of onwettelijk handelen;
- een misleidende voorstelling van zaken;
- het oogmerk om economisch voordeel te halen.

Fraude en financieel-economische criminaliteit zijn niet als zodanig omschreven in de wet. Juridisch gezien wordt fraude meestal omschreven als een combinatie van handelingen, zoals valsheid in geschrifte, bedrog, oplichting en diefstal. In het Wetboek van Strafrecht is oplichting onder artikel 326¹ opgenomen. Oplichting is de meest gebruikte optie voor registratie van fraudezaken in de politiesystemen, maar dekt een bredere lading dan fraude, hoewel de scheidslijn dun is. Een inventarisatie op internet leert dat de meeste voorbeelden die worden gegeven, van toepassing zijn op de vormen van fraude zoals die in dit deel rapport worden besproken. We vonden de volgende voorbeelden: *advance fee fraud* (voorschotfraude), malafide telefoonlijnen (telecomfraude), een kat in de zak (fraude met online handel) of spookfacturen (acquisitiefraude). Deze vormen van fraude kunnen ook samengevat worden onder de noemer fraude op internet of *massmarketingfraude*, omdat voor alle vormen internet wordt gebruikt om de fraude te plegen.

In dit deelrapport hanteren we de volgende definitie voor fraude:

Een opzettelijke handeling waarbij een fraudeur gebruik maakt van valse voorwendzelen met het oogmerk om zich op basis van deze bedrieglijke gegevens ten koste van anderen te bevoordelen dan wel te verrijken.

¹ Hij die, met het oogmerk om zich of een ander wederrechtelijk te bevoordelen, hetzij door het aannemen van een valse naam of van een valse hoedanigheid, hetzij door listige kunstgrepen, hetzij door een samenweefsel van verdichtsels, iemand beweegt tot de afgifte van enig goed, tot het ter beschikking stellen van gegevens met geldswaarde in het handelsverkeer, tot het aangaan van een schuld of tot het teniet doen van een inschuld, wordt, als schuldig aan oplichting, gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie.

Deze definitie is van toepassing op alle vormen van fraude die in dit rapport beschreven worden: op sommige in zijn geheel, zoals acquisitiefraude of fraude met online handel, op andere voor een deel, zoals merkfraude. Kopers van bijvoorbeeld nagemaakte merkkleding kopen dit doelbewust omdat deze artikelen goedkoper zijn, en zowel koper als aanbieder behalen voordeel (ten koste van de eigenaar van het merk die inkomsten misloopt).

Over het algemeen wordt een indeling in fraude naar horizontale, verticale en diagonale fraude gehanteerd. We spreken van horizontale fraude als particulieren, bedrijven, financiële instellingen of organisaties slachtoffer zijn. Horizontale fraude valt in de politiestructuren voornamelijk onder oplichting, art. 326 Wetboek van Strafrecht.

Bij verticale fraude is de overheid slachtoffer. Het gaat over het verkeer tussen overheid en burger, waarbij de burger iets onrechtmatig ontvangt van de overheid (uitkering, subsidie, identiteitsbewijs) of waarbij de burger iets af moet staan aan de overheid en daarbij met opzet bedrog pleegt (te weinig belasting of te lage premies).

Daar waar mengvormen optreden, wordt gesproken van diagonale fraude. Wij noemen als voorbeeld faillissementsfraude en identiteitsfraude, waarin zowel burgers, bedrijven als de overheid benadeeld kunnen worden.

In dit deelrapport richten we ons op horizontale fraude. Het Functioneel Parket (FP) prioriteert voornamelijk op verticale fraude, en heeft eind 2010 een dreigingsanalyse over financieel-economische criminaliteit opgeleverd. Doel van dit rapport was te onderzoeken welke fraudevormen een dreiging zijn voor de komende jaren (grootte, ernst, maatschappelijke gevolgen). Dit is gedaan op basis van literatuurstudie, expertmeetings en zaaksanalyse.

In de zaaksanalyse van het FP zijn voornamelijk zwaardere verticale en diagonale fraudezaken onderzocht. Dit betroffen zaken die naar het Openbaar Ministerie (OM) waren gegaan en afkomstig waren van Bijzondere Opsporingsdiensten (BOD's), de Bovenregionale Recherche (BR) en toezichhouders. Op basis van dit rapport zijn door het FP de volgende dreigingen benoemd: carrouselfraude, subsidiefraude, malafide dienstverleners, witwassen, integriteitsschendingen in de semi-publieke sector en *massmarketingfraude* tegen burgers.

De resultaten van de dreigingsanalyse van het FP zijn grotendeels richtinggevend voor het verticale en diagonale fraudedomein, en geeft voor wat betreft *massmarketingfraude* richting aan het horizontale fraudedomein.

Hoewel de Fiscale Inlichtingen- en Opsporingsdienst –Economische Controle-dienst (FIOD-ECD) en andere BOD's zich bezighouden met beleggings-, faillissements- en intellectueleigendomsfraude, ontbreekt overzicht in de aard en omvang van horizontale fraude, en daarom ontbreekt ook een goed sturingsinstrument. In dit deelproject is ervoor gekozen het domein af te bakenen tot horizontale fraude, dat wordt onderverdeeld in:

- fraude met online handel;
- fraude met betaalmiddelen;
- voorschotfraude;
- acquisitiefraude;
- hypotheekfraude;
- telecomfraude;
- verzekeringsfraude;
- faillissementsfraude;
- beleggingsfraude;
- merkfraude.

Voor opname in het Nationaal dreigingsbeeld is georganiseerdheid² een noodzakelijk criterium. Van georganiseerdheid is sprake wanneer personen 'structureel' samenwerken met het oog op het gezamenlijk halen van financieel of materieel gewin³. De eerste onderzoeksactiviteiten van dit deelproject waren gericht op het verkrijgen van inzicht in de mate van georganiseerdheid van de diverse vormen van horizontale fraude. De opzet was dat wanneer deze niet georganiseerd waren, ze niet voor verdere verdieping in aanmerking zouden komen. Een rondgang langs de diverse fraude-experts en een inventarisatie van de beschikbare literatuur leerde dat alle hoofdvormen van fraude in meer of mindere mate georganiseerd worden gepleegd. Daarom is voor dit deelproject gekozen om alle hoofdvormen van fraude in kaart te brengen. Omdat dit nog niet eerder op deze manier is gedaan, kan het deelrapport daarom als nulmeting worden beschouwd.

² In het NDB van 2008 wordt het domein van de georganiseerde criminaliteit aangeduid als: 'criminaliteitsverschijnselen die tot stand komen in (1) de structurele samenwerking tussen personen, die worden gepleegd met het oog op (2) het gezamenlijk behalen van financieel of materieel gewin.' Het kenmerk 'structurele samenwerking tussen personen' betekent niet alleen dat sprake is van (de intentie tot) herhaald plegen van een delict of misdrijf, maar ook van enige consistentie in de samenstelling van het samenwerkingsverband.'

³ Om een indicatie te krijgen van de georganiseerdheid van fraudegroepen is experts gevraagd of de groepen die actief zijn een vaste samenstelling hebben, de (fraude)delicten herhaaldelijk plegen of veel financiële schade veroorzaken bij hun slachtoffers.

1.3 Onderzoeksvragen en leeswijzer

De vragen voor het onderzoek naar horizontale fraude zijn afgeleid van de algemene vragen uit het NDB en luiden als volgt:

1. Hoe heeft de aard van georganiseerde horizontale fraude zich ontwikkeld voor wat betreft de wijze waarop deze wordt gepleegd?
2. Hoe heeft de omvang van de georganiseerde horizontale fraude zich ontwikkeld?
3. Hoe heeft de aard van georganiseerde horizontale fraude zich ontwikkeld voor wat betreft de kenmerken van personen respectievelijk criminele samenwerkingsverbanden die van (betrokkenheid bij) het plegen daarvan worden verdacht?
4. Wat zijn de gevolgen van georganiseerde horizontale fraude voor de Nederlandse samenleving?
5. Welke criminaliteitsrelevante factoren zijn, in welke mate en op wat voor wijze, van invloed op georganiseerde horizontale fraude?
6. Wat zijn de verwachtingen over omvang, werkwijze, betrokkenen en maatschappelijke gevolgen van georganiseerde horizontale fraude in de komende jaren?
7. Welke aanknopingspunten voor beleid dat is gericht op het tegenhouden of terugdringen van georganiseerde horizontale fraude komen uit het onderzoek naar voren?
8. In hoeverre en op welke manier zijn Nederlanders in het buitenland actief bij het uitvoeren of faciliteren van georganiseerde horizontale fraude? En wat zijn de gevolgen?

Alle onderzoeksvragen, behalve vraag 8, worden beantwoord in hoofdstuk 4, waarin de tien onderzochte hoofdvormen van fraude aan bod komen. Over vraag 8 is geen informatie uit ons onderzoek naar voren gekomen. In hoofdstuk 5 worden de gemeenschappelijke kenmerken van de verschillende hoofdvormen van fraude beschreven. Hoofdstuk 6 bevat een voorstel voor een aanpak van horizontale fraude.

1.4 Onderzoeksmethode

Om inzicht te krijgen in horizontale fraude is gebruikgemaakt van literatuur, databestanden, interviews en zijn via internet open bronnen geraadpleegd. Gelet op de beperkte beschikbare tijd en de geringe onderzoekscapaciteit is er geen uitgebreid dossieronderzoek gedaan.

Literatuur

Verschillende organisaties, instanties en overheden besteden aandacht aan horizontale fraude. Met enige regelmaat verschijnen rapporten, beleidsnotities, (wetenschappelijke) onderzoeken en Kamerstukken over de verschillende fraudeterreinen. De frequentie van verschijnen verschilt per fraudevorm. Met deze publicaties wordt getracht inzicht te geven in (de omvang van) het fenomeen horizontale fraude en de personen die zich daarmee bezighouden. Er zijn echter nauwelijks studies gedaan die specifiek gericht zijn op (georganiseerde) dadergroepen die bovenregionaal en internationaal actief zijn. Daarom hebben we ons voor een groot deel gebaseerd op literatuur over horizontale fraude in het algemeen afkomstig van politie, overheidsinstanties, brancheorganisaties, universiteiten en onderzoeksbureaus.

Databestanden

Om informatie over de (ontwikkeling van de) omvang van de horizontale fraude te kunnen geven, zijn databestanden en registraties van politie en andere instanties gebruikt. Hierbij is getracht om zo veel mogelijk informatie in handen te krijgen over de periode 2008 tot en met 2010. Alleen wanneer dit niet mogelijk bleek, is teruggevallen op minder recente data.

De volgende registers en databestanden zijn geraadpleegd:

- Cijfers van de Fraudehelpdesk en het Meldpunt Internetoplichting (MIO) zijn gebruikt om inzicht te krijgen in onder andere fraude met online handel, voorschotfraude en acquisitiefraude.
- Uit het politiesysteem Blueview zijn aangiften gehaald die geregistreerd staan als oplichting. Om inzicht te krijgen in de (ontwikkeling van de) omvang van de verschillende hoofdvormen van horizontale fraude is een steekproef genomen van tien procent uit de aangiften over de jaren 2008, 2009 en 2010. Bovendien is op alle aangiften van een kalenderjaar een verdiepende analyse uitgevoerd.
- De csv-manager waarin de regiokorpsen criminele samenwerkingsverbanden (csv's) invoeren. Gekeken is naar de criminele samenwerkingsverbanden die zich onder meer bezighouden met hoofdvormen van horizontale fraude.
- Lopende en afgesloten bovenregionale rechercheonderzoeken.

Interviews

Zowel binnen als buiten de politie zijn deskundigen benaderd die vanuit hun eigen invalshoek expertise hebben opgebouwd op het gebied van fraude. Zij zijn geïnterviewd met als doel lacunes in de informatie op te vullen, opkomende trends te signaleren en bevindingen te toetsen. In deze gesprekken stonden de onderzoeksvragen centraal. In bijlage I staat een overzicht van de geïnterviewden.

Internet

Op internet is gezocht naar openbare publicaties, persberichten en krantenartikelen en op het interne netwerk van het KLPD en de Politieacademie is gezocht naar aanvullende politie-informatie.

2

Versnippering in registratie en aanpak

In 2004 heeft de Algemene Rekenkamer een rapport over fraudebestrijding uitgebracht. Hierin staat dat het ontbreken van inzicht in de aard en omvang van horizontale fraude en in de opsporingsprestaties een goede bepaling van de capaciteitsinzet en de aansturing van de opsporing in de weg staat. In 2008 werden voorschot- en beleggingsfraude in het Nationaal dreigingsbeeld (KLPD, Dienst IPOL, 2008b) gekwalificeerd als dreiging. De omvang zou het topje van de ijsberg zijn en de psychische schade voor slachtoffers enorm. De dreiging uit het NDB 2008 is de afgelopen vier jaar niet omgezet in beleid zoals valt op te maken uit een rapport van het Openbaar Ministerie en de politie (2011).

Het onderzoeksbureau Intraval concludeerde in 2010 dat er sinds het verschijnen van het rapport van de Algemene Rekenkamer in 2004 weinig is veranderd; er bestaat nog steeds geen inzicht in de omvang van horizontale fraude (Tromp, Snippe, Bieleman & De Bie, 2010). De onderzoekers noemen als uitzondering acquisitie-, telecom- en verzekeringsfraude waarvan grove schattingen van de omvang zijn gedaan. Deze schattingen zijn onder andere gebaseerd op rapporten van het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) en een schatting van het Steunpunt Acquisitiefraude (SAF).

In de volgende paragrafen worden verschillende bronnen beschreven die ieder op hun eigen wijze tot cijfers over fraude komen. Dit om te laten zien dat de registratie en aanpak van fraude in hoge mate versnipperd is, en om aan te tonen dat iedere bron zijn eigen definities van fraude hanteert. Het is evident dat dit het doen van uitspraken over aard en omvang bemoeilijkt. Er ontstaat een vicieuze cirkel, waarbij aard en omvang nauwelijks zijn vast te stellen, met als gevolg dat niet geprioriteerd kan worden.

2.1 Steekproef uit de politiesystemen

In 2009 constateerde het Bovenregionaal Recherche Overleg (BRO) dat fraude qua volume de derde plaats in de categorie bovenregionale middencriminaliteit innam. Omdat betrouwbare en eenduidige cijfers over fraude ontbraken, gaf het BRO opdracht aan de Dienst IPOL om de haalbaarheid van een *fraude-monitor* te onderzoeken. Doel was om aard en omvang van fraude in Nederland inzichtelijk te maken voor een betere sturing en prioritering. Deze opdracht leidde tot twee vragen: ten eerste welke fraudevormen worden geregistreerd in

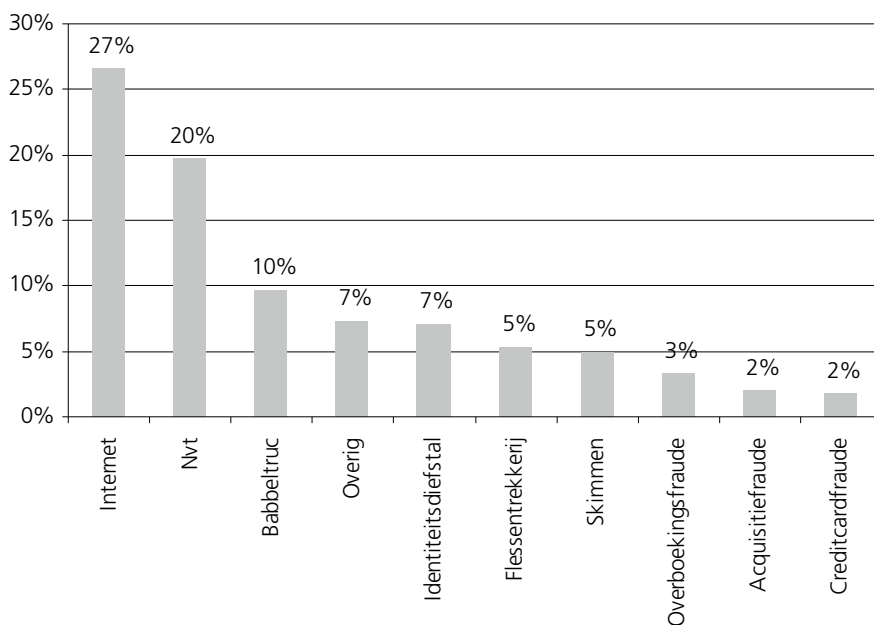
de politiesystemen en ten tweede hoe is de bestrijding van fraude georganiseerd in Nederland? Ook werd verwacht dat de ontwikkelingen in kaart gebracht zouden worden.

Om de eerste vraag te beantwoorden, is gebruikgemaakt van aangiften uit de politiesystemen. Aangiften over fraude worden onder verschillende codes geregistreerd, zoals oplichting, vervalsing, vals geld uitgeven en subsidiefraude (in totaal 22 omschrijvingen). Het aantal aangiften over fraude schommelt rond de 30.000 per jaar, en het merendeel wordt als oplichting geregistreerd. Uit de aangiften van 2008 werd een aselechte steekproef getrokken. De aangiften waren afkomstig van de 25 politieregio's, het KLPD en de Koninklijke Marechaussee (KMar). Van elk van deze onderdelen werd vier procent van de aangiften geselecteerd. Dit leverde in totaal 1.238 aangiften voor analyse op.

Om de aangiften te analyseren is gebruikgemaakt van een analysekader dat door het Functioneel Parket (FP) is opgesteld. Dit is omgezet in een voor het doel van het onderzoek bruikbaar analyse-instrument, dat voldoet aan de criteria dat categorieën zo veel mogelijk wederzijds uitsluitend moeten zijn, en niet te breed of te smal gedefinieerd. Een en ander is tijdens de analyse van de aangiften verder bijgesteld, omdat er meer categorieën en constructies bleken te bestaan dan in het analysekader waren opgenomen. De volgende stap was het lezen en categoriseren van de aangiften (35 tot 50 aangiften per dag). Dit is een zeer arbeidsintensieve methode, waarbij het categoriseren van een aangifte vaak ruimte geeft voor subjectiviteit. Binnen de ICT-omgeving van de politie was destijds geen analysetoepassing voorhanden waarmee dit op een efficiëntere manier uitgevoerd had kunnen worden. Als gevolg daarvan zijn binnen de beschikbare tijd in totaal 837 aangiften geanalyseerd die verdeeld waren over zeventien regio's, het KLPD en de KMar (deze waren willekeurig gekozen uit de gehele steekproef).

Figuur 1

Meest voorkomende vormen van fraude in 2008 (17 van de 25 regio's, het KLPD en de KMar; N= 837)



De resultaten zijn weergegeven in figuur 1. Hierbij maken wij een aantal kanttekeningen. Ten eerste zijn de in het figuur genoemde fraudevormen in overleg met de makers van de csv-manager herbenoemd om te komen tot eenduidige definities. Dat is noodzakelijk omdat alleen uitspraken over de aard en omvang gedaan kunnen worden wanneer alle betrokken partijen dezelfde definities gebruiken. 'Internet' uit figuur 1 heeft in de nieuwe indeling, die ook wordt gebruikt in dit rapport, de benaming 'fraude met online handel' gekregen, hetgeen de lading van de aangiften beter dekt. De babeltruc betreft een modus operandi en is als trend opgenomen in hoofdstuk 3. Identiteitsdiefstal wordt beschouwd als een faciliterende fraudevorm, ook wel *de moeder des fraudes* genoemd, en wordt in hoofdstuk 5 beschreven. Alle vormen van flessentrekkerij zoals gevonden in de politiesystemen waren door individuen gepleegd, en het NDB gaat over georganiseerde criminaliteit. Maar aangezien flessentrekkerij ook betrekking heeft op misbruik van rechtspersonen, wordt het besproken in de paragrafen over beleggingsfraude en faillissementsfraude. Skimmen komt voor een deel terug in het hoofdstuk over fraude met

betaalmiddelen, waarin ook creditcardfraude uitgebreid aan de orde komt. Acquisitiefraude is gehandhaafd. Tot slot komt overboekingsfraude niet meer terug. Deze vorm van fraude, waarbij papieren overschrijvingskaarten werden misbruikt, is in hoog tempo aan het verdwijnen, omdat steeds meer mensen overgaan op internetbankieren.

Ten tweede zijn de weergegeven cijfers een indicatie van de werkelijkheid. Niet iedereen doet aangifte: ongeveer 25 procent van de slachtoffers van fraude doet aangifte⁴. Slachtoffers doen bijvoorbeeld geen aangifte wanneer het schadebedrag klein is en de tijdsinvestering om aangifte te doen hoog is. Ook worden aangiften onder meerdere omschrijvingen in de politiesystemen weggeschreven. Tijdens de analyse bleek dat regio's aangiften wegschrijven onder hoofdgroepen die geen relatie hebben met fraude, zoals 'milieu'. Zo leverde zoeken op 'milieu' gecombineerd met 'fraude' 128 hits op over een periode van veertien dagen. De babbeltroc, een werkwijze om geld van slachtoffers te ontfutselen, komt in de politiesystemen voor onder de code 'oplichting', maar ook onder 'diefstal uit woning zonder braak'.

Fraude kan ook deel uitmaken van andere typen criminaliteit, en ook deze komen niet naar boven wanneer op de gerichte codes (zoals *oplichting*) wordt gezocht. De werkelijke aantallen gepleegde fraude-incidenten zullen dan ook een veelvoud van de werkelijkheid zijn.

Ten derde is twintig procent van het aantal geanalyseerde aangiften alleen onder de noemer 'niet van toepassing' te categoriseren. Dit heeft verschillende oorzaken: wanneer uit de politiesystemen een steekproef onder de code 'oplichting' wordt getrokken, komen niet alleen aangiften naar boven, maar ook mutaties (en dit is niet te voorkomen, aldus een expert). Zo werden mutaties gevonden die betrekking hadden op een aanhouding of verhoor. Soms hoorde een mutatie bij de aangifte, soms niet, dan was het simpelweg niet correct geregistreerd. Soms vinden dubbele registraties plaats, terwijl het in feite om één registratie gaat (een persoon doet telefonisch melding, maar besluit later naar het bureau te komen: niet altijd wordt dit als één registratie beschouwd). Ook kwam het voor dat een aangifte geen informatie bevatte. In totaal zeven procent van de aangiften betrof de categorie 'overig'; daarvan verschilden zaken onderling dusdanig dat ze niet onder één noemer waren te categoriseren.

⁴ Dit is afhankelijk van het al dan niet aanwezig zijn van een meldpunt; een meldpunt verlaagt de drempel voor het doen van aangifte aanzienlijk. In dat geval schatten experts dat 25 procent van de slachtoffers aangifte doet, terwijl dat bij 'geen meldpunt' wordt geschat op hooguit 5 tot 10 procent.

De percentages in figuur 1 zijn bij elkaar opgeteld minder dan 100 procent, omdat alleen de belangrijkste resultaten zijn weergegeven. Het blijkt dat in de zeventien onderzochte politieregio's fraude met online handel het meest voorkwam. Dit gebeurt overwegend via de website Marktplaats.nl. Bij dit type fraude gaat het meestal om het aanbieden van producten (vaak mobiele telefoons, navigatiesystemen en computerspelletjes), die vooruit betaald moeten worden, maar vervolgens niet geleverd worden. De fraudeur kan van achter zijn computer door het hele land (en daarbuiten) slachtoffers maken. Aangiften worden daardoor over verschillende regio's verspreid gedaan. Aangezien gegevens (nog) niet gekoppeld worden en als gevolg daarvan een landelijk overzicht ontbreekt, kunnen fraudeurs lang hun gang gaan.

In de grote regio's kwamen de babbeltruc en skimmen vaker voor dan in de kleine regio's. Bij een babbeltruc doen oplichters zich bijvoorbeeld voor als medewerker van een zorginstelling of bank, of als dakdekker. Zij bellen bij mensen aan, vaak ouderen, en proberen binnen te komen met het doel om de bankpas te ontvreemden en de pincode te ontfutselen. Vervolgens halen zij de bankrekening leeg. Ook komt het zogenaamde *shouldering* regelmatig voor: fraudeurs kijken over de schouder van een pinnend slachtoffer mee, stelen vervolgens de pinpas om daarna de bankrekening te plunderen. Bij skimmen wordt door criminelen de magneetstrip van een bankpas gekopieerd en de pincode bemachtigd op het moment dat er een betaaltransactie wordt verricht. Vervolgens maken ze een kopie van de pas, en samen met de pincode kunnen ze geld opnemen en betalen in binnen- en buitenland.

2.2 Nieuw onderzoek

Bovengenoemde steekproef gaf aanleiding tot het uitvoeren van een nieuw onderzoek naar de aangiften. De resultaten die in de steekproef naar voren kwamen, zijn hierbij als uitgangspunt genomen. Omdat deze steekproef over aangiften uit 2008 ging, zijn aangiften van meer recente datum onderzocht om te bezien of er verschillen zijn. De nieuwe onderzoeksperiode loopt van 1 september 2010 tot en met 31 augustus 2011 en gaat eveneens over aangiften die als oplichting zijn geregistreerd. In tegenstelling tot de vorige analyse, die een steekproef betrof, zijn nu alle aangiften onderzocht en dat zijn er bijna 30.000. De resultaten worden uitgebreid beschreven in hoofdstuk 3.

2.3 Buitenlandse rechtshulpverzoeken

Inkomende buitenlandse rechtshulpverzoeken over fraude komen binnen bij het Landelijk Internationaal Rechtshulpcentrum (LIRC) van het KLPD. De verzoeken worden ingevoerd in Luris, een landelijk werkend postarchiefsysteem.

Tabel 1

Fraude in Luris			
Buitenlandse rechtshulpverzoeken	2008	2009	2010
Bancaire fraude	46	95	119
Beleggingsfraude	14	9	11
Computercriminaliteit	38	119	197
EAB ⁵ -fraude, incl. schade financiële belangen EU	9	51	51
EAB-oplichting	11	60	62
EAB-opzettelijke brandstichting	4	3	– ⁶
EU-fraude	20	60	46
Fiscale fraude	91	290	347
Geneesmiddelen	15	30	17
Internetfraude	46	137	137
Krediet-/faillissementsfraude	11	19	30
Oplichting	172	1549	1475
Overige economische delicten	44	134	127
Overige fraude	131	910	654
Skimmen	41	224	204
Telecomfraude	1	– ⁶	2
Valse merkartikelen	23	46	20
Verzekeringsfraude	5	8	2
Werknemers-/werkgeversfraude	8	56	22

⁵ Het EAB (Europees Aanhoudingsbevel) is na de aanslagen van 11 september 2001 ingevoerd, om het uitleveren van verdachten of veroordeelden binnen de EU te vergemakkelijken.

⁶ Geen informatie beschikbaar.

2.4 Bovenregionale Recherche

Het programma Versterking Programmatische Aanpak Financieel-Economische Criminaliteit (FinEC) richtte zich onder meer op het terugdringen van financieel-economische criminaliteit en fraude. De Bovenregionale Recherche (BR) leverde haar bijdrage door middelzware en zware horizontale fraudezaken op te sporen.

In de jaren 2008, 2009 en 2010 hadden de verschillende BR's gemiddeld 25 onderzoeksvoorstellen met betrekking tot middelzware zaken. Het zwaartepunt lag op faillissementsfraude (7 zaken), oplichting (4) en hypotheekfraude (4). Bij de vijftien onderzoeksvoorstellen met betrekking tot zware zaken lag het zwaartepunt op witwassen (4), beleggingsfraude (2) en bancaire fraude (2).

2.5 De Financial Intelligence Unit (FIU)

Bij veel vormen van fraude wordt geld overgemaakt naar bankrekeningen of door middel van *moneytransfers*. De FIU beschikt over een database waarin een groot aantal *moneytransfers* als ongebruikelijke transactie is vastgelegd (de meldgrens is 2000 euro). Door koppeling van informatie van de melders over de wijze van betaling en de relevante financiële stromen, in combinatie met analyse van gegevens uit deze database, kunnen verbanden worden blootgelegd waardoor daders geïdentificeerd worden. Wanneer ongebruikelijke transacties als verdacht worden aangemerkt, worden ze overgedragen aan de regiokorpsen voor verder onderzoek.

Aan de FIU is gevraagd om op basis van *moneytransfers* een overzicht te geven van de ongebruikelijke en verdachte transacties richting Ghana en Nigeria voor subjecten met een Nederlandse afkomst. Het doel was om zicht te krijgen op mogelijke slachtoffers van voorschotfraude. De onderzoeksperiode betrof veertig maanden tussen januari 2008 en mei 2011. Bij de beantwoording merkte de FIU (2011) allereerst op dat de uitgaande geldstroom naar Ghana en Nigeria groter is dan die naar andere landen in de wereld: 89 procent van alle transacties met Ghana en Nigeria was uitgaand, terwijl dat percentage wereldwijd op 82 ligt.

Van de ruim 31.000 transacties naar Ghana en Nigeria werden er iets meer dan 17.600 gedaan door Nederlandse subjecten. Hierbij waren vijfduizend subjecten betrokken en het ging om een bedrag van 4,7 miljoen euro. Het aantal transacties en de gemoeide bedragen naar beide landen zijn ongeveer gelijk. Tot 2008 was het aantal transacties naar Nigeria hoger, maar tussen 2006 en 2008

is een daling te zien. Dit was het gevolg van de aandacht destijds vanuit de opsporing naar 419-fraude of voorschotfraude (project Apollo). Vanaf het derde kwartaal van 2009 nam het aantal transacties naar Nigeria weer toe. Van alle transacties naar Nigeria en Ghana door Nederlandse subjecten werd 40 procent vanuit Amsterdam verstuurd.

Bovenstaande resultaten zijn op deze plaats opgenomen, en niet in de paragraaf over voorschotfraude. De FIU richt zich namelijk alleen op geldstromen en onderzoekt niet het achterliggende delict. Daarom kunnen hierover geen uitspraken worden gedaan. Een expert schat dat echter zeventig procent van de ongebruikelijke transacties die gemeld worden bij de FIU, het gevolg is van een of andere vorm van fraude.

2.6 De Fraudehelpdesk

Aan het eind van 2010 kreeg het Steunpunt Acquisitiefraude (SAF) in Apeldoorn de opdracht om met financiële steun van het ministerie van Justitie een fraudehelpdesk in te richten. De Fraudehelpdesk startte op 26 februari 2011 en heeft het karakter van een telefonische hulplijn. Het doel is om burgers en bedrijven te behoeden voor oplichtingspraktijken en gedupeerden te verwijzen naar instanties die hen verder kunnen helpen. Burgers en bedrijven kunnen over allerlei frauduleuze zaken contact zoeken, zoals verdachte mailing waarin gevraagd wordt naar persoonlijke gegevens of waarin fantastische financiële aanbiedingen worden gedaan. Ook kunnen zij navraag doen over facturen die niet bekend voorkomen. De Fraudehelpdesk werkt samen met een groot aantal publieke en private partijen, zoals de Autoriteit Financiële Markten (AFM), MKB Nederland, de Reclame Code Commissie, VNO-NCW en het Meldpunt Cybercrime.

De Fraudehelpdesk registreert en rubriceert meldingen en dit leverde over de periode 26 februari tot en met 31 december 2011 de volgende aantallen op:

Er werd 10.811 maal contact gezocht met de Fraudehelpdesk en er was in totaal afgerond 9,5 miljoen euro aan betaalde schade. Dit bedrag had betrekking op 843 melders, die gemiddeld 11.200 euro aan daders betaald hadden. De gemelde schade bedroeg afgerond 12 miljoen euro.

Een meerderheid van de meldingen had betrekking op:

- acquisitiefraude en spooknota's: 594 meldingen. In totaal 63 slachtoffers betaalden gemiddeld 641 euro (totaal 40.445 euro).
- fraude met online handel: 608 meldingen, 403 slachtoffers betaalden gemiddeld 492 euro (totaal 158.000 euro).
- voorschotfraude: 556 meldingen, 76 slachtoffers betaalden gemiddeld 42.280 euro (totaal 3,2 miljoen euro); 40 meldingen hadden betrekking op *datingfraude*, de slachtoffers hiervan maakten afgerond 1,7 miljoen euro over, dat was gemiddeld 43.000 euro.
- cybercrime: 2037 meldingen, 15 melders hadden een gemiddeld schadebedrag van 7700 euro (totaal 116.000 euro). Negen slachtoffers van *phishing* hadden een schade van 113.292 euro.
- beleggingsfraude: 52 meldingen, 29 slachtoffers betaalden gemiddeld 62.740 euro (totaal 1,8 miljoen euro).

Melders en slachtoffers waren bij de Fraudehelpdesk terechtgekomen via Twitter, de televisieprogramma's *Vara's Kassa* en *Tros Opgelicht*, de NOS en het SAF (dat onderdeel is van de Stichting Aanpak Financieel-Economische Criminaliteit in Nederland (SafeCin)).

Begin 2012 zijn de activiteiten van de Fraudehelpdesk geëvalueerd, en op basis daarvan is de subsidie met een jaar verlengd.

2.7 De Fraudemeldpunten

De Fraudemeldpunten (FMP's) zijn rond 1998 opgericht om als meldpunt voor private partijen te dienen en, indien mogelijk, de fraude aan te pakken.

De zes Fraudemeldpunten zijn opgericht onder verantwoordelijkheid van het Openbaar Ministerie. Bij ieder arrondissementsparket, waarin een centrumkorp van een bovenregionaal rechercheteam was gevestigd, werd een FMP ingericht. Ieder FMP kreeg taakaccenten toebedeeld, kreeg informatie van de branches (banken, verzekeringsmaatschappijen of telecombedrijven) en verzamelde informatie van fraudezaken die voldeden aan de bovenregionale criteria. Het doel was dat de FMP's een cruciale rol zouden vervullen bij het inwinnen en verder verwerken van de bovenregionale fraude-informatie.

Uit interviews met vertegenwoordigers van de FMP's in 2008 naar de informatiebronnen, de wijze van verwerking van de fraude-informatie en de aard, omvang en ernst van de belangrijkste vormen van fraude kwam het volgende naar voren:

- De fraude-informatie uit de politiesystemen bleek voor een aantal FMP's niet toegankelijk en kon niet worden benut (deze informatie is alleen toegankelijk wanneer politiemensen werkzaam zijn bij het FMP).
- De FMP's gebruikten ieder eigen systemen om fraude-informatie vast te leggen, waardoor onderlinge uitwisseling niet mogelijk was. De door henzelf verzamelde informatie werd niet in de politiesystemen vastgelegd. Bovendien had een aantal FMP's onvoldoende capaciteit om alle fraudesignalen te verwerken.
- De branches melden selectief en doen in veel gevallen alleen aangifte als er ook een onderzoek volgt. Hierdoor worden de keuzemogelijkheden en prioritering beperkt. De FMP's hebben daardoor een beperkt zicht op de aard, omvang en ernst van de fraude in hun gebied.

De conclusie was dat de FMP's van elkaar verschillen qua personele bezetting en de wijze waarop fraude-informatie wordt ingewonnen en vastgelegd. De interviews gaven de stand van zaken in 2008-2009 en omdat de werkwijze van de fraudemeldpunten verbetering behoeft, is besloten tot een doorontwikkeling. Ten tijde van het opstellen van dit deelrapport was de volgende informatie beschikbaar: de intelligencetaak wordt overgedragen aan de politie, de Regionale Informatie Organisatie en de Dienst IPOL; de landelijke accounts (Verbond van Verzekeraars, Nederlandse Vereniging van Banken, VNO-NCW) worden beleidsmatig belegd bij het Functioneel Parket en tot slot worden de zes Fraudemeldpunten vervangen door tien FinEC-punten (op elk regioparket één) voor expertiseopbouw, beleidsontwikkeling, sturing op intelligence en zaaksafdoening.

De transitie wordt door OM en politie samen vormgegeven aan de hand van twee prioritaire thema's: verzekeringsfraude en faillissementsfraude, en er wordt aangesloten bij de inrichting van de nationale politie.

2.8 Meldpunt Internetoplichting

Omdat er signalen waren dat op online handelsplaatsen veelvuldig werd gefraudeerd, is in oktober 2010 een proeftuin van start gegaan met financiering van het Programma Aanpak Cybercrime (PAC). De proeftuin werd ondergebracht bij het Fraudemeldpunt Noordwest Nederland onder de naam Meldpunt Internet-

oplichting (MIO). Aanvankelijk was het de bedoeling om alle vormen van internetoplichting op te nemen, maar omdat het aantal meldingen over fraude op Marktplaats.nl overweldigend was, heeft het MIO besloten zich alleen daarop te richten. Na evaluatie zal het meldpunt mogelijk worden uitgebreid naar andere online handelsplaatsen, zoals eBay, Speurders en Tweakers.

De werkwijze van het meldpunt is als volgt:

Er is aansluiting gezocht bij www.politie.nl, waarin een aantal (niet alle) korpsen een boete- en aangiftevolgsysteem heeft ondergebracht. Op deze website kan iedere inwoner van Nederland aangifte doen van fraude op een van de online handelsplaatsen: de aangever wordt naar een formulier geleid met verschillende verplichte velden (er wordt onder meer gevraagd naar het burgerservice-nummer). Het voordeel is dat gedupeerden geen aangifte hoeven doen bij de politie, wat niet alleen efficiënt is voor de melder, maar ook de politie veel werk uit handen neemt.

In eerste instantie konden gedupeerden slechts een melding doen. Alleen de meldingen die voor vervolgactie in aanmerking kwamen, werden omgezet in een aangifte, maar inmiddels zijn alle meldingen aangiftes. Vervolgens bepaalt het MIO of de aangifte in aanmerking komt voor strafrechtelijk onderzoek. In dat geval wordt de uitgeprinte aangifte per post naar de aangever gestuurd, met het verzoek deze te tekenen en van een kopie van het legitimatiebewijs te voorzien, en dan te retourneren. Aangevers kunnen via het aangiftevolgsysteem de status van de aangifte volgen. Als de status niet wijzigt, krijgen de aangevers na zes weken automatisch een mailbericht waarin wordt aangegeven dat de aangifte nog niet in onderzoek is genomen. Na zes maanden volgt een mail dat de aangifte vooralsnog niet voor verder onderzoek in aanmerking komt.

Marktplaats.nl krijgt een afschrift van de melding. Dit is mogelijk op grond van art. 20 Wet Politiegegevens, informatieverstrekking buiten het politiedomein. Ook de verdachte krijgt een reactie in de vorm van een waarschuwing (waardoor in sommige gevallen toch tot snelle levering van een product wordt overgegaan).

Deze aanpak is efficiënt en effectief. Er kan laagdrempelig aangifte worden gedaan, er vindt centrale intake en bundeling van informatie plaats, het MIO bereidt zaken voor, vooral gericht op veelplegers, en tot slot is er een goede samenwerking en kennisdeling tussen het Openbaar Ministerie, de politie en Marktplaats.

Het aantal meldingen en aangiften die via het MIO zijn gedaan, en de omvang van de schade staan vermeld in paragraaf 4.1.

2.9 Overige meldpunten

Naast de Fraudemeldpunten en het Meldpunt Internetoplichting zijn er de volgende meldpunten:

- het Meldpunt Cybercrime van het KLPD: in het leven geroepen voor meldingen over kinderporno en terrorisme, maar krijgt ook meldingen over verschillende vormen van fraude binnen. Hierover wordt geen informatie vastgelegd.
- het Centraal Meldpunt Identiteitsfraude (CMI) is ondergebracht bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. In een periode van een jaar (maart 2010 – maart 2011) kreeg het 260 concrete meldingen, waarvan 75 procent afkomstig was van burgers, de overige meldingen kwamen van private en publieke partijen. De identiteit van burgers was vooral misbruikt voor het plegen van fraude bij banken, telecombedrijven, webwinkels en energiebedrijven. Het gemiddelde schadebedrag was 8800 euro (CMI, 2012).
- Het Steunpunt Acquisitiefraude (SAF), zie paragraaf 4.4.

2.10 Nationaal Platform Criminaliteitsbeheersing

In februari 2012 heeft de minister van Veiligheid en Justitie het Actieplan Criminaliteit tegen Bedrijven naar de Tweede Kamer gestuurd. Naast winkeldiefstal en heling is de aanpak van fraude tot speerpunt benoemd. Aandacht krijgen acquisitiefraude en *massmarketingfraude* omdat het bedrijfsleven daarvan veel schade heeft en hinder ondervindt. De nadruk ligt op voorlichting, alarmeringen en het opwerpen van barrières om zoveel mogelijk slachtoffers te voorkomen. Het Actieplan wordt uitgevoerd onder regie van het Nationaal Platform Criminaliteitsbeheersing (NPC), dat een samenwerkingsverband is op bestuurlijk niveau tussen overheid en bedrijfsleven.

2.11 Landelijk skimmingpoint

Op 1 december 2011 is het startsein gegeven voor de lancering van het landelijk skimmingpoint. Het doel hiervan is informatie over skimmen op één centrale plek te verzamelen en te analyseren. Behalve politie participeren het OM en

Equens⁷, en wordt samengewerkt met de Electronic Crimes TaskForce (ECTF) van het KLPD, het Interregionale Bureau Geld- en Waardeverkeer (IBGW), de BR's Zuid-West en Zuid-Nederland en Europol.

2.12 Expertiseknooppunt FinEC

Binnen de nieuwe Nationale Politie ligt de oprichting van een centraal Expertiseknooppunt FinEC in het verschiet. Het expertiseknooppunt streeft naar vier taakgebieden, namelijk zaaksondersteuning, informatieknooppunt, centraal aanspreekpunt en strategische beïnvloeding.

⁷ Equens zorgt op Europees niveau voor de verwerking van girale – en cards gerelateerde betalingen.

3

Analyse aangiften

Zoals beschreven in paragraaf 2.1 is een steekproef geanalyseerd bestaande uit aangiften die in 2008 onder *oplichting* zijn geregistreerd in de politiesystemen. Dit gebeurde in opdracht van het BRO om aard en omvang in beeld te brengen, en de haalbaarheid van een fraudemonitor te onderzoeken. Omdat uit deze steekproef bleek dat het merendeel van de fraudezaken onder *oplichting* is geregistreerd, is dit ook het uitgangspunt geworden voor de twee datasets die zijn gebruikt voor dit deelrapport. De eerste dataset bestrijkt een periode van een jaar (1 september 2010-31 augustus 2011) en dat zijn er in totaal 29.713. Met deze (grote) dataset was het mogelijk om een beeld te geven van de aantallen van de verschillende hoofdvormen van fraude, maar daarnaast ook een verdieping te maken op vormen die minder frequent voorkomen. Voor de tweede dataset is per jaar, uit de periode 2007 tot en met 2010, een steekproef getrokken van tien procent uit *oplichting*. Met deze steekproef was het mogelijk om uitspraken te doen over de ontwikkeling van onder andere de omvang van de fraudevormen, en een vergelijking te maken met de steekproef uit 2008.

Van de eerste dataset zijn niet alle 29.713 aangiften gebruikt voor onze analyse-doelstellingen, maar alleen de ruim 10.500 die binnen de tien hoofdvormen van horizontale fraude passen. Dit had een aantal redenen. Ten eerste hebben niet al deze aangiften betrekking op fraude. Ten tweede omdat wij ons in dit rapport door een tijdslimiet hebben beperkt tot die tien hoofdvormen van fraude. Van iedere aangifte is bepaald of deze in één van de tien hoofdvormen kon worden ingedeeld. Alle andere aangiften zijn in het vervolg van dit rapport buiten beschouwing gelaten. Dit wil niet zeggen dat in deze restgroep geen fraudegevallen voorkomen. Een klein aantal daarvan zijn aangiften die, ondanks onze zorgvuldig geformuleerde zoekvragen, onterecht in de groep 'overige' zijn achtergebleven. Bij een groot aantal aangiften in deze restgroep zal het waarschijnlijk niet om fraudegevallen gaan. Ten slotte zal een aantal aangiften gaan over fraudesoorten die buiten ons onderzoeksdomein vallen en daardoor niet worden meegenomen in onze zoekvragen. Weliswaar is deze laatste groep interessant om in beeld te krijgen, maar hiervoor is een grondige analyse van de 'overige' aangiften noodzakelijk, en dat was binnen het tijdsbestek van dit onderzoek niet mogelijk.

In dit hoofdstuk wordt beschreven hoe de analyse is uitgevoerd. Het doel hiervan is om de totalen van de verschillende hoofdvormen van horizontale fraude in beeld te krijgen uitgaande van de politiesystemen. Indien de informatie aanwezig is in de aangiften, worden ook specifieke modi operandi of kenmerken, zoals schadebedragen, in kaart gebracht. Tot slot wordt in kaart gebracht hoe de verschillende fraudevormen zich in de afgelopen jaren qua omvang hebben ontwikkeld. Bij de resultaten tekenen wij aan dat het gaat om de totalen in de politiesystemen. De aangiftebereidheid bij het delict fraude is vaak niet hoog, maar verschilt ook per fraudevorm: aangiften van merkfraude, bijvoorbeeld, zijn waarschijnlijk minder talrijk dan het aantal meldingen of aangiften van fraude met online handel. Hieruit kan echter niet automatisch worden geconcludeerd dat de ene fraudevorm minder voorkomt dan de andere.

Wanneer een vorm van fraude in de politiesystemen vaak voorkomt, zegt dit iets over het aantal slachtoffers van deze specifieke fraudevorm. Ook kan het iets zeggen over de opvattingen die bij de burgers leven over waar de politie zich bij de bestrijding op dient te richten. De overweging om wel of niet aangifte te doen, hangt af van veel factoren. Het is onder andere afhankelijk van de mate van eigen schuld die burgers al dan niet ervaren, en de schaamte of verontwaardiging die zij voelen over wat hen is overkomen. Het is ook afhankelijk van het beeld dat burgers hebben van de mate van actiebereidheid van de politie na het doen van de aangifte. Dit beeld is vaak niet positief. Tot slot speelt het hebben van een meldpunt een rol, omdat een meldpunt de drempel tot het doen van aangifte verlaagt.

BRAINS

Binnen de politie worden veel gegevens verzameld, en informatie over incidenten en delicten worden uitgebreid gedocumenteerd. Het probleem is dat veel van de opgeslagen gegevens achteraf moeilijk te doorzoeken zijn, omdat de informatiesystemen niet aansluiten bij de huidige informatiebehoefte. De applicatie BRAINS (Basaal Recherche Analyse INStrument) maakt het mogelijk om de informatie die is opgeslagen in de politiesystemen te ontsluiten en te analyseren (DREO, 2010; KLPD, Dienst IPOL, 2010b).

Om na te gaan welke aangiften onder welke hoofdvorm van fraude vallen, zijn zoekvragen geformuleerd. Een overzicht hiervan is terug te vinden in bijlage III. Wanneer alle zoekvragen tegelijk worden toegepast op het totaal, blijven de aangiften over die onder de tien hoofdvormen kunnen worden gecategoriseerd. Tabel 2 geeft een overzicht hiervan.

Tabel 2

Aantal aangiften per jaar en het aantal hoofdvormen gebruikt voor analyse			
Jaar	Aangiften	Aangiften hoofdvormen	Percentage
Referentiejaar (2010-2011)	29.713	10.586	35,6
2010	2940	1315	44,7
2009	2219	823	37,1
2008	930	275	29,6
2007	807	248	30,1

Door het toepassen van de geformuleerde zoekvragen blijven 10.586 van de 29.713 aangiften over voor verder onderzoek en dat is iets meer dan 35 procent van het totaal. Om na te gaan hoe de omvang zich heeft ontwikkeld, is per jaar over de periode 2007 – 2010 naar steekproeven uit de politiesystemen gekeken. De aantallen zijn daardoor kleiner.

De zoekvragen geven de verdeling van de hoofdvormen van horizontale fraude zoals weergegeven in tabel 3. Hieruit blijkt bijna 90 procent van de aangiften kunnen worden herleid tot fraude met online handel en fraude met betaalmiddelen. Daarnaast komt alleen voorschotfraude relatief vaak voor, met bijna zes procent. De overige zeven hoofdvormen van fraude komen slechts beperkt terug in de aangiften. In het vervolg van dit hoofdstuk zal per fraudevorm worden bekeken hoe de omvang zich in de afgelopen jaren heeft ontwikkeld. Waar mogelijk zal worden ingegaan op specifieke modi operandi.

Tabel 3

Hoofdvormen van horizontale fraude referentiejaar 2010-2011		
Fraudehoofdvorm	Aangiften ⁸	Percentage
1. Fraude met online handel	7306	69,0
2. Fraude met betaalmiddelen	2011	19,0
3. Voorschotfraude	604	5,7
4. Acquisitiefraude	255	2,4
5. Hypotheekfraude	253	2,4
6. Telecomfraude	172	1,6
7. Verzekeringsfraude	142	1,3
8. Faillissementsfraude	81	0,8
9. Beleggingsfraude	14	0,1
10. Merkfraude	10	0,1

3.1 Fraude met online handel

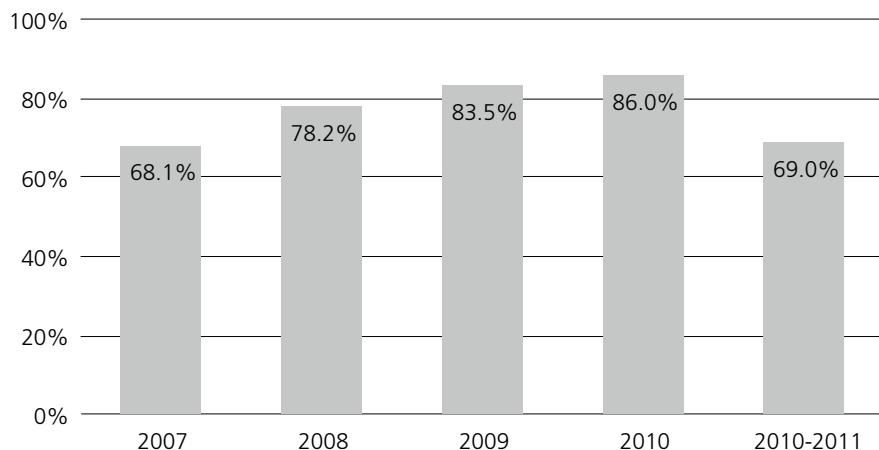
Fraude met online handel, meestal Marktplaats.nl, is verreweg de meest voorkomende vorm van fraude. In het referentiejaar 2010-2011 is bijna een kwart van alle aangiften die geregistreerd staan onder *oplichting*, fraude met online handel; in de steekproef van 2008 was dat 27% (zie paragraaf 2.1).

In de periode 2007-2010 varieert dat van ongeveer 70 procent in 2007 tot 86 procent in 2010 (zie figuur 2). Het neemt van jaar tot jaar toe, en in het referentiejaar 2010-2011 (de laatste kolom) neemt het weer af. Dit is te verklaren door de oprichting van het Meldpunt Internetoplichting (MIO). In het eerste jaar konden gedupeerden bij het MIO wel melding, maar geen aangifte doen van fraude. Daardoor kwamen minder aangiften binnen. Wanneer tot vervolging werd overgegaan, werd de melding omgezet in een aangifte. Sinds kort hebben alle meldingen bij het MIO het karakter van een aangifte, maar dit is nog niet terug te zien in figuur 2 (de aantallen zouden dan hoger moeten zijn).

⁸ Het opgetelde aantal aangiften is niet gelijk aan de 10.362, en de percentages tellen op tot boven de 100 omdat aangiften in meer dan een hoofdvorm kunnen worden gecategoriseerd.

Figuur 2

Fraude met online handel 2007-2011



De modus operandi van deze fraudevorm bestaat vrijwel altijd uit het niet opsturen van goederen, waarvoor door het slachtoffer wel is betaald, ofwel voor het niet betalen van goederen die wel zijn opgestuurd. In de meeste gevallen gaat het om relatief lage bedragen: variërend van rond de honderd euro tot enkele honderden euro's. Zaken van duizend euro zijn een uitzondering. Tabel 4 geeft een overzicht van de soorten goederen en de modi operandi in het referentiejaar.

Tabel 4

Fraude met online handel (producten en modi operandi)			
Goederen	Aantal aangiften	Modus operandi	Aantal aangiften
(Mobiele) telefoon	1615	Betaald, niet ontvangen	1579
(Spel)computers	1393	Verstuurd, niet betaald	189
Toegangskarten (o.a. concert of evenement)	795		
Schoenen	302		
Ipods en mp3-spelers	244		

Het gaat in bijna alle gevallen om elektronische producten en gadgets. Uitzondering hierop is de categorie schoenen en toegangskarten. Binnen alle categorieën vinden grote verschuivingen plaats op basis van modetrends. Zo heeft een derde van de aangiften van niet geleverde schoenen betrekking op het merk Uggs, in de afgelopen jaren een erg 'gewild' merk. Hetzelfde speelt binnen de categorie mobiele telefoons, waarbij een groot deel, 563 aangiften, is terug te voeren op de iPhone 4. De fraudeurs volgen de hypes en trends in de legale markten. Wat betreft modus operandi komt het niet leveren van producten waarvoor wel betaald is veel vaker voor dan het omgekeerde waarbij niet betaald is voor wel geleverde goederen.

Binnen deze aangiften zijn ongeveer vijftientig groeperingen van daders actief die terugkomen in vijf of meer verschillende aangiften⁹. Een aantal van deze groepen schermde zich af door gebruik te maken van bankrekeningen die katvangers tegen een geringe vergoeding ter beschikking stelden voor de betalingen. Producten die door deze groepen werden aangeboden, zijn doorgaans de eerder genoemde populaire producten als mobiele telefoons, mp3-spelers of toegangskarten voor evenementen als concerten en dansfeesten. Soms boden ze ook op het oog minder populaire producten aan, zoals gourmetstellen of bepaalde koffieapparaten.

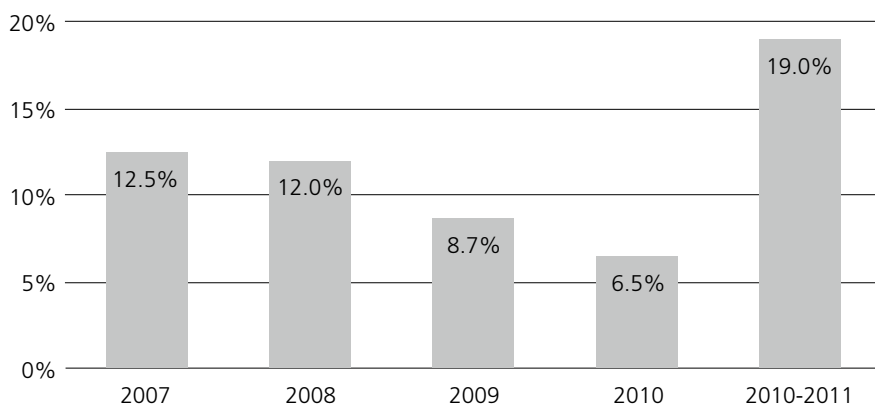
3.2 Fraude met betaalmiddelen

Fraude met betaalmiddelen komt eveneens frequent voor. In de periode 2007-2010 is het percentage aangiften jaarlijks afgenomen van ongeveer 12,5 procent in 2007 tot 6,5 procent in 2010 (zie figuur 3).

⁹ In deze analyse spreken we van georganiseerdheid als één of meer daders verantwoordelijk zijn voor vijf of meer aangiften. Daarvoor is gekozen omdat kenmerken over georganiseerdheid vaak ontbreken in de aangiften.

Figuur 3

Fraude met betaalmiddelen 2007-2011



Maar in het referentiejaar 2010-2011 is er weer een forse toename te zien, namelijk tot 19 procent. In het referentiejaar 2010-2011 gaat het in bijna zeven procent van alle aangiften die geregistreerd staan onder *oplichting*, om fraude met betaalmiddelen (niet in de figuur).

Fraude met betaalmiddelen wordt op diverse manieren gepleegd, bijvoorbeeld door het *skimmen* van betaalpassen of het *phishen* van inloggegevens van (internet)rekeninghouders. In tabel 5 is een overzicht te zien van de frequentie van een aantal modi operandi. Daaruit blijkt dat fraude met internetbankieren verreweg het meest voorkomt in de aangiften, gevolgd door respectievelijk skimming, phishing en hengelen. De laatste modus operandi, waarbij men betaalpassen letterlijk uit de brievenbus hengelt, komt slechts in 29 aangiften terug.

Tabel 5

Fraude met betaalmiddelen	
Modus operandi ¹⁰	Aantal aangiften
Internetbankieren	1181
Skimming	544
Phishing	292
Hengelen	29

Vormen van fraude met betaalmiddelen waarbij men geen gebruik maakt van 'moderne technieken' zoals het internet, zijn in de loop der jaren een steeds minder grote rol gaan spelen.

Binnen de aangiften is er weinig zicht op de groeperingen die deze vorm van fraude plegen. Slechts drie groepen van daders kwamen terug in vijf of meer verschillende aangiften. De eerste groep hield zich bezig met het *skimmen* van betaalpassen. Leden van de tweede groep hielden zich bezig met fraude met internetbankieren. Rekeninghouders werden benaderd door een lid van deze dadergroep die zich voordeed als een medewerker van de bank. De bank zou bezig zijn met het controleren van persoonsgegevens of willen weten of men wel eens had gehoord van internetfraude. Vervolgens werd deze personen gevraagd naar hun tan-codes, waardoor de fraudeurs geld van de rekening konden afboeken. Voorafgaand aan het telefonisch contact hadden de slachtoffers een *phishingmail* ontvangen waarin zij op een link moesten klikken om actief gebruik te kunnen blijven maken van hun internetrekening. De derde groep fraudeurs ronselde mensen om hun bankrekening ter beschikking te stellen. Veelal ging het om scholieren in de leeftijd van 15 tot 18 jaar, hoofdzakelijk met een niet-Nederlandse etniciteit. Vaak deden zij zelf aangifte dat ze hun pas en pincode hadden verloren. Bedragen die via hun rekening werden overgemaakt, werden in andere delen van het land opgenomen.

3.3 Voorschotfraude

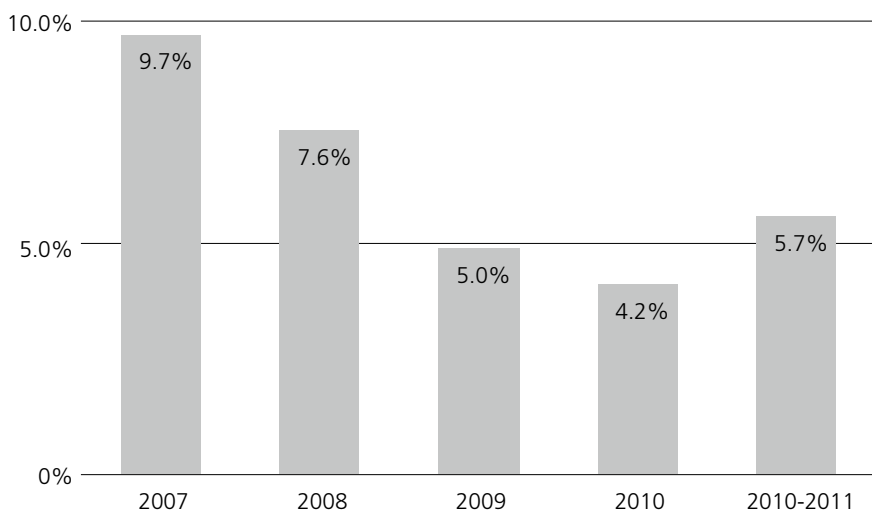
Voorschotfraude is qua frequentie de derde hoofdvorm van fraude. In de periode 2007-2010 is het percentage aangiften dat betrekking heeft op voorschotfraude steeds afgenomen van ongeveer 9,7 procent in 2007 tot

¹⁰ In deze tabel staan de modi operandi los van elkaar vermeld, maar in de praktijk gaan ze vaak samen.

4,2 procent in 2010 (zie figuur 4). Maar in het referentiejaar 2010-2011 is weer een lichte stijging te zien. Voorschotfraude is verantwoordelijk voor 5,7 procent van de aangiften binnen de tien hoofdvormen van fraude. In het referentiejaar 2010-2011 gaat het in twee procent van alle aangiften die onder *oplichting* geregistreerd staan, om voorschotfraude.

Figuur 4

Voorschotfraude 2007-2011



Voorschotfraude bestaat uit allerlei vormen van oplichting waarbij het slachtoffer onder valse voorwendselen wordt verzocht voorschotten te betalen, met een veel grotere beloning in het vooruitzicht. Binnen de aangiften van voorschotfraude was er in ongeveer 100 van de 604 gevallen sprake van erfenisfraude; in 53 gevallen was er sprake van datingfraude; tot slot was bij 29 aangiften sprake van loterijfraude¹¹. Om in contact te komen met hun slachtoffers maken de fraudeurs gebruik van de vele mogelijkheden die internet biedt, zoals e-mail, datingsites, chatrooms, veilingssites en online handelsplaatsen.

¹¹ Voor een uitgebreide beschrijving van erfenis-, dating- en loterijfraude verwijzen we naar paragraaf 4.3.

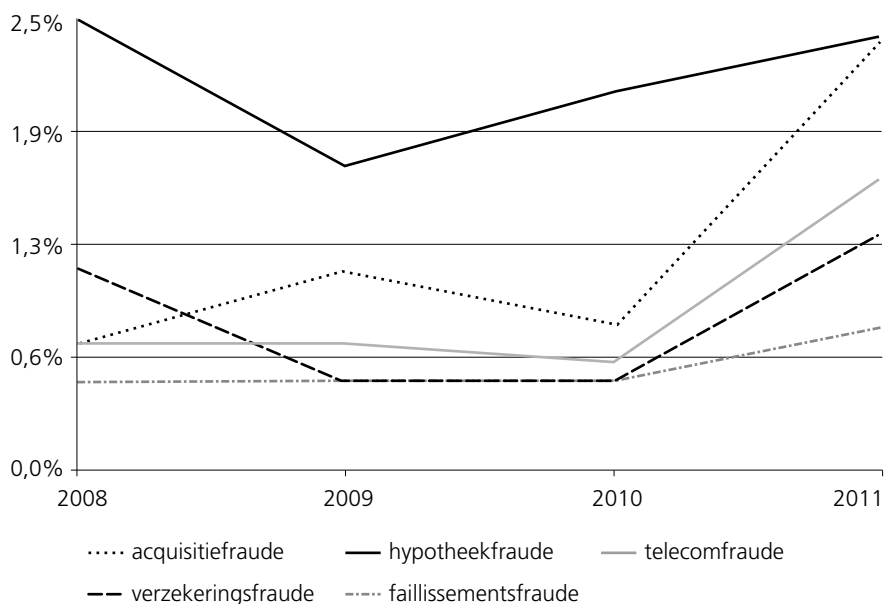
Uit de aangiften zijn geen groeperingen te halen die verantwoordelijk zijn voor vijf of meer aangiften van voorschotfraude. Dit komt waarschijnlijk omdat de fraudeurs vaak vanuit het buitenland opereren. Hierdoor zijn zij weinig in beeld, waardoor het moeilijk is om aangiften te koppelen. Het gaat bij voorschotfraude altijd om georganiseerde vormen van criminaliteit. Dit wordt nader omschreven in paragraaf 4.3.

3.4 Laagfrequente vormen van fraude

De nog niet besproken vormen van fraude komen in veel mindere mate voor in de aangiften¹². Daarom dienen de uitkomsten van de ontwikkelingen in de afgelopen jaren met enige terughoudendheid te worden beschouwd.

Figuur 5

Laagfrequente vormen van fraude 2008-2011 in percentages van de tien hoofdvormen



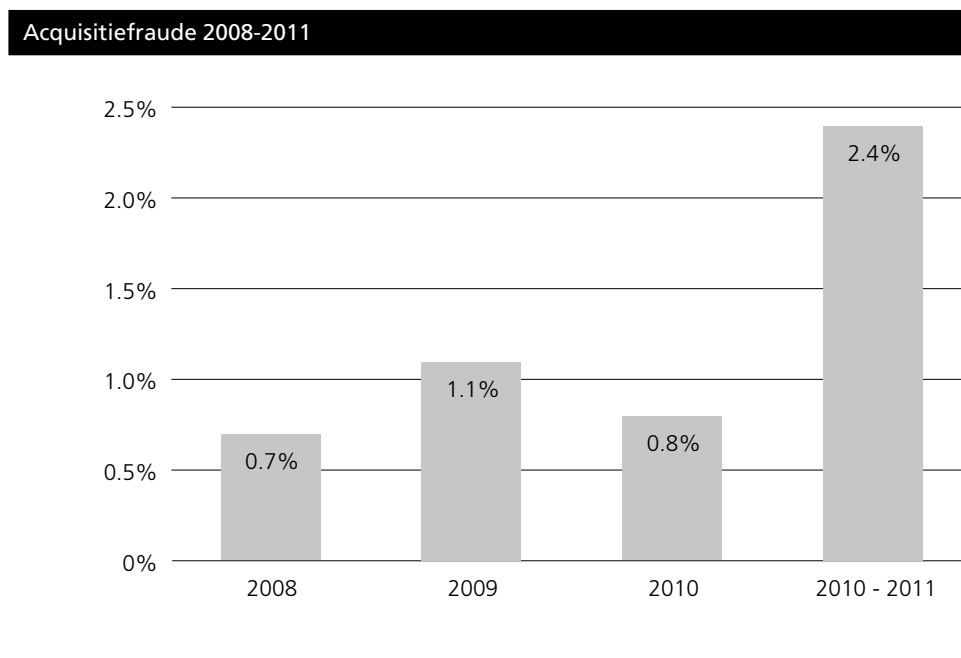
¹² Het jaar 2007 is niet meegenomen, omdat de aantallen in de eerste jaren zo laag zijn, dat kleine veranderingen in de aantallen leiden tot grote veranderingen in de percentages. Dit kan een vertekend beeld geven.

De ontwikkeling van de omvang van de zes laagfrequente hoofdvormen van fraude wordt gezamenlijk weergegeven in figuur 5. Uit deze figuur komt naar voren dat alle zes fraudevormen een stijgende trend vertonen na 2009. Een eventuele toekomstige analyse kan uitwijzen of deze stijging zal doorzetten.

3.4.1 Acquisitiefraude

Slechts 2,4 procent van de fraudeaangiften binnen de tien hoofdvormen gaat over acquisitiefraude (zie figuur 6). Wanneer we meer specifiek kijken naar de ontwikkeling van de omvang, dan zien we dat deze relatief stabiel is gebleven. In het referentiejaar is echter sprake van een verdrievoudiging, namelijk van 0,8 procent naar 2,4 procent. Deze stijging is waarschijnlijk toe te schrijven aan de spooknota's, die vanaf dat jaar ook als melding bij het Steunpunt Acquisitiefraude (SAF) werden meegenomen, bovenop de meldingen over acquisitiefraude. Het SAF stimuleert melders om aangifte te doen, omdat dit een zaak sterker maakt wanneer deze voor de rechter komt. Aangezien het om relatief kleine aantallen gaat, moet in de komende jaren blijken of de stijging doorzet.

Figuur 6



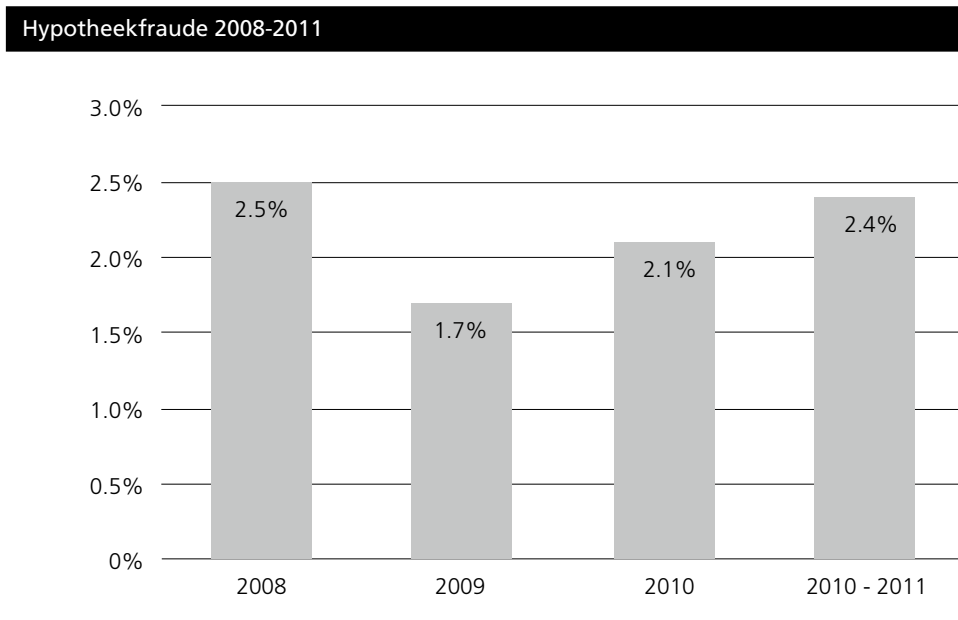
Binnen de aangiften gaat het in de meeste gevallen om spookfacturen die aan bedrijven worden opgestuurd. Hierin wordt de suggestie gewekt dat de klant een betalingsverplichting heeft, terwijl het slechts een offerte betreft.

Binnen de aangiften van acquisitiefraude is één dadergroep verantwoordelijk voor zes aangiften. Deze groep was actief in het versturen van facturen waarin zij het plaatsen van advertenties in rekening bracht. Hiervoor was door de gefactureerde geen opdracht gegeven. Onder dreiging van deurwaarders en incassokosten is een aantal slachtoffers tot betaling overgegaan.

3.4.2 Hypotheekfraude

Hypotheek – en bouwdepotfraude beslaat slechts 2,4 procent van de fraude-aangiften. In de afgelopen jaren is de omvang van deze fraudevorm stabiel gebleven, schommelend tussen de 1,7 en 2,5 procent van de fraudeaangiften (zie figuur 7).

Figuur 7



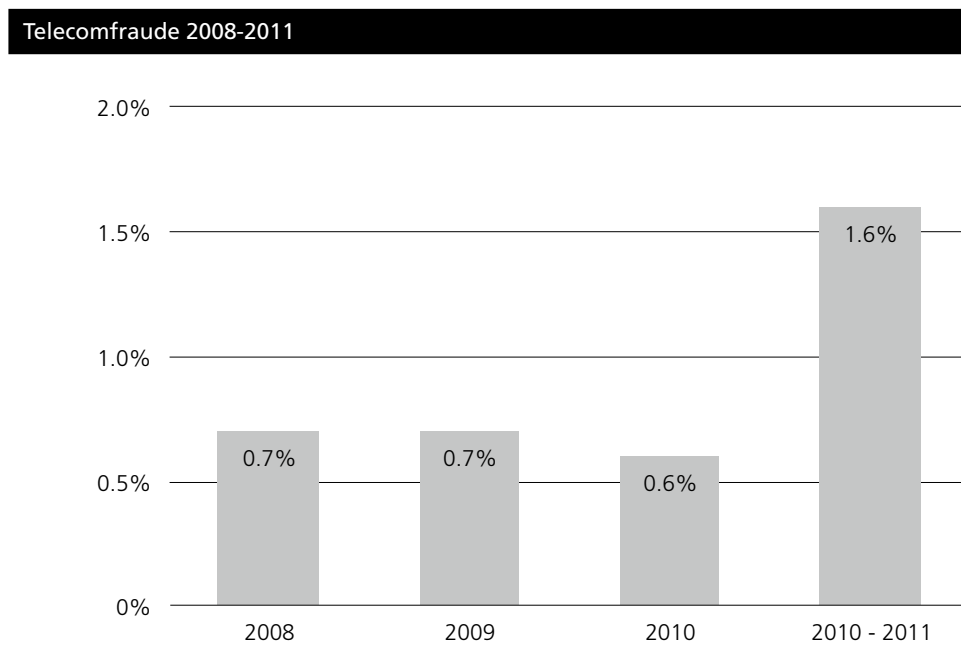
Het merendeel heeft betrekking op hypotheekfraude (234 aangiften) en een klein deel op bouwdepotfraude (46 aangiften). Vaak gaat bouwdepotfraude samen met hypotheekfraude, waardoor overlap in de aangiften kan bestaan.

Uit de aangiften komen twee groepen naar voren die gekoppeld kunnen worden aan vijf of meer aangiften. Beide groepen hadden een aantal maal een hypotheek aangevraagd met vervalste salarisgegevens en werkgeversverklaringen. Na afsluiting van de hypotheek werden de termijnnota's niet betaald en werden de eveneens afgesloten bouwdepots leeggehaald.

3.4.3 Telecomfraude

Van de fraudeaangiften van 2010-2011 ging slechts 1,6 procent over telecomfraude. De omvang van deze fraudevorm is stabiel gebleven, schommelend tussen de 0,6 en 1,6 procent van de fraudeaangiften (zie figuur 8).

Figuur 8



Het merendeel gaat over fraude met abonnementen, en een kleiner deel gaat over telefooncentrales die worden gehackt. Hierbij kraken fraudeurs de beveiliging van een telefooncentrale, waarna via deze centrales veel telefoonverkeer, met name naar het buitenland en naar dure betaalnummers wordt gegenereerd. De gemiddelde schade voor een bedrijf als gevolg van hacken loopt van ongeveer duizend euro tot enkele tienduizenden euro's.

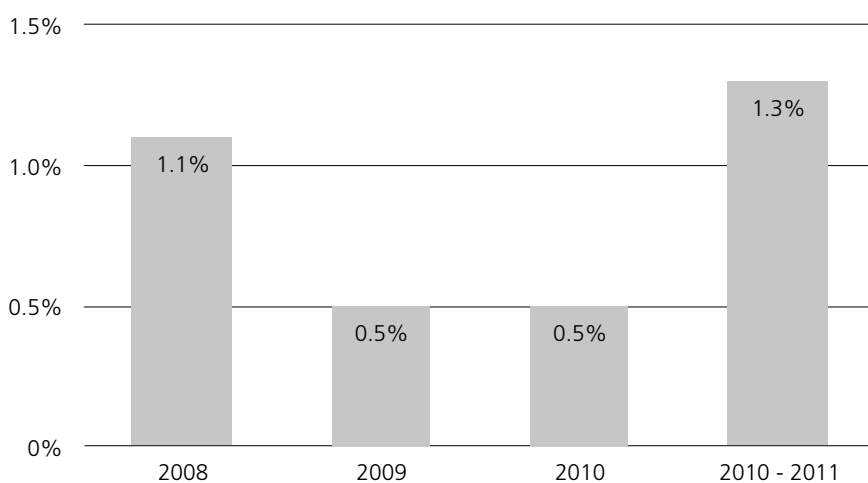
Uit de aangiften van telecomfraude zijn geen groeperingen te halen die verantwoordelijk zijn voor vijf of meer aangiften. De oorzaak is, evenals bij voorschotfraude, dat de daders van deze fraudevorm veelal vanuit het buitenland opereren. Hierdoor zijn zij weinig in beeld, waardoor het moeilijk wordt om aangiften te koppelen.

3.4.4 Verzekeringsfraude

De aangiften van verzekeringsfraude schommelden in de afgelopen jaren tussen de 0,5 en 1,3 procent van het totale aantal fraudeaangiften (zie figuur 9).

Figuur 9

Verzekeringsfraude 2008-2011



De aangiften binnen verzekeringsfraude kunnen betrekking hebben op tal van zaken. Slechts één groep kon worden gekoppeld aan vijf of meer aangiften. Deze groep lichtte de verzekering op verschillende manieren op. De fraudeurs richtten zich vooral op voertuigen waarvan de waarde een stuk hoger werd getaxeerd dan de werkelijke waarde. Dit was mogelijk door voertuigen om te katten waardoor deze op papier *oldtimers* zijn, terwijl het in werkelijkheid om een ander model ging. Vervolgens lieten de fraudeurs de voertuigen in het water zakken om de waarde waarvoor het voertuig oorspronkelijk was verzekerd te kunnen innen. Daarnaast bleken ze ook enkele elektrische fietsen als gestolen te hebben opgegeven en de facturen te hebben vervalst. In termen van schade

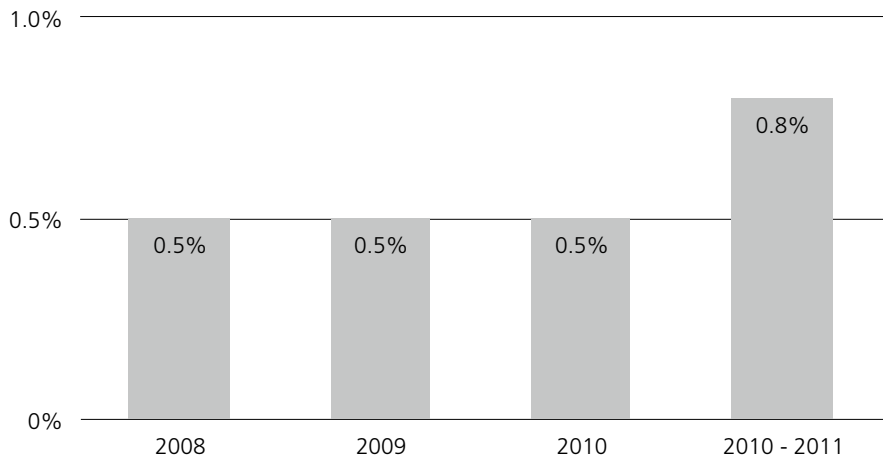
ging het om zo'n 2800 euro per fiets. Bij de voertuigen waren bedragen van 26.000 euro per voertuig gemoeid.

3.4.5 Faillissementsfraude

De hoofdvorm faillissementsfraude beslaat slechts 0,8 procent van de fraudeaangiften. In de afgelopen jaren heeft deze fraudevorm altijd tussen de 0,5 en 0,8 procent van alle fraudeaangiften uitgemaakt (zie figuur 10).

Figuur 10

Faillissementsfraude 2008-2011



Binnen de aangiften van faillissementsfraude komen met name zaken naar voren waarbij sprake is van (een vorm van) flessentrekkerij. De fraudeurs gaan verbintenissen aan met andere ondernemingen, waarbij ze goederen bestellen of diensten afnemen zonder te betalen. Hierbij gaat het onder andere om auto's, sieraden, voedsel en elektronica. De geleverde goederen worden doorverkocht, zonder betaling aan de leverancier. Uit de aangiften van faillissementsfraude zijn geen groeperingen te vinden die verantwoordelijk zijn voor vijf of meer aangiften.

3.4.6 Beleggingsfraude

Beleggingsfraude kwam slechts veertien keer voor. Daarmee is het op merkfraude na de minst voorkomende hoofdvorm van fraude. Het merendeel had betrekking op beleggingsfraude¹³, in drie gevallen was sprake van boilerroomfraude en twee aangiften hadden betrekking op piramidespelen. Bij boilerroomfraude worden potentiële slachtoffers vanuit een klein kantoor in een buitenland telefonisch benaderd met een aantrekkelijk aanbod. Bij een piramidespel krijgen deelnemers een hoog rendement op hun inleg voorgespiegeld¹⁴. De deelnemers moeten zelf nieuwkomers rekruteren, die ook geld inleggen dat (zogenaamd) wordt belegd. In de acht gevallen van beleggingsfraude werden mensen opgelicht voor bedragen variërend tussen enkele duizenden euro's tot en met 50.000 euro. Bij de drie aangiften van boilerroomfraude raakten de slachtoffers respectievelijk 6.500, 80.000 en 200.000 euro kwijt aan de fraudeurs¹⁵. De twee slachtoffers van piramidespelen waren voor respectievelijk 1.500 en 60.000 euro opgelicht. Deze bedragen bevestigen het beeld uit de *Criminaliteitsbeeldanalyse fraude* van de politie Haaglanden dat slachtoffers van beleggingsfraude gemiddeld hoge bedragen verliezen (Politie Haaglanden, 2011).

3.4.7 Merkfraude

Merkfraude betrof slechts tien aangiften. Hiermee is het met 0,1 procent van het totaal van de fraudeaangiften de minst voorkomende hoofdvorm van fraude. De slachtoffers hadden meestal via het internet, maar ook eenmaal op een braderie, valse merkartikelen gekocht, zoals een iPhone (twee maal), kettingzaag, horloge, kostuum of bodywarmer.

¹³ Om de aantallen vast te stellen zijn verschillende soorten zoekvragen gemaakt. De aangiften die niet de kenmerken van boilerroomfraude of piramidespelen hebben, vallen automatisch in de algemene categorie *beleggingsfraude*.

¹⁴ Voor een uitgebreide beschrijving van de verschillende vormen van beleggingsfraude verwijzen we naar paragraaf 4.9.

¹⁵ Dat de aantallen niet optellen tot veertien, hangt samen met de inrichting van de zoekvragen. Mogelijk is er overlap tussen de aangiften. Om dit met zekerheid vast te stellen zou een selectie van de aangiften handmatig moeten worden bekeken; dit was binnen het tijdsbestek van dit rapport niet mogelijk.

3.5 Conclusie

Uit de analyse van fraudeaangiften blijkt dat deze worden gedomineerd door twee hoofdvormen: fraude met online handel en fraude met betaalmiddelen. Samen beslaan zij bijna 90 procent van de fraudeaangiften. Slachtoffers van fraude met online handel zijn vooral particulieren die betalen voor producten die zij nooit geleverd krijgen. Bij fraude met betaalmiddelen gaat het voornamelijk om skimming en phishing, en draaien vooral banken op voor de schade die zij aan de gedupeerden vergoeden.

Vooralsnog zelden worden de gedupeerden van fraude met online handel hun geld terug gegeven. De fraudeurs die hierin actief zijn, zijn vaak individuen maar gaan regelmatig ook in georganiseerd verband te werk. Ze maken grote aantallen slachtoffers. In verhouding tot de grote hoeveelheid advertenties op de online handelsplaatsen is het aantal aangiften beperkt. Fraudeurs worden vooralsnog zelden aangepakt en hebben hierdoor vrij spel. Het gevaar bestaat dat op de lange termijn het vertrouwen in deze vorm van handel wordt ondermijnd.

Kenmerkend van de niet vaak voorkomende fraudevormen is dat het, behoudens beleggingsfraude, voornamelijk om bedrijven en private partijen gaat. Middelgrote en kleine bedrijven die de dupe worden van acquisitiefraude melden zich doorgaans bij MKB Nederland en het Steunpunt Acquisitie Fraude (SAF). Hoewel ze gestimuleerd worden om aangifte te doen, om sterker te staan wanneer het tot een zaak komt, doen ze dit weinig. Het leidt namelijk zelden tot een strafrechtelijk onderzoek en tot een rechtszaak. Ondanks de lichte stijging blijft het aantal aangiften achter bij het aantal meldingen bij MKB Nederland. De private partijen, banken, telecombedrijven, verzekeringsmaatschappijen en curatoren op het gebied van faillissementsfraude kunnen hun meldingen kwijt bij de fraudemeldpunten, maar proberen ook vaak de fraude zelf op te lossen. Van slachtoffers van beleggingsfraude is bekend dat ze uit schaamte zelden aangifte doen. Tot slot neemt merkfraude een aparte plaats in, omdat de aanpak onder andere via Europol en de douane loopt.

3.6 Discussie

De analyse van de fraudeaangiften heeft zich binnen dit onderzoek beperkt tot de omvang van de tien verschillende hoofdvormen van fraude. We hebben gekozen om de aangiften te onderzoeken die als *oplichting* geregistreerd staan, omdat onder dit label het merendeel wordt weggeschreven. In toekomstig onderzoek zou, met de binnen BRAINS ontwikkelde zoekvragen, onderzocht

kunnen worden of fraude ook in andere categorieën in de politiesystemen voorkomt, en of het om andere vormen van fraude gaat dan de vormen die nu onderzocht zijn. Er kan bijvoorbeeld worden gekeken naar alle aangiften over meerdere jaren. Het resultaat van een dergelijke analyse zou het beeld van de fraudeomvang verder kunnen aanscherpen.

Als het hanteren van de hoofdvormen wordt losgelaten, zou ook naar een bredere fraude-indeling kunnen worden gekeken, zoals massamarketingfraude. Alternatief hierop zou zijn om te focussen op een of meerdere modi operandi die de hoofdvormen van fraude overstijgen, zoals internetfraude of de babbeltruc. In deze aanpak staat de techniek veel meer centraal en niet het onderscheid in fraudevormen. Bij de keuze voor deze invalshoek ligt een sterkere nadruk op de handelswijze van fraudeurs, die zich meer en meer op het internet ophouden.

Tot slot tekenen wij aan dat de babbeltruc in de eerdere analyse van de aangiften als derde grote fraudevorm naar voren kwam. De babbeltruc wordt in de politiesystemen geregistreerd onder *oplichting* en *diefstal uit de woning zonder braak*. Een vervolgonderzoek is daarom nodig om de werkelijke omvang van de babbeltruc vast te stellen. Aangezien de groep potentiële slachtoffers als gevolg van de vergrijzing groter wordt, bestaat de inschatting dat deze trend zich niet zal keren. Een vervolgonderzoek zou ook gericht kunnen zijn op dadergroepen, omdat een verschuiving lijkt plaats te vinden van individuele daders of duo's, naar (rondtrekkende) bendes (mannen, vrouwen en zelfs kinderen) uit Oost-Europa. Naar de mening van een expert verleggen deze bendes hun aandacht van skimmen, dat steeds moeilijker wordt, naar de babbeltruc, met als doelgroep kwetsbare ouderen.

Binnen deze analyse was geen tijd om bovenstaande vragen uit te diepen. In een vervolgonderzoek naar fraudeaangiften zou de beantwoording van deze onderzoeksvragen centraal kunnen staan.

4

Hoofdvormen van fraude

In dit hoofdstuk wordt per hoofdvorm ingegaan op de onderzoeksvragen naar aard, omvang, criminele samenwerkingsverbanden, maatschappelijke gevolgen, criminaliteitsrelevante factoren, verwachtingen en aanpak.

4.1 Fraude met online handel

In paragraaf 2.1 wordt onder andere beschreven hoe een steekproef uit de aangiften is geanalyseerd. Hieruit bleek dat fraude met online handel het meest vaak voorkwam in de politiesystemen. De informatie in deze paragraaf berust op interviews met medewerkers van het Meldpunt Internetoplichting (MIO) en Marktplaats. Ook is gebruik gemaakt van cijfers uit de analyse van aangiften zoals beschreven in hoofdstuk 3, en een recent onderzoek van de Hogeschool van Leeuwarden naar daderprofielen.

4.1.1 Aard

Fraude met online handel gaat voornamelijk over het niet nakomen van leveringsverplichtingen en/of betalingsverplichtingen. Fraudeurs bieden producten aan op één van de handelsplaatsen, vragen vooruit te betalen en leveren vervolgens niet. Het gaat bij dit type fraude vaak om gadgets, zoals mobiele telefoons, navigatiesystemen en computerspelletjes, vooral producten die een trend zijn (Uggs, de nieuwe iPhone, iPad). Daarnaast kan het gaan om producten die vanuit het buitenland worden aangeboden, zoals auto's en caravans. Via internet kunnen fraudeurs producten aanbieden in een ander land dan waar ze zelf wonen, en daardoor blijven zij buiten beeld van de opsporing. Daarnaast is het mogelijk dat fraudeurs een product kopen of bestellen, aan de leverancier vragen om vooruit te leveren, maar vervolgens niet betalen. Veel van dit soort transacties worden gedaan vanuit internetcafés, waardoor een onderzoek naar IP-adressen niet zinvol is. Een variant is het niet betalen voor producten die wel zijn geleverd. Hierbij bieden fraudeurs juist (relatief) hoge bedragen voor de producten die mensen aanbieden.

Steeds vaker is sprake van *fake*-websites die Nederlanders waarschijnlijk in het buitenland hosten. Op die websites wordt consumentenelektronica aangeboden, die na betaling niet geleverd wordt. Ook worden in Nederland gehoste *fake*-websites opgezet met gebruikmaking van een *payment service provider*, zoals

iDEAL, waardoor het betrouwbaar oogt. Dit komt minder vaak voor, omdat een in Nederland gehoste website gemakkelijker is op te sporen na klachten en te sluiten dan een buitenlandse.

Bij deze vorm van fraude is sprake van het zogenaamde *many-little*-principe. Fraudeurs plaatsen aanbiedingen op online handelsplaatsen voor relatief lage bedragen, of voor bedragen die te mooi zijn om waar te zijn (zoals te goedkope iPhone's). Ze bereiken veel slachtoffers en het risico is laag. Internet biedt een uitgelezen kans om dit type fraude anoniem te plegen, waardoor fraudeurs heel lang ongestraft hun gang kunnen gaan.

4.1.2 Omvang

Uit verschillende bronnen komen cijfers voort: dat zijn cijfers van het MIO, van de Fraudehulpdesk en uit de analyse van aangiften (hoofdstuk 3).

Het MIO richt zich vanuit een proeftuin uitsluitend op fraude op Marktplaats. In de toekomst zal het initiatief, bij een positieve beoordeling, mogelijk worden uitgebreid naar andere online handelsplaatsen. Na de start in oktober 2010 kwamen 150 meldingen per dag binnen; de stand van zaken na een jaar tijd is ruim 30.000 meldingen, waarvan ruim 2300 in aangiften zijn omgezet. Daarbij waren 7600 bankrekeningnummers betrokken. Op 1082 rekeningen zijn vijf of meer stortingen gedaan, hetgeen duidt op een meer structurele uitoefening van fraude. Het grootste aantal betrof 220 stortingen op één bankrekeningnummer. Dat niet alle gedupeerden aangifte doen blijkt uit het volgende: een bankrekeningnummer waarop zestien gedupeerden hadden overgeboekt, bleek bij navraag bij de bank in werkelijkheid 123 overboekingen te hebben gekregen. De overige gedupeerden is verzocht om aangifte te doen, maar niet iedereen heeft hieraan gehoor gegeven. Of dit aangeeft dat sprake is van het topje van de ijsberg is niet te zeggen, maar het is wel een indicatie dat een deel van deze fraude onzichtbaar blijft.

De genoemde betalingen waren in Nederland gedaan, maar ook werden in totaal 240 IBAN-betalingen geconstateerd. Dat zijn betalingen naar of vanuit het buitenland: hierbij kwamen Nigeria, Groot-Brittannië en Litouwen naar voren. Vooral vanuit Groot-Brittannië bieden fraudeurs auto's tegen een schappelijke prijs aan, zonder deze te leveren. Er is geen zicht op de personen die zich daarmee bezighouden.

De gemiddelde schadebedragen bij fraude met online handel zijn niet hoog. Hierna volgt een overzicht van het aantal meldingen per instantie en de gemiddelde schadebedragen:

Bij het MIO variëren de schadebedragen per persoon van een paar tientjes tot een paar honderd euro; het gemiddelde ligt op 350 euro (uitschieters ofwel extreem lage en extreem hoge bedragen, zijn in de berekening meegenomen). Marktplaats zelf kwam op een gemiddeld schadebedrag van 125 euro.

De Fraudehelpdesk kreeg 500 meldingen over fraude op online handelsplaatsen en webwinkels, en ook van fraude op andere handelsplaatsen. In totaal betaalden 342 slachtoffers een bedrag van (afgerond) 145.000 euro. Het gemiddelde schadebedrag is 423 euro, en ook hierin zijn uitschieters meegenomen.

Uit de analyse van de steekproef in 2009 bleek dat 27 procent van de 837 aangiften over online handelsplaatsen ging (zie paragraaf 2.1). Een (grobe) doorberekening op basis van deze analyse gaf een geschatte schade van 1,7 miljoen euro. Het gemiddelde schadebedrag bedroeg 312 euro, exclusief uitschieters. Uit de recente analyse van de 30.000 aangiften bleek dat een kwart van de aangiften over online handelsplaatsen gaat, dat zijn er ruim 7300. Hierbij is sprake van dubbele registraties: de aangiften die het MIO in onderzoek neemt, worden ook in de politiesystemen geregistreerd en dat waren er in totaal 1500. De overige fraudes zijn dus via de regiokorpsen aangegeven en dit betekent dat lang niet alle melder de weg naar het MIO weten te vinden. Uit deze analyse konden geen gemiddelde schadebedragen worden berekend.

Uit bovengenoemde schadebedragen is op te maken dat het gemiddelde schadebedrag iets meer dan 300 euro bedraagt.

Recentelijk deed Van Wilsem (2011) onderzoek naar de risicofactoren voor slachtofferschap bij online aankopen. Hij becijferde dat 2,5 procent van de Nederlandse internetgebruikers per jaar slachtoffer is van fraude bij internetaankopen en komt daarmee op 300.000 slachtoffers per jaar. Bij een gemiddeld schadebedrag van gemiddeld 300 euro zou de totale schade jaarlijks 90 miljoen euro bedragen.

Een en ander moet in het licht van de totale handel op handelsplaatsen worden gezien en dan is de schade beperkt. In totaal verhandelen particulieren in Nederland jaarlijks voor ongeveer 10 miljard euro via alle handelssites en voor ruim 8 miljard aan online aankopen. Afgelopen jaar (2011) kocht vier op de tien

Nederlanders producten op een online handelsplaats, van een particulier of van een zakelijk verkoper.

Op Marktplaats alleen worden jaarlijks zo'n 110 miljoen advertenties geplaatst:

- 9.000.000 nieuwe advertenties per maand;
- 300.000 nieuwe advertenties per dag, dat zijn er meer dan drie per seconde, en op enig moment in totaal 7.000.000 advertenties op de site;
- 6.500.000 unieke bezoekers per maand;
- 1.300.000 unieke bezoekers per dag.

4.1.3 Criminele samenwerkingsverbanden

Bij deze fraudevorm zijn criminele groeperingen betrokken, maar er was ten tijde van het schrijven van dit deelrapport geen precieze informatie bekend. Een aantal daders lijkt uit de Turkse gemeenschap afkomstig te zijn en is overwegend actief vanuit Zuidoost-Nederland.

Ook kwam naar voren dat fraudeurs katvangers gebruiken (meestal twintigjarigen), aan wie wordt gevraagd hun bankrekening ter beschikking te stellen. Ze worden waarschijnlijk via chatrooms gelokt: een webshop die op naam van een katvanger in Den Haag stond, werd gesloten en de volgende dag vanuit Klazinaveen opnieuw geopend. Hieruit blijkt dat achter deze vorm van fraude soms een behoorlijke graad van organisatie schuilt. Het gaat in deze gevallen om zeer complexe zaken met veel betalingen.

Over de daders zelf is iets meer bekend door een recent onderzoek waarin e-fraudeurs werden vergeleken met klassieke fraudeurs. In totaal 400 dossiers uit een politieregio werden geanalyseerd en daar kwam het volgende beeld uit naar voren: e-fraudeurs zijn gemiddeld jonge daders, 27 jaar, waar klassieke fraudeurs 33 jaar zijn; driekwart is man, een kwart vrouw, meestal laagopgeleid en meer dan de helft heeft gemiddeld al drie antecedenten op zijn naam staan (Leukfeldt & Stol, 2011).

Toekomstig onderzoek zal meer duidelijkheid kunnen verschaffen over het type dader, en dan vooral over de vraag of het overwegend solisten zijn en/of criminele groeperingen die zich met deze vorm van fraude bezighouden. Daarnaast dringt de vraag zich op of ze voornamelijk in Nederland actief zijn, of ook vanuit andere (omringende) landen.

4.1.4 Maatschappelijke gevolgen

De geschatte financiële schade van fraude met online handel bedraagt 90 miljoen euro per jaar bij 300.000 slachtoffers. Het gaat om veel fraudeincidenten en als dat lang doorwoekert, ondermijnt dit het vertrouwen in de online handel. De gevolgen voor de individuele slachtoffers zijn waarschijnlijk gering: het gaat vaak om kleine bedragen, waarbij een aantal slachtoffers een zeker risico incalculeert (wanneer het aanbod te mooi is om waar te zijn). Een aantal slachtoffers zal zich gedupeerd voelen en terughoudender worden, of zelf een aantal preventieve maatregelen nemen, zoals niet meer vooruit betalen of een ontmoeting met de aanbieder arrangeren.

4.1.5 Criminaliteitsrelevante factoren

Een criminaliteitsrelevante factor is een maatschappelijke factor die van invloed is op criminele verschijnselen: deze factor kan criminaliteitsremmend of criminaliteitsbevorderend werken (Klerks & Kop, 2007).

Het MIO is een initiatief tot aanpak waar alle samenwerkende partijen op dit moment tevreden over zijn. Alle meldingen hebben sinds kort de vorm van een aangifte, en de drempel daartoe is aanzienlijk verlaagd. De regio's hebben met betrekking tot dit type aangifte beduidend minder capaciteit nodig en analyse leidt tot bundeling van informatie en tot daderclusters. Er is echter weinig zicht op de opvolging, dat wil zeggen op het aantal daders dat daadwerkelijk opgepakt en vervolgd wordt. Aan de regio's is gevraagd terugmelding te doen, maar dit gebeurt incidenteel. Wanneer in de toekomst blijkt dat geen accurate opvolging heeft plaatsgevonden, zal niet alleen het imago van de politie hieronder lijden, maar ook dat van Marktplaats. Een opvolging die onder de maat blijft, kan dan ook worden opgevat als een criminaliteitsbevorderende factor.

De tweede factor is meer van algemene aard en op meer fraudevormen van toepassing. Internet maakt het mogelijk dat op relatief gemakkelijke wijze en met weinig risico's gefraudeerd kan worden. Het bereik is groot en door het steeds afhandig maken van (relatief) kleine bedragen blijven fraudeurs lang buiten beeld. Door de grote aantallen slachtoffers die worden gemaakt, lopen de opbrengsten voor fraudeurs enorm op. Door deze enorme succesratio blijft het, ondanks het inmiddels wijdverspreide bewustzijn van mensen, een sterk winstgevende activiteit.

4.1.6 Verwachtingen

Internet maakt de drempel tot fraude met online handel laag. Op dit moment wordt veel aan preventie gedaan, door Marktplaats, het MIO en de Fraude-helpdesk. Het is echter wel noodzakelijk dat een aantal stelselmatig frauderende groeperingen in kaart wordt gebracht en aangepakt. Wanneer dit achterwege blijft, dan is de verwachting dat fraude met online handel niet zal afnemen.

4.1.7 Aanpak

De transacties leveren voor het MIO informatie op over e-mailadressen, telefoonnummers en bankrekeningnummers, op basis waarvan wordt getracht daderclusters te vormen. Het MIO maakt onderscheid tussen grote zaken, 25 meldingen of meer, en kleine zaken. Tijdens het tot stand brengen van dit deelrapport waren 175 zaken geselecteerd, 53 bestonden uit clusters met 25 of meer meldingen, de overige zaken bestonden uit clusters van 10 of meer meldingen. Veertig zaken werden overgedragen aan de regiokorpsen, en de meeste korpsen meldden terug dat zij de zaak zouden oppakken of al opgepakt hadden, maar over de afloop is geen informatie bekend.

Er vindt altijd een strafrechtelijk onderzoek plaats wanneer sprake is van tien meldingen of meer, en van meer dan 5000 euro schade of wanneer de verdachte minderjarig is.

Onlangs is een nieuwe preventiemaatregel ingevoerd. Op de website www.politie.nl kunnen aspirant-kopers op een online handelsplaats nagaan of rekeningnummer, e-mailadres of telefoonnummer al door andere gedupeerden is gemeld. Dit geeft een indicatie van de (on)betrouwbaarheid van de verkoper. De aspirant-koper krijgt dan na het invullen van de gegevens een advies over de voorgenomen transactie. Dit blijkt een groot succes te zijn: in twee maanden tijd hebben consumenten 248.000 keer gekeken of een verkoper betrouwbaar was. Tot slot is recentelijk de juridische mogelijkheid geschapen om altijd aangifte te doen. De tussenstap van melding naar aangifte is vervallen.

4.2 Fraude met betaalmiddelen

Fraude met betaalmiddelen houdt in dat transacties worden gedaan in naam van een ander. Dit gebeurt door het overnemen van de oorspronkelijk aan de kaarthouder uitgegeven (betaal)kaart, door het stelen van de kaartgegevens of door overname van de identiteit van een ander.

4.2.1 Aard

De meest in het oog springende vormen van fraude met betaalmiddelen zijn fraude met internetbankieren en fraude met betaalkaarten.

Fraude met internetbankieren

Met internetbankieren beheert een individu een bankrekening via het internet. Met een inlogcode en wachtwoord is het mogelijk om in te loggen op een bankrekening. Afhankelijk van de soort rekening kunnen rekeninghouders hun saldo opvragen, bij- en afschrijvingen controleren, en overboekingen en betalingen doen (nationaal en internationaal). In Nederland bankieren inmiddels zo'n elf miljoen mensen via internet. Dit trekt kwaadwillenden aan die hun aandachtsgebied steeds vaker verleggen naar het internetbankieren.

Fraude met internetbankieren gaat meestal over phishingactiviteiten¹⁶. Met het massaal versturen van misleidende e-mails proberen criminelen bankgegevens van rekeninghouders te ontfutselen, zoals TAN-codes, wachtwoorden en rekeningnummers. Zij versturen de e-mails uit naam van een bank. Als aanleiding wordt dan aangegeven dat er problemen zijn met de gegevens van het slachtoffer, bijvoorbeeld dat zijn gegevens verloren zijn gegaan, of het gaat onder het mom van fraudepreventie zodat de rekening niet onnodig geblokkeerd wordt. Via een link in de e-mail worden de slachtoffers doorgestuurd naar een website. Dit blijkt dan een namaaksite te zijn, die de door het slachtoffer ingevoerde gegevens opslaat. Vanaf dat moment heeft de fraudeur toegang tot de bankgegevens van het slachtoffer.

Fraude met internetbankieren gebeurt ook met behulp van katvangers, ook wel geldezels (money mules) genoemd die, veelal tegen betaling, hun bankrekening laten misbruiken voor criminele activiteiten. Deze katvangers sluizen (on)bewust frauduleus verkregen geld door naar criminelen. Door gebruik van zo'n 'tussenstation' is de identiteit van de crimineel moeilijker te achterhalen. Personen die hiervoor worden benaderd, zijn vaak (minderjarige) jongeren.

¹⁶ Phishing is een verzamelnaam van technieken die criminelen gebruiken om vertrouwelijke gegevens, bijvoorbeeld inlogcodes, te bemachtigen om daarmee vervolgens te frauderen. Meestal gebeurt dat via ongevraagde e-mails (spam). Ongeveer 90 procent van het e-mailverkeer in de wereld bestaat uit spam (NVB, 2011).

Fraude met betaalkaarten

Een betaalkaart is een kunststof pas waarmee betalingen kunnen worden verricht. Afhankelijk van de wijze waarop de betalingen worden afgehandeld, is sprake van:

- een elektronische portemonnee (zoals een chipknip): betalingen worden verrekend met een reeds van de bankrekening afgeschreven som geld;
- een debetkaart (pinpas): bedragen worden afgeschreven van de bankrekening bij het doen van de betaling;
- een creditcard (o.a. VISA en Mastercard): betalingen worden op een later moment (en eventueel in termijnen) verrekend.

Op veel betaalkaarten worden functies gecombineerd. Zo worden de meeste debetkaarten ook voorzien van een chipknip. Sommige passen zijn zowel elektronische portemonnee, debetkaart als creditcard.

Fraude met betaalkaarten richt zich vooralsnog op debetkaarten en creditcards. De fraude met deze betaalpassen begint ofwel met diefstal van de fysieke kaart of met het in handen krijgen van de betaalgegevens van een slachtoffer, zoals naam, rekeningnummer, pincode, vervaldatum en verificatiecode. Daarna kunnen de fraudeurs transacties doen op naam van de rechtmatige houder van de kaart. Het in handen krijgen van de persoonlijke gegevens en de wijze waarop transacties plaatsvinden, gebeurt op soortgelijke wijze als bij fraude met internetbankieren.

Een vorm van fraude met betaalkaarten die met name bij creditcards voorkomt, is de zogenaamde *card-not-presentfraude*. Ongeveer de helft van alle creditcardfraude komt voort uit deze vorm van fraude, waarbij op afstand betalingen worden gedaan, via de post, telefoon of internet. Er is geen rechtstreeks contact tussen winkelier en klant, waardoor de fysieke creditcard niet kan worden gecontroleerd. De verkopende partij, vaak een online winkel, kan in dit geval alleen afgaan op de betaalgegevens die hij ontvangt van de kopende partij. Wanneer deze betaalgegevens kloppen, staat de verkoper niets in de weg om de transactie te voltooien en de aangekochte goederen te versturen. Eventuele maatregelen om fraude te voorkomen, gaan vaak ten koste van de klantvriendelijkheid. Daardoor dreigen (online) winkels klandizie te verliezen aan concurrenten die deze maatregelen niet nemen. Vooral bij transacties met een laag bedrag zullen verkopers eerder een gecalculeerd risico nemen. Fraudeurs spelen hierop in bij de bestellingen die zij doen, vaak huishoudelijke artikelen, gadgets of ander populaire goederen met een waarde tot enkele honderden euro's. Deze goederen worden frequent besteld waardoor fraudeurs weinig

argwaan wekken. De creditcardgegevens die nodig zijn om deze vorm van fraude te plegen, worden voor een groot deel door middel van phishing verkregen. Er zijn ook gevallen bekend waarbij door middel van hacking grote aantallen creditcardgegevens worden ontvreemd uit de databanken van online winkels.

Bij een aantal andere modi operandi van fraude met betaalkaarten komen de credit- of debetkaarten fysiek in handen van fraudeurs door verlies of diefstal, komen de aangevraagde betaalkaarten niet aan bij de rechtmatige houders of betreft het valse aanvragen van betaalkaarten. Bij verlies of diefstal is de kaarthouder meestal het slachtoffer geworden van zakkenrollerij en heeft er, voordat de kaart geblokkeerd werd, al een transactie plaatsgevonden. In het geval van de niet-ontvangen kaarten worden deze onderschept in het posttraject. De meeste kaartverstrekkers verzenden hun betaalkaarten per post naar de kaarthouders. Het komt voor dat criminelen erin slagen de kaarten te bemachtigen voordat deze bij de rechtmatige houder aankomen. Bij valse aanvragen wordt er informatie verzameld door phishing of door het hacken van bestanden uit computersystemen. Deze gegevens worden gebruikt om een nieuwe (vervangende) betaalkaart aan te vragen¹⁷. De fraudeurs laten de aangevraagde creditcards meestal op een locatie bezorgen waar hoogbouw is en een centrale brievenbus, zodat zij deze uit de brievenbus kunnen 'hengelen'. In sommige gevallen komt het voor dat een medewerker van TNT in het complot zit en de opgestuurde betaalkaarten achterhoudt. Valse aanvragers maken bij deze praktijken ook misbruik van de verhuisservice, waarmee zij post kunnen laten doorsturen naar een ander adres.

Tot slot vindt fraude met betaalkaarten ook vaak plaats door middel van skimming. Nadat fraudeurs de pincode en de gegevens op de magneetstrip hebben verkregen, is het mogelijk om met behulp van een laptop, *cardreader* en een *cardwriter* blanco passen te maken. Daarmee kan geld worden opgenomen van de rekening van de originele pashouder. In de praktijk zitten er enkele dagen tot maanden tussen het kopiëren van de pinpas en het opnemen van het geld. Over het algemeen vinden opnames en betalingen in het buitenland plaats, vaak in Marokko, Mexico en de Verenigde Staten.

¹⁷ Bij valse aanvragen is er sprake van identiteitsdiefstal. Wanneer een fraudeur een vervangende creditcard aanvraagt, neemt hij een reeds bestaande identiteit over.

4.2.2 Omvang

Om zicht op de aard en omvang van de fraude in het betalingsverkeer te hebben, verzamelt en analyseert de Nederlandse Vereniging van Banken (NVB) fraudecijfers. In 2010 bedroeg de schade die de banken gezamenlijk hebben geleden, inclusief skimmen, ruim 57 miljoen euro (NVB, 2011). In 2011 is de totale schade van fraude in het betalingsverkeer gestegen naar 92 miljoen euro (NVB, 2012). Dit is een stijging van ruim 60 procent. Het grootste deel van de fraude met betaalmiddelen vond plaats door middel van internetbankieren en het skimmen van betaalpassen.

Uit onze analyse van de aangiften (hoofdstuk 3) blijkt dat fraude met betaalmiddelen na fraude met online handel het meest voorkomt. In totaal gaat het om 2011 aangiften. Deze fraudevorm is daarmee verantwoordelijk voor 19 procent van alle aangiften. De meeste aangiften hadden betrekking op internetbankieren (1181), gevolgd door skimming (544) en phishing (292)¹⁸.

Fraude met internetbankieren

Fraude met internetbankieren is in de afgelopen jaren flink toegenomen. In 2009 was de schade 1,9 miljoen euro en dit bleek in 2010 te zijn verviervoudigd tot een bedrag van 9,8 miljoen euro (NVB, 2011). In 2011 heeft deze stijging doorgezet, wat resulteerde in een schade van 35 miljoen euro (NVB, 2012).

Ook het aantal slachtoffers steeg sterk. De NVB rapporteerde 1383 incidenten met fraude in 2010, en dit was in 2011 opgelopen tot 8000 incidenten, wat een ruime verviervoudiging inhoudt. Wanneer men de cijfers van 2011 bekijkt, dan valt op dat het aantal fraude-incidenten in de tweede helft van dat jaar een stuk hoger ligt. In het eerste half jaar zijn 2.418 incidenten waargenomen en in het tweede half jaar zijn dat er 5.500. Dit verschil duidt erop dat het aantal fraude-incidenten bij internetbankieren nog steeds toeneemt.

Ondanks deze stijgingen leert een eenvoudige rekensom dat het gemiddelde schadebedrag per slachtoffer is afgenomen, namelijk van 7000 euro in 2010 naar 4.400 euro in 2011. De reden van deze daling is niet bekend.

Naast de informatie van de banken, geven de aangiften in de politiesystemen enige indicatie over de omvang. Het verschil tussen het aantal aangiften in de politiesystemen (1192) en het aantal fraude-incidenten dat de banken

¹⁸ Vanwege overlap in de aangiften tellen de aantallen niet op tot 2011.

constateren (8000) is groot. Hiervoor zijn twee redenen aan te dragen. Allereerst is de aangiftebereidheid voor het doen van aangifte bij fraude in het algemeen laag. Ten tweede wordt de schade van internetbankieren in bijna alle gevallen vergoed, waardoor motivatie voor het doen van aangifte, voor zover die er al was, ontbreekt. Het lijkt aannemelijk dat alleen aangifte wordt gedaan wanneer niet tot schadevergoeding is overgegaan. Dit is onder andere het geval wanneer mensen onzorgvuldig met betaalgegevens zijn omgesprongen door bijvoorbeeld anderen hun inloggegevens voor internetbankieren te geven. De aangiften geven dus een vertekend beeld, de cijfers van de NVB over de omvang van fraude met internetbankieren zijn nauwkeuriger. Eenzelfde redenering gaat op voor de verschillen in skimmingcijfers.

Fraude met betaalkaarten

Uit de fraudecijfers van de NVB blijkt dat deze schade bijna is verdubbeld van 19,7 miljoen euro in 2010 naar 38,9 miljoen euro in 2011 (NVB, 2012). Binnen fraude met betaalkaarten is schade ten gevolge van skimming de grootste schadepost. Bij 32.000 betaalpassen was sprake van skimming op een totaal van 25 miljoen passen die in omloop waren. De toename kan vermoedelijk worden toegeschreven aan de invoering van het nieuwe pinnen vanaf 1 januari 2012. De nieuwe chiptechnologie is namelijk minder fraudegevoelig dan de oude magneetstrip en skimmers proberen zoveel mogelijk hun slag te slaan bij winkeliers die nog gebruikmaken van de oude technologie. Overigens is de verwachting dat de oude magneetstrip pas in 2013 helemaal zal zijn verdwenen.

Naast het skimmen, leveren ook andere vormen van fraude met creditcards voor banken veel schade op. In 2010 was er sprake van een schade van 12,5 miljoen euro (NVB, 2011). In 2011 daalde dit met meer dan 40 procent naar 7,1 miljoen (NVB, 2012). Ongeveer de helft van alle creditcardfraude komt voort uit card-not-presentfraude. De grootste Nederlandse uitgever van MasterCard en Visa, International Card Services (ICS), schat de totale schade als gevolg van gestolen creditcardgegevens op tientallen miljoenen euro's per jaar. Koepelorganisatie Thuiswinkel.org komt tot eenzelfde schatting op basis van eigen onderzoek¹⁹. De schade neemt toe door de toename in online aankopen en daarmee het online betalen. Met de invoering van 3-D Secure²⁰ willen VISA en Mastercard online creditcardtransacties veiliger maken. Volgens ICS heeft dit een dempend effect gehad op deze vorm van fraude.

¹⁹ <http://www.wijnandjongen.com/cms/showpage.aspx?id=1839>

²⁰ 3-D Secure vormt een extra stap bij het plaatsen van een bestelling teneinde de veiligheid te vergroten. De creditcardhouder wordt beschermd tegen misbruik van zijn creditcardnummer door voor de betaling eerst zijn identiteit te bevestigen.

Banken lijden ook schade als gevolg van verlies of diefstal van kaarten, van kaarten die verdwijnen in het posttraject of valse aanvragen. Volgens het jaarrapport van de NVB bedraagt de gezamenlijke schade daardoor meer dan 17 miljoen euro in 2010 (NVB, 2011).

Hoewel de schade als gevolg van creditcardfraude in Nederland aanzienlijk is, is het in vergelijking met andere landen niet groot. Dit komt doordat in Nederland in tegenstelling tot andere landen veel internetaankopen met het betaalproduct iDEAL worden afgerekend. Deze betaalwijze is vooralsnog veiliger gebleken dan betalingen met credit cards. Hierbij dient te worden opgemerkt dat een internationale vergelijking van fraudegegevens wordt bemoeilijkt doordat de meeste landen over geen of onvolledige fraudestatistieken beschikken. Bovendien zijn functionaliteiten van bankpassen in een aantal landen verschillend. In het Verenigd Koninkrijk, Frankrijk en Spanje kan de bankpas ook gebruikt worden voor betalen via internet. Daardoor zijn de fraudecijfers in die landen hoger.

4.2.3 Criminele samenwerkingsverbanden

Over de criminele groepen die achter fraude met betaalmiddelen zitten, is niet veel bekend. De meeste informatie heeft betrekking op criminele samenwerkingsverbanden die zich bezighouden met skimming. Voor een overzicht van samenwerkingsverbanden wordt verwezen naar het deelrapport *Skimmen* (KLPD, Dienst IPOL, 2012c).

Fraude met betaalmiddelen gebeurt grotendeels in georganiseerd verband. Zo worden de in Nederland geskimde betaalpassen binnen korte tijd door anderen *gecashed* in het buitenland. Bij phishing en hacking is een duidelijk onderscheid tussen degenen met de technische kennis om online betaalgegevens te bemachtigen, en de uitvoerders, die online gecompromitteerde creditcardgegevens kopen om goederen of diensten aan te schaffen. Deze twee groepen treffen elkaar voor een groot deel op het internet, waar vraag en aanbod samenkomen. Doordat zij zich goed afschermen, onder meer door gebruik te maken van katvangers, en doordat zij internationaal opereren, blijft het zicht op deze groepen beperkt.

Volgens een expert opereert ongeveer tien tot twintig procent van de criminele samenwerkingsverbanden die zich bezighouden met fraude met betaalmiddelen vanuit Nederland. Het grootste deel opereert vanuit het buitenland, vooral vanuit Rusland, Litouwen en in mindere mate Roemenië.

In Nederland houden minimaal drie tot vijf criminele samenwerkingsverbanden zich bezig met het veelvuldig valselijk aanvragen van betaalkaarten. Daarbij maken zij onder andere misbruik van de verhuisservice, waarmee zij post kunnen laten doorsturen naar een ander adres. Bij een aantal incidenten was een medewerker van TNT betrokken die opgestuurde betaalkaarten achterhield. Binnen deze groepen is er een scheiding tussen de mensen die de (valse) aanvragen verzorgen en de *facilitators*, zoals een TNT-medewerker.

4.2.4 Maatschappelijke gevolgen

In 2011 was de financiële schade die de banken gezamenlijk hebben geleden als gevolg van fraude met betaalmiddelen ruim 92 miljoen euro (inclusief skimmen). In het algemeen draaien houders van (internet)rekeningen, creditcards of betaalpassen zelden op voor de schade van dit type fraude. Deze schade komt meestal voor rekening van banken of online winkels (als *acceptants* van de cards).

Ondanks de stijging van fraude met internetbankieren en betaalpassen in 2011 blijft de omvang van de schade voor banken beperkt in verhouding tot de omzetten. De omzetten waren 3,2 biljoen euro voor internetbankieren en 138 miljard euro voor gebruik van betaalpassen. De fraude bedraagt daardoor slechts 0,001 procent voor het internetbankieren en 0,03 procent voor skimming (NVB, 2012, 1 juni). Vooralsnog zien de banken dan ook geen reden hun vergoedingsbeleid aan te passen. Desalniettemin kan op lange termijn de toename van fraude met betaalmiddelen ondermijnend zijn voor het vertrouwen in het betalingsverkeer.

Geldezels vormen een uitzondering op het vergoedingsbeleid van banken. Deze katvangers, meestal jongeren die tegen een vergoeding hun rekening beschikbaar stellen, draaien wel op voor de (financiële) consequenties van de fraude. Aangezien de consequenties vaak jarenlang blijven doorwerken, wordt het voor hen moeilijk om een toekomst op te bouwen. Het totaal aantal geldezels in 2011 ligt ten minste op 5.000.

4.2.5 Criminaliteitsrelevante factoren

Het internet heeft in de afgelopen jaren een enorme invloed gehad op fraude met betaalmiddelen. De drempel om te frauderen voor zowel individuen als criminele bendes is hierdoor aanzienlijk verlaagd. In de komende jaren zal de verschuiving naar online betalen waarschijnlijk alleen maar toenemen, waardoor het aannemelijk is dat met name fraude met internetbankieren eveneens zal

blijven toenemen. Het aantal mensen dat via internet bankiert, bedraagt in 2011 rond de elf miljoen.

In de komende jaren zullen betalingen steeds minder plaatsvinden door middel van het fysiek overhandigen van geld. Dit zal positieve gevolgen hebben voor middenstanders die, omdat ze minder geld in huis hebben, minder aantrekkelijk worden voor overvallen. Online betaaldiensten worden steeds meer geïntegreerd. Betaalopdrachten worden verstuurd vanaf mobiele telefoon, tablet of de computer. Fraudeurs zullen dan ook trachten om mensen via deze verschillende kanalen te benaderen.

Factoren die deze ontwikkeling versterken, zijn de toename van persoonlijke informatie op het internet en de slechte beveiliging van veel computers.

De toenemende populariteit van het online winkelen heeft ervoor gezorgd dat op veel verschillende plekken persoonlijke gegevens van mensen zijn opgeslagen. Bovendien onderhouden mensen steeds meer virtuele contacten op zogenaamde *social media*. Dit zal in de komende jaren alleen maar toenemen. Daardoor komt meer en meer persoonlijke informatie op het internet te staan, wat mogelijkheden biedt voor fraudeurs. De gemiddelde Nederlander komt tegenwoordig voor in maar liefst 500 databases (Schermer, 2009). Er hoeft maar een van deze databases een kwetsbaarheid in de beveiliging te hebben om criminelen de gelegenheid te geven persoonlijke data te stelen. In welke mate deze criminaliteitsbevorderende factor van invloed zal zijn, is moeilijk aan te geven.

Een andere versterkende factor hangt samen met de matige beveiliging van veel pc's. Bij het vergroten van de betaalmogelijkheden naar andere apparaten, zoals tablets en smartphones zullen automatisch ook extra kwetsbaarheden ontstaan. Het is namelijk niet te verwachten dat gebruikers deze apparaten ineens beter gaan beveiligen.

Tot slot zal de economische crisis ook mogelijkheden scheppen voor fraudeurs. De verwachting is dat de werkloosheid de komende jaren sterk gaat toenemen. In november 2011 stelde het Centraal Planbureau (CPB) dat het met de werkloosheid in Nederland tijdens de vorige crisis erg was meegevallen. Nu de economische crisis waarschijnlijk nog jaren gaat duren, zullen meer mensen geraakt worden en zullen de gevolgen ernstiger zijn. De reserves die bedrijven en mensen hadden, zijn voor een groot gedeelte al aangesproken en raken wellicht op (KLPD, Dienst IPOL, 2012b). Daardoor komen in de komende jaren waarschijnlijk meer mensen in geldnood. De kans is groot dat in Nederland,

evenals in andere Europese landen, ook de jeugdwerkloosheid sterk zal toenemen²¹, waardoor het aantal jonge geldezels niet zal afnemen. Fraudeurs zullen als gevolg van deze ontwikkeling mogelijk gemakkelijker geldezels kunnen rekruteren.

4.2.6 Verwachtingen

In de afgelopen jaren is de financiële schade als gevolg van fraude met betaalmiddelen flink toegenomen. Fraude met internetbankieren vervijfvoudigde in een jaar tijd. Deze trend zal waarschijnlijk doorzetten, omdat de mogelijkheden om online te betalen steeds verder worden uitgebreid, zoals beschreven in de vorige paragraaf. Skimmen veroorzaakt al jaren de meeste schade, maar door het invoeren van betalen via een chip in plaats van een magneetstrip, wordt een daling verwacht vanaf 2012. Er is echter nog een groot aantal automaten, zoals bij onbemande tankstations, waar de magneetstrip nog steeds kan worden uitgelezen, waarna in het buitenland gecashd kan worden. De banken proberen dit voor te blijven met nieuwe maatregelen, zoals het blokkeren van passen voor gebruik buiten Europa (zie paragraaf 4.2.7). Of de daling van het aantal skimincidenten doorzet of uitblijft, laat zich daardoor moeilijk voorspellen.

Creditcardfraude is in Nederland al jaren een relatief klein probleem. Dit zal in de komende jaren waarschijnlijk niet veranderen, mede doordat iDEAL een veilig alternatief is voor online betalingen.

Tot slot is de verwachting dat het aantal katvangers dat financieel in de problemen komt, zal stijgen. Een stijging in de jeugdwerkloosheid als gevolg van de economische crisis, zoals beschreven in de vorige paragraaf, geeft fraudeurs waarschijnlijk meer mogelijkheden om jonge geldezels te rekruteren. Daardoor kunnen zij de komende jaren frequenter misbruik maken van (internet) rekeningen en pinpassen van kwetsbare individuen. Deze personen draaien zelf op voor de financiële gevolgen, met als gevolg dat een grote groep van vooral jongeren langdurig in de (financiële) problemen kan komen.

²¹ Zie o.a.: Elsevier (2012) en Standaard (2012).

4.2.7 Aanpak

Fraude met internetbankieren

Naast de strenge beveiligingsmaatregelen die banken nemen en hun voortdurende monitoring is het ook belangrijk dat klanten zelf maatregelen nemen om te voorkomen dat anderen toegang krijgen tot hun bankrekening. Maatregelen die gericht zijn op preventie vormen daarom een belangrijk deel van de aanpak. Campagnes die in dit verband zijn gestart, zijn onder andere *Veilig bankieren* en *pasopjepas*. De campagne *Veilig bankieren* is in 2010 gelanceerd door de NVB om misbruik van internetbankieren tegen te gaan²². Via deze campagne worden klanten onder meer geïnformeerd over het fenomeen phishing (*geef nooit inlog- en/of betaalkodes af*) en worden adviezen gegeven hoe de kans te verkleinen dat computers worden besmet met malware. De campagne *pasopjepas*²³ richt zich vooral op jongeren die hun betaalpas uitlenen aan criminelen.

Om fraude met internetbankieren terug te dringen hebben het KLPD, het Landelijk Parket en de NVB in maart 2011 gezamenlijk de *Electronic Crime Taskforce* (ECTF) opgericht. In dit 'bankenteam' waarin experts vanuit de banken en het KLPD zijn gedetacheerd, wordt door middel van analyses en versterking van de informatiepositie de aanpak van cybercrime geïntensiveerd. De ECTF is een initiatief van het KLPD en is voorlopig voor één jaar van start gegaan. In het buitenland blijken dergelijke bankenteams succesvol, of deze aanpak in Nederland ook succesvol is, zal nog moeten blijken.

Fraude met betaalkaarten

De NVB heeft zich de afgelopen twee jaar intensief ingezet voor meer prioriteit voor opsporing en vervolging van skimming. Uiteindelijk heeft dit geresulteerd in de toezegging van politie en het Openbaar Ministerie om een gezamenlijk *skimmingpoint* in te richten met als doel de stijgende trend te doorbreken.

De intensieve samenwerking bestaat onder andere uit het (internationaal) uitwisselen en analyseren van informatie, waardoor criminele netwerken eerder kunnen opgespoord en vervolgd. Het *skimmingpoint* houdt zich ook bezig met kennisontwikkeling en –deling, onderzoek naar het opwerpen van barrières om skimming tegen te gaan, samenwerking in de strafrechtketen en

²² Veilig Bankieren (www.veiligbankieren.nl) is een vervolg op de campagne *Drie keer kloppen*.

²³ <http://www.pasopjepas.nl/index.php?p=1>

versterking van de repressieve aanpak. Skimmen wordt daardoor een stuk minder aantrekkelijk gemaakt (Dienst Regionale Informatie, 2011).

Hoewel de gedupeerden in beginsel schadeloos worden gesteld, schaadt skimming het vertrouwen in het elektronisch betalen. Skimming is daarmee niet alleen een bancaire probleem, maar ook een maatschappelijk probleem. Dit was een belangrijke overweging om van de magneetstrip over te gaan op de veiliger EMV-chiptechnologie²⁴. Omdat de EMV-chip beter te beveiligen is dan de magneetstrip worden wereldwijd alle bankpassen en creditcards voorzien van deze chip. In Nederland is die aanpassing in 2005 gestart en sinds 1 januari 2012 zijn alle bankpassen en creditcards voorzien van de chip.

Nieuw beleid van banken zal skimmen in de toekomst bemoeilijken. Sinds 1 juni 2012 blokkeert de Rabobank standaard betaalpassen van particuliere klanten voor gebruik buiten Europa. Skimmers nemen doorgaans geld op bij geldautomaten buiten Europa, hetgeen door dit beleid wordt voorkomen²⁵. Volgens de Rabobank is de maatregel in het buitenland succesvol gebleken en heeft deze geleid tot een sterke daling van het aantal fraudegevallen. De andere banken gaan in de toekomst waarschijnlijk dezelfde maatregelen nemen (NOS, 2012)

Creditcard

De invoering van 3D-Secure heeft als doel om (online) creditcardfraude tegen te gaan door de creditcardhouder voor de betaling eerst, via een extra stap, zijn identiteit te laten bevestigen. Daarmee pogen VISA en Mastercard online card-not-presenttransacties veiliger te maken. Vanaf begin 2010 zijn alle creditcards voorzien van de 3D-Secure code. De implementatie hiervan verschilt echter per bank, variërend van een statisch (altijd hetzelfde) eigen gekozen wachtwoord, een pincode tot het gebruik van bankeigenmiddelen zoals de calculator. Het veiligheidsniveau van dit laatste middel is vanzelfsprekend hoger dan een eigen wachtwoord.

²⁴ De letters "EMV" staan voor Europay, Mastercard en Visa, de drie betaalkaartsystemen.

²⁵ Overigens kunnen klanten van de Rabobank de blokkade zelf opheffen en de pinmogelijkheid per werelddeel tijdelijk aanzetten als ze daarvoor kiezen.

4.3 Voorschotfraude

Informatie in deze paragraaf is afkomstig uit interviews met experts van de politie en uit rapporten van de Fraudehelpdesk en van Onderzoeksbureau Ultrascan. Daarnaast zijn gegevens gebruikt uit *Gouden Bergen* (Schoenmakers, De Vries Robbé & Van Wijk, 2009), van de Quickscan Nigerianen (KLPD, Dienst IPOL, 2009), en ook uit het vorige dreigingsbeeld (KLPD, Dienst IPOL, 2008b).

4.3.1 Aard

Voorschotfraude vond al plaats in de 16e eeuw. In de loop van de tijd zijn er talloze varianten verzonnen, maar het uitgangspunt blijft in principe hetzelfde: voorschotfraude omvat allerlei vormen van oplichting waarbij het slachtoffer onder valse voorwendselen wordt verzocht voorschotten te betalen, met een veel grotere beloning in het vooruitzicht. De voorschotten kunnen onkosten zijn – zoals belasting, smeergeld, notariskosten en bemiddelingskosten – die nodig zijn om de beloofde deal te voltooien. Slachtoffers komen er na één of vele betalingen, achter dat de beloofde geldsommen, goederen, of diensten niet worden geleverd. Op dat moment hebben zij (opgeteld) vaak al grote bedragen overgemaakt. Soms wel tienduizenden tot honderdduizenden euro's, dollars of andere valuta.

In de laatste decennia hebben vooral Nigeriaanse fraudeurs deze fraudevorm geperfectioneerd. Het massaal benaderen van potentiële slachtoffers ontstond voor het eerst in de jaren tachtig in Nigeria. De Nigerianen verstuurden wereldwijd brieven, gebruikmakend van hun voertaal Engels, waarin hulp werd gevraagd voor het wegsluizen van een grote som corrupt geld uit een oliecontract. Toen dit een groot succes bleek, slachtoffers betaalden heel gemakkelijk, werd dezelfde werkwijze herhaald maar met andere methoden en een andere inhoud. De methode veranderde van brieven, telefoon of fax, naar e-mail en internet (datingsites, chatrooms, veilingssites, online handelsplaatsen, zoals Marktplaats, eBay). Is er eenmaal contact dan wordt het meestal voortgezet via de telefoon of andere social media. Slachtoffers worden bewogen hun betalingen te blijven doen en betalen veelal via moneytransferagentschappen, die in sommige gevallen door criminele organisaties worden beheerd. Vooral door het gebruik van het digitale verkeer is de fraude grenzeloos geworden en kan de inhoud eenvoudig aan een bepaalde doelgroep worden aangepast.

Om reden dat dit soort praktijken ooit vanuit Nigeria begon, wordt het ook wel 419-fraude genoemd, verwijzend naar het betreffende artikel in het Nigeriaanse wetboek van strafrecht. Internationaal worden naast 419-fraude ook andere

termen gebruikt, zoals *advance fee fraud* of *Nigerian Scam*; in de Verenigde Staten, in Groot-Brittannië en Canada wordt het *mass marketing fraud* genoemd en in Australië hanteert men de term *consumer fraud*. In dit deelrapport hanteren we de term voorschotfraude, omdat dit de lading beter dekt en inmiddels ook niet-Nigerianen zich aan deze vorm van fraude bezondigen. Het massaal benaderen van slachtoffers, vindt ook bij andere vormen van fraude plaats. In hoofdstuk vijf gaan we hier nader op in.

Voorschotfraude heeft een aantal verschijningsvormen. De meest in het oog springende zijn:

- *Erfenisfraude*: een stervende rijkard wil zijn erfenis niet aan zijn familie of de staat nalaten, of heeft geen familie. De geadresseerde van de mailing zou een ver familielid zijn, die de erfenis kan ontvangen, mits hij allerlei (oplopende) onkosten vergoedt.
- *Loterijfraude*: er worden twee vormen van loterijfraude onderscheiden. Bij de ene vorm worden potentiële slachtoffers massaal via de e-mail benaderd met de boodschap dat ze een grote prijs in een loterij of in een promotiecampagne van een groot bedrijf hebben gewonnen. Om de prijs in ontvangst te mogen nemen, dient de geadresseerde eerst een (steeds meer oplopend) bedrag over te maken. Deze vorm wordt grotendeels door Nigerianen uitgeoefend en er worden aanzienlijk hogere bedragen betaald dan bij de tweede vorm, loterijfraude en 'sweepstakes'²⁶ via postbussen. Bij deze vorm worden slachtoffers massaal benaderd door 'bulkmail', dat via de post wordt toegezonden. Slachtoffers sturen vervolgens geld naar postbussen.
- *Dating- of relatiefraude*: fraudeurs scannen allerlei websites af op geschikte advertenties en leggen dan contact. De fraudeur doet zich voor als 'de liefde van iemands leven', bouwt een vertrouwensband op, en vraagt na verloop van tijd om geld te mogen 'lenen'. Een reden die hierbij bijvoorbeeld wordt aangedragen is de aankoop van een vliegticket voor de behandeling van een zieke moeder.

²⁶ Sweepstakes zijn acties waarbij unieke nummers worden toegezonden aan potentiële winnaars die vervolgens geretourneerd moeten worden, zodat de adverteerder kan verifiëren of het nummer winnend is.

- *Veiling- of verkoopfraude*: de fraudeur brengt een erg hoog bod uit op een product dat te koop wordt aangeboden (vaak op eBay of een andere online handelsplaats) en betaalt met een te hoge valse cheque. Het slachtoffer wordt gevraagd het verschil 'terug' over te maken, of door te sturen naar een 'verscheppingsbedrijf' waar de dader aan gelieerd is.
- *Recovery fraud*²⁷: slachtoffers worden benaderd om het bedrag dat ze door eerdere fraude verloren hebben, terug te krijgen. Hierbij doen oplichters alsof ze van de politie zijn of van een stichting, die de belangen behartigt, en eventueel (juridische) actie kan ondernemen tegen de daders. Om het geld terug te vorderen is eerst een 'contributie' vereist.
- *Employment fraud*: er wordt een lucratieve baan aangeboden, maar daarvoor moet wel inschrijfgeld betaald worden.

Bovenstaande verschijningsvormen worden heel gemakkelijk aangepast aan actuele situaties. Zo werden de tsunami aan de kust van Sumatra en de aardbeving in Haïti ook ingezet voor frauduleuze doeleinden.

De laatste jaren lijken vooral dating- en loterijfraude sterk in opkomst. Daarnaast is een toename waar te nemen van Nederlandse slachtoffers die vanuit het buitenland worden benaderd, met name vanuit Groot-Brittannië, Spanje, Maleisië, West-Afrika en Zuid-Afrika. Door de gebrekkige registratie van voorschotfraude is het echter lastig om deze ontwikkelingen concreet te bevestigen.

4.3.2 Omvang

In het Nationaal dreigingsbeeld 2008 (KLPD, Dienst IPOL, 2008a) zijn voorschotfraude en beleggingsfraude gekwalificeerd als dreiging:

“De omvang van de fraudeconstructie Fata Morgana is moeilijk vast te stellen. Wel is duidelijk dat de financiële schade van voorschot- en beleggingsfraude omvangrijk is, zelfs als we ons baseren op schattingen die als ondergrens moeten worden beschouwd. Daarbij komen dan nog gevolgen van niet-financiële aard, vooral psychische schade voor slachtoffers. De vooruitzichten voor de komende vier jaar zijn niet hoopgevend. Oplichters zijn flexibel en vinden telkens nieuwe invullingen van dezelfde fraudeconstructie. Toezicht kan

²⁷ *Recovery Fraud* komt ook voor bij beleggingsfraude en is omschreven in paragraaf 4.9.1.

eenvoudig worden ontdoken. De fraudeconstructie Fata Morgana wordt daarom gekwalificeerd als dreiging voor de Nederlandse samenleving".

Ook werd geschreven dat "het maken van een betrouwbare schatting van de omvang van fraudeconstructies niet mogelijk is, omdat fraudeconstructies zijn opgebouwd uit verschillende onderliggende fraudevormen. Schattingen over de omvang van deze fraudevormen zijn om diverse redenen moeilijk te maken. Onder meer registratie-effecten, dark-numbers en definitieverschillen zijn van invloed op de geregistreerde omvang van fraude".

In deze situatie is weinig veranderd. Betrouwbare cijfers over voorschotfraude lijken nog steeds niet te bestaan. Dat geldt voor de meeste landen, waar de registratie- en definitieproblematiek vergelijkbaar is met die in Nederland. Wanneer cijfers worden genoemd (niet alleen bij voorschotfraude), worden deze meestal als het topje van de ijsberg omschreven. In deze paragraaf maken we gebruik van informatie uit het project Apollo, uit meldingen en aangiften die door de jaren heen zijn gedaan bij de politie, en in het laatste jaar bij de Fraudehelpdesk. Daarnaast maken we gebruik van informatie uit een Engels onderzoek naar loterijfraude. Deze informatie is door een expert verstrekt.

Het aantal meldingen bij de Nederlandse politie met betrekking tot fraude gepleegd door in Nederland verblijvende Nigerianen liep tussen 1998 en 2007 gestaag op tot ongeveer 400 per jaar. Het ging hier om meldingen van buitenlandse slachtoffers die door in Nederland verblijvende Nigeriaanse criminele groeperingen werden opgelicht. De slachtoffers die betrekking hadden op deze 400 meldingen betaalden in totaal ongeveer 15 miljoen euro (gemiddeld 37.500 euro).

Op basis van deze meldingen werden de projecten Apollo (*hit-and-run*) en Dutch Treat (diepgaand met uitlevering van verdachten aan de VS) gestart. In het kader van deze projecten werd een centraal meldpunt voor de aangiften van de buitenlandse slachtoffers ingericht en werden de geldstromen via de bankrekeningen en moneytransfers onderzocht en geblokkeerd. Er werden circa 150 verdachten aangehouden, waaronder een aantal kopstukken van organisaties, die werden uitgeleverd aan de Verenigde Staten. Door het beeld van de geldstromen en de in beslag genomen administraties van de verdachten kon worden vastgesteld dat het om 150 tot 200 miljoen euro per jaar ging en om 2.536 slachtoffers. De Bovenregionale Recherche (BR) schatte dat ten tijde van deze projecten slechts vijf tot tien procent van de buitenlandse slachtoffers aangifte deed.

Het aantal meldingen is inmiddels gedaald naar ongeveer 40 per jaar. Deze 40 buitenlandse meldingen kwamen binnen de Dienst IPOL en gingen voornamelijk over erfenis-, loterij- en datingfraude. Daarnaast zijn meldingen gedaan bij de regiokorpsen waardoor het aantal hoger ligt, maar het zicht hierop ontbreekt. De schade die wordt betaald door buitenlandse slachtoffers aan in Nederland verblijvende (West-Afrikaanse) criminele groeperingen wordt echter nog altijd geschat op 50 miljoen per jaar. Dit lijkt om een aantal redenen een hoge schatting. Het schadebedrag zou op basis van die 40 meldingen en een gelijkblijvend gemiddeld schadebedrag (37.500 euro) ongeveer 1,5 miljoen per jaar zijn. Wanneer we ervan uitgaan dat slechts een tiende van de slachtoffers zich meldt, zou dit leiden tot een geschatte omvang van 15 miljoen euro per jaar. Het geringe aantal meldingen kan het gevolg zijn van de acties van de projecten Apollo en Dutch Treat, waardoor het aantal in Nederland verblijvende criminele groeperingen daalde. Op wereldwijde schaal stond Nederland in het jaar 2008 nog in de top 3, anno 2011 komt Nederland niet meer voor in de top 20 van daderlanden die veel buitenlandse slachtoffers maken. Daarnaast wordt niet actief meer gerechercheerd op geldstromen, en ontbreekt een centraal meldpunt voor buitenlandse slachtoffers.

De analyse van aangiften van Nederlandse slachtoffers (hoofdstuk 3) laat zien dat voorschotfraude na een aanvankelijke daling recent weer toeneemt: het was 9,7 procent in 2007, dit daalde in 2010 naar 4,2 procent maar steeg in het referentiejaar weer naar 5,7 (periode 1 september 2010-31 augustus 2011). In totaal is in de onderzoeksperiode 604 keer aangifte gedaan van voorschotfraude. Het neemt daarmee een derde plaats in, in het totaal van de geanalyseerde aangiften. In 100 van de 604 gevallen was sprake van erfenisfraude; in 53 gevallen betrof het datingfraude; tot slot ging het bij 29 aangiften om loterijfraude. Binnen het tijdsbestek van dit rapport was het niet mogelijk om de totale schade vast te stellen. Daarom hebben we een kleine inventarisatie gedaan en zagen dat bij ieder van zes aangiften met betrekking tot erfenis-, dating- of loterijfraude²⁸ rond de 10.000 euro aan fraudeurs is overgemaakt. Op basis van de aangiften hadden Nederlandse slachtoffers in het referentiejaar ongeveer 6 miljoen euro geregistreerde schade. Een expert schat het *dark number* op 90 procent, en veronderstelt dan dat de schade voor Nederlandse slachtoffers ongeveer 60 miljoen euro moet bedragen. Nader onderzoek naar alle aangiften zou hier uitsluitsel over moeten geven.

²⁸ Gezien de hoogte van de betaalde bedragen, veronderstellen wij dat het hier de tweede vorm van loterijfraude betreft.

Wij tekenen hierbij aan dat een gemiddeld schadebedrag van 10.000 euro aan de lage kant is, omdat tijdens het project Apollo bleek dat de gemiddelde gemelde schade ongeveer 15.000 euro bedroeg. Ook de gemiddelde schade die bij de Fraudehelpdesk wordt gemeld over voorschotfraude ligt hoger, namelijk 42.000 euro. Tot slot was het genoemde *dark number* van 90 procent of meer gebaseerd op een controle van moneytransfers, die in het derde kwartaal van 2011 richting Maleisië gingen. Er werd vastgesteld dat 40 personen aan het slachtofferprofiel voldeden, terwijl slechts twee van hen melding van de fraude hadden gedaan. Later meldden zich nog twee personen van de eerder geselecteerde 40 personen als slachtoffer. Dit is ook de ervaring bij andere projecten rond fraude, zoals bij het MIO (Meldpunt Internetoplichting): een bankrekeningnummer waarop zestien gedupeerden hadden overgeboekt, bleek bij navraag bij de bank in werkelijkheid 123 overboekingen te hebben gekregen. De overige 107 gedupeerden deden, nadat zij op de fraude waren gewezen, mondjesmaat aangifte.

De Fraudehelpdesk kreeg in een periode van tien maanden ruim 550 meldingen over verschillende vormen van voorschotfraude, waarbij in concreto 76 slachtoffers ruim 3,2 miljoen euro overmaakten naar fraudeurs (gemiddeld 42.000 euro per persoon). Hierbij tekenen wij aan dat de Fraudehelpdesk een andere indeling hanteert ten aanzien van voorschotfraude dan in dit deelrapport, waardoor een goede vergelijking niet mogelijk is. Voor de schatting van de financiële omvang van Nederlandse slachtoffers is in dit deelrapport uitgegaan van het aantal van 604 aangiften in de politiesystemen. Daarbij is waarschijnlijk wel sprake van overlap, omdat de Fraudehelpdesk in veel gevallen de slachtoffers naar de politie doorverwijst. De mate van overlap tussen beide registraties is niet bekend.

De financiële schade voor buitenlandse slachtoffers van de zogenaamde tweede vorm van loterijfraude, waarbij het geld naar postbussen in Nederland wordt gestuurd, wordt geschat op 150 miljoen euro. Deze schade is gebaseerd op gegevens uit onderzoek in Groot-Brittannië en een onderzoek van de FIOD-ECD. In Groot-Brittannië werd de post opgevangen van slachtoffers van een zogenaamde *suckerlist* en deze konden worden herleid tot 300 postbussen in Nederland, die in gebruik waren voor deze vorm van fraude. Zowel uit onderzoek in Groot-Brittannië naar acht postbussen als uit onderzoek van de FIOD-ECD in Nederland naar vier postbussen is gebleken dat per postbus ongeveer 500.000 euro per jaar wordt ontvangen. Of de schatting van de financiële schade, die hierop gebaseerd is, aan de hoge kant is of niet, is nauwelijks te zeggen. Uit de volgende voorbeelden blijkt wel dat het om veel postbussen gaat, waarin aanzienlijke bedragen omgaan. Sinds 2004 is vanuit

het buitenland (Canada, Groot-Brittannië) verschillende keren melding gemaakt van het gebruik van Nederlandse postbussen op verschillende plaatsen in het land, en hierbij ging het afgerond om 160 postbussen. In Groot-Brittannië werden acht postbussen over een periode van tien jaar onderzocht, waarbij 118 miljoen pond aan frauduleus geld werd getraceerd. Dat is gemiddeld 1,5 miljoen pond per postbus per jaar. Ook de Nederlandse douane meldde dat wekelijks 20.000 euro uit postbussen in beslag werd genomen.

De door de individuele slachtoffers betaalde bedragen zijn relatief laag (50 tot 150 euro), maar de hoeveelheid slachtoffers is zo massaal dat het uiteindelijk zeer winstgevend blijkt. Door de gehanteerde *suckerlists* is er vaak sprake van herhaald slachtofferschap, vooral onder ouderen. De Britse politie heeft vastgesteld dat sommige slachtoffers wel 80 tot 100 frauduleuze brieven per week ontvangen. Tijdens het onderzoek van de FIOD werden deze getallen bevestigd door verschillende betrokkenen die werkzaam zijn bij bedrijven die faciliteren bij het beheer van die postbussen. Volgens het Britse onderzoek is de omzet van één postbedrijf (*Spring Global*) voor deze frauduleuze bulkmail ongeveer 10 miljoen pond.

Samengevat bedraagt de geschatte omvang van de schade ongeveer 50 miljoen euro voor buitenlandse slachtoffers die door in Nederland verblijvende criminele samenwerkingsverbanden worden opgelicht. De omvang van de schade voor Nederlandse slachtoffers die opgelicht worden door, met name in het buitenland verblijvende criminele groeperingen, bedraagt ongeveer 60 miljoen euro. De geschatte schade voor buitenlandse slachtoffers van de tweede vorm van loterij-fraude waarbij Nederlandse postbussen en in Nederland verblijvende faciliteerders zijn betrokken, bedraagt ongeveer 150 miljoen euro.

Dat het in alle gevallen om aanzienlijke bedragen gaat, staat niet ter discussie. Echter door het ontbreken van een goede registratie en een adequate aanpak in de afgelopen jaren, waardoor de bedragen op basis van de aangiften veel lager zijn, is het lastig om op basis van deze schattingen uitspraken te doen. Gezien de hoge bedragen en de emotionele schade die slachtoffers veelal lijden, is het echter van groot belang om meer zicht te krijgen op de omvang van voor-schotfraude. Tot dat moment lijken de geschatte bedragen de beste indicatie voor de omvang van de financiële schade.

4.3.3 Criminele samenwerkingsverbanden

Nederland staat op de achtste plaats in de top 25 van daderlanden. In 2009 waren 32 groeperingen actief, dat wil zeggen dat zij vanuit Nederland

slachtoffers in andere landen benaderen. Na een aanvankelijke daling in 2007 en 2008 lijkt er weer een stijging plaats te vinden. Tussen januari 2011 en augustus 2011 worden 38 groeperingen waargenomen. Daders in Nederland richten zich vooral op de Verenigde Staten, Canada, Italië, Australië en het Verenigd Koninkrijk. Hoewel de daders zich naar andere landen verplaatsen, wordt het overgrote deel van de fraude, wereldwijd, nog steeds uitgevoerd door Nigerianen. Zo wordt loterijfraude voor 95 procent door Nigerianen uitgevoerd (Ultrascan, 2010). In het algemeen richten criminele groeperingen die in Nederland verblijven zich vooral op slachtoffers in het buitenland. Nederlandse burgers zijn echter vaak slachtoffer van in het buitenland opererende oplichters.

Nigerianen werken vaak samen in (goed georganiseerde) voor de gelegenheid ontstane cellen, in wisselende samenstelling en rollen. De structuur is flexibel, ze verplaatsen zich gemakkelijk (KLPD, Dienst IPOL, 2009) en maken gebruik van valse identiteiten en katvangers (Schoenmakers et al., 2009; Ultrascan, 2010), en soms werken ze samen met andere etniciteiten, wanneer deze over specifieke expertise beschikken. Ze houden zich ook bezig met allerlei andere vormen van criminaliteit, zoals cocaïnehandel, waarbij ze gebruik maken van Colombiaanse expertise, en waarbij Nederland een transitrol heeft. Ook in mensenhandel en mensensmokkel spelen Nigerianen een prominente rol. Tot slot zijn ze betrokken bij het grootschalig witwassen van geld waarbij ze misbruik maken van bankrekeningen, moneytransfers en ondergronds bankieren.

Al enige tijd lijken veranderingen in de omvang van de criminele samenwerkingsverbanden plaats te vinden. Zo worden Nigeriaanse groeperingen kleiner, was de grootte voorheen tussen de vijf en acht personen, nu is dat minder dan vijf. Dit lijkt ingegeven te zijn door het feit dat men steeds ervarener wordt en zo min mogelijk met anderen wil delen. Deze groeperingen komen regelmatig voor korte tijd (drie tot negen maanden) vanuit Groot-Brittannië, België, Duitsland en Frankrijk naar Nederland om zich met specialisaties bezig te houden (dienstverlening rond witwassen en ondergronds bankieren). Ook kan het gaan om gespecialiseerde afsplitsingen van grotere samenwerkingsverbanden, die voor zichzelf beginnen.

Ook vindt vaker samenwerking met criminele samenwerkingsverbanden van een andere oorsprong plaats, zoals met Roemenen (voor het witwassen van geld) en Somaliërs. Er zijn aanwijzingen dat Nigerianen onder meer in eigen land wapens leveren voor terroristische aanslagen.

Dinsdag 22 november 2011 deed Bureau Financieel Economische Recherche (BFER) van de regiopolitie Amsterdam-Amstelland een inval bij een bedrijf en vijf woningen in Zuidoost, Osdorp en Utrecht. Drie mannen die verdacht worden zich schuldig te hebben gemaakt aan het witwassen van geld zijn aangehouden. Een vierde persoon is aangehouden voor overtreding van de Opiumwet. Tijdens de doorzoeken zijn ook drie vreemdelingen aangehouden. Zij zijn aangehouden en overgedragen aan de vreemdelingendienst.

Het fraudegeld is vermoedelijk verkregen door middel van de zogenoemde 419-fraude. Deze vorm van fraude wordt veelal gepleegd door West-Afrikanen, en is vernoemd naar een Nigeriaans wetsartikel. "De 419-fraude komt veelvuldig voor," zegt de projectleider van BFER van het korps Amsterdam-Amstelland. "Slachtoffers worden over het algemeen via e-mail benaderd. De ene keer omdat ze een loterij zouden hebben gewonnen, de andere keer omdat iemand ze veel geld nagelaten zou hebben. In alle gevallen moet de 'gelukkige' persoon om het bedrag te bemachtigen eerst een onkostenvergoeding betalen." De onkostentruc wordt herhaald tot het slachtoffer afhaakt, waarna de oplichters spoorloos verdwijnen. Op deze manier worden miljoenen euro's verkregen. Langedijk: "Een van de slachtoffers in deze zaak is voor 1,2 miljoen euro opgelicht."

Het illegaal verkregen geld wilden de West-Afrikanen naar hun land van herkomst sluisen. Overmaken via de bank, of meenemen met het vliegtuig zou mogelijk zorgen voor achterdocht, daarom is vermoedelijk een andere manier bedacht. Van het geld werden in Nederland voertuigen gekocht. Die voertuigen werden verscheept naar Nigeria, en daar ter plaatse betaald waardoor het geld elders ter beschikking komt van de verdachten.

Bron: website korps Amsterdam-Amstelland

In het deelrapport *De Staatsruif en de Fata Morgana* over fraudeconstructies (KLPD IPOL, 2008b) is de verwachting uitgesproken dat West-Afrikaanse daders, na het stopzetten van het project Apollo, weer in toenemende mate in Nederland zullen neerstrijken. De hiervoor genoemde cijfers lijken dit te bevestigen. In 2010 verzocht het Openbaar Ministerie de Dienst IPOL een kort overzicht te maken van de problematiek (KLPD, Dienst IPOL, 2009). Dit betrof niet alleen een overzicht van de voorschotfraude, maar van alle vormen van criminaliteit waarmee in Nederland gevestigde Nigerianen zich bezighouden. In dit rapport wordt bevestigd dat al enige tijd een groep criminelen gevestigd is in

Amsterdam-Zuidoost, dit heeft de aandacht van de regio Amsterdam-Amstelland. Ze lijken zich echter weer te verspreiden over Nederland, in Den Haag werden bijvoorbeeld meer fraudemutaties geregistreerd tussen 2008 en 2010. De daling die inzette door de aanpak van het project Apollo lijkt daarmee te zijn gekeerd.

Met betrekking tot loterijfraude met postbussen (tweede vorm) is bekend dat dit wereldwijd wordt gepleegd door ongeveer vijf grote criminele organisaties. Twee jaar geleden kwam een MOT-melding over een Colombiaan die geld stortte naar het buitenland. De FIOD-ECD startte een onderzoek en traceerde vier postbussen in Nederland op naam van deze organisatie (die grotendeels uit Colombianen en Colombiaanse Amerikanen bestond). Het gaat hier om een grote organisatie, waarvan de leden eerst werkten vanuit Nederland en de Verenigde Staten, maar later hebben ze hun activiteiten naar Spanje verlegd. Zoals vaker te zien, zijn deze organisaties zeer mobiel. Hun werkwijze is als volgt: groeperingen in de VS ontwikkelen de loterijvormen. Legale bedrijven in Las Vegas printen en mailen een en ander, en ontvangen adreslijsten (*leads*). Potentiële slachtoffers worden gevraagd een antwoordstrook in te vullen en een relatief klein bedrag te betalen, voordat ze een prijs ontvangen. De betaling gebeurt via creditcards, cheques of met contant geld dat in retourenveloppen naar één van de postbussen moet worden gestuurd. De winst wordt ontvangen in Nederland en dan naar allerlei landen overgemaakt. Nederland is wereldwijd koploper in aantal misbruikte postbussen. Het is niet duidelijk waarom dat het geval is (waarschijnlijk door de lage pakkans en strafmaat).

Slachtoffers wonen vooral in Engelssprekende landen: de VS, Australië, Canada, Israël en Europa, of Midden- en Zuid-Amerika, en ook in Japan. Het merendeel van de leden van de criminele organisaties, die gebruik maken van Nederlandse postbussen, is afkomstig uit de VS, Zuid-Afrika en Canada. Het ontvangen van de retourenveloppen met *leads* en cash geld, en het doorsturen van het geld met creditcardbetalingen gebeurt grootschalig via het misbruiken van postbussen in Nederland. De rol van Nederland hierbij is niet alleen dat er postbussen geëxploiteerd worden, maar ook dat faciliteerders in Nederland betrokken zijn bij het leeghalen van de postbussen, en geld en andere formulieren doorsturen naar hun 'collega's' in het buitenland. Zij maken deel uit van internationale criminele groeperingen, wat de opsporing aanzienlijk bemoeilijkt. Nederlandse slachtoffers worden vooral benaderd vanuit de VS, Australië of Oost-Europa en betalen naar postbussen in die landen.

Loterij- en datingfraude zijn in opkomst, zoals blijkt uit de meldingen die bij de Fraudehelpdesk binnenkomen (paragraaf 2.6). Niet alleen Nigerianen, maar ook

Russen houden zich bezig met datingfraude, en er blijkt een toename te zijn in het aantal Ghanezen en Maleisiërs dat zich ermee bezighoudt. In deze meldingen valt op dat sommige vrouwen, die al slachtoffer zijn van een dating, ook worden misbruikt om kleding die met valse creditcards is besteld op te halen bij webwinkels.

4.3.4 Maatschappelijke gevolgen

De totale financiële schade voor voorschotfraude wordt geschat op 260 miljoen euro per jaar. De voorschotfraudes met de grootste aantallen meldingen en aangiften, erfenis-, dating- en loterijfraude, kosten de slachtoffers gemiddeld het meeste geld en geven ook het meeste leed. Er zijn gevallen bekend waarin individuele slachtoffers honderdduizenden euro's zijn kwijtgeraakt. Ook worden personen herhaaldelijk slachtoffer van verschillende vormen van fraude. De fraudeurs hanteren zogenoemde *suckerlists*, dat wil zeggen dat ze lijsten bijhouden van slachtoffers en deze tegen betaling uitwisselen. Bovendien komt het regelmatig voor dat slachtoffers weigeren te geloven dat ze worden opgelicht, zelfs als ze worden ingelicht door de politie (Schoenmakers, et al., 2009).

De laatste jaren is er, ook vanuit de politiek, toenemende aandacht voor slachtoffers. Ook wordt onderzoek gedaan naar de vraag waarom slachtoffers erin trappen, en als ze erin getrap zijn, heel lang doorgaan met betalen en niet willen of kunnen inzien dat ze opgelicht worden. Inmiddels zijn verschillende onderzoeken uitgevoerd en is zo langzamerhand een beeld ontstaan van de slachtoffers, maar ook van de psychologische en intimiderende tactieken die de daders hanteren. De fraudeurs maken gebruik van verschillende vormen van beïnvloedingstechnieken. Pak en Shadel (2007) onderscheiden er dertien die worden gebruikt afhankelijk van het type fraude en het stadium van de 'verkoop'. Veel van de door fraudeurs gehanteerde tactieken lijken op de technieken die commerciële bedrijven gebruiken om hun waren aan de man te brengen. De kennis over de slachtofferprofielen als ook de technieken die daders hanteren is om twee redenen belangrijk. Ten eerste laat het zien dat niet iedereen die slachtoffer van fraude wordt, weggezet kan worden als hebberig, dom of te goed van vertrouwen, wat al te gemakkelijk gebeurt (Corpeleijn, 2008). Ten tweede kan door het geven van voorlichting over beïnvloedings-technieken, meer de nadruk gelegd worden op de wijze waarop slachtoffers worden benaderd.

Bij loterijfraude, een opkomende trend, worden voornamelijk vrouwen van 75 jaar of ouder slachtoffer, die een ingrijpende gebeurtenis hebben meegemaakt

(bijvoorbeeld ziekte of verlies van hun partner) en daar moeilijk mee overweg kunnen. Ze hebben vaak een laag opleidingsniveau en inkomen, zijn financieel niet goed onderlegd en bagatelliseren hun slachtofferstatus. (Pak & Shadel, 2007). Bij datingfraude, dat in Nederland in opkomst is, gaat het om mannen en vrouwen in de leeftijd van 40 tot 50 jaar, die gescheiden zijn of hun partner verloren hebben. De verhouding mannen – vrouwen die slachtoffer worden is nagenoeg gelijk. Vaak hebben ze een moeilijke tijd achter de rug en zoeken een nieuwe partner. Ze blijken in die fase extra kwetsbaar. Mensen komen uit alle lagen van de bevolking, met allerlei soorten beroepen en achtergronden, en ook de economische achtergrond zegt niets over het slachtofferschap.

Daders treffen slachtoffers vaak feilloos in hun zwakte, de één zit in een persoonlijke financiële crisis, de ander heeft behoefte aan aandacht. Dit verklaart voor een deel waarom de één wel slachtoffer wordt en de ander niet. De daders bouwen een vertrouwensband op met het slachtoffer, waardoor deze uiteindelijk meer emotionele schade oploopt omdat het vertrouwen diepgaand wordt beschaamd. Veel slachtoffers handelen vanuit eenzelfde soort perspectief, namelijk vanuit onwetendheid, goed van vertrouwen en/of naïviteit. En of ze nu handelen uit een zeker winstbejag, zoals bij investeringsfraude of loterijfraude, of uit een gevoel van goed te willen doen, zoals bij erfenisfraude, er is meestal sprake van goed vertrouwen (Corpeleijn, 2008).

De ernst van voorschotfraude ligt vooral in de wijze waarop fraudeurs inspelen op de kwetsbaarheden van hun slachtoffers. De slachtoffers worden financieel leeggezogen door personen die zij vertrouwen. Dit vertrouwen wordt vervolgens diepgaand beschaamd, waardoor ze, naast financiële schade, ook veel emotionele schade hebben.

4.3.5 Criminaliteitsrelevante factoren

De criminaliteitsrelevante factoren die de komende jaren van invloed zullen zijn op het fenomeen voorschotfraude, zijn onder andere de lage prioriteit binnen de opsporing, ontwikkelingen op het internet en de globalisering (het internationale aspect).

Nederland bleek een erg aantrekkelijk land voor Nigeriaanse fraudeurs. Tot de start van het project Apollo was de prioriteit laag en was de strafmaat laag. De prioriteit is, na beëindiging van het project, na een opleving gedurende het Apollo-project, wederom laag. Dit kan gezien worden als een criminaliteitsbevorderende factor in de komende jaren. Omdat er geen onderzoeken worden ingesteld, ontbreekt het werkelijke zicht op de aard en omvang. Recentelijk

wordt echter door verschillende experts een stijging waargenomen in het aantal fraudes, daders en slachtoffers. Hoewel voorschotfraude ondanks deze stijging nog niet het niveau heeft van een aantal jaren geleden, zal het bij een blijvend lage prioritering vermoedelijk doorzetten.

Een andere criminaliteitsbevorderende factor is het toenemend gebruik van internet. Dit geldt voor meerdere vormen van fraude, maar vooral voor voorschotfraude geldt dat het de fraudeurs faciliteert in het vinden en benaderen van hun slachtoffers. Via websites, social media, chatrooms, datingsites en e-mail (spam) wordt gezocht naar geschikte slachtoffers, waarna contact wordt gelegd en onderhouden met alle gevolgen van dien. Vooral ouderen ontdekken en gebruiken steeds meer deze faciliteiten, maar zijn extra kwetsbaar, omdat ze veelal naïef en te goed van vertrouwen zijn. Ook lijkt het erop, dat in de contacten via deze media, mensen minder voorzichtig zijn met het prijsgeven van persoonlijke informatie. Gedrag lijkt hierdoor te veranderen: mensen overschrijden grenzen die ze in het dagelijks leven nooit zouden overschrijden. Naar verwachting worden hierdoor de kansen voor fraudeurs verhoogd. Dit is niet nieuw, maar in de komende jaren zullen verdere ontwikkelingen op het internet, met name in social media, fraudeurs in staat stellen hun slachtoffers (nog) doeltreffender te benaderen. Een andere criminaliteitsbevorderende factor die met het gebruik van internet samenhangt, is de globalisering.

Voorschotfraude is een sterk internationaal fenomeen. Fraudeurs maken slachtoffers over de hele wereld, waarbij meestal wordt gewerkt vanuit andere landen dan waar de slachtoffers worden gemaakt. Door internet kan dit veel gemakkelijker. Daarbij zijn de samenwerkingsverbanden mobiel en goed georganiseerd. Hierdoor kunnen ze hun activiteiten gemakkelijk verplaatsen wanneer dit noodzakelijk is. De globalisering zal in de komende jaren waarschijnlijk niet afnemen en daarom een criminaliteitsbevorderende factor blijven.

4.3.6 Verwachtingen

De omvang van voorschotfraude is moeilijk vast te stellen. De aangiftebereidheid is erg laag, waardoor de aangiften slechts een zeer beperkt deel van de slachtoffers weerspiegelen. Desondanks zien experts een duidelijke toename van deze vorm van fraude in de afgelopen jaren. Schattingen geven aan dat de financiële schade voor Nederlandse slachtoffers 60 miljoen bedraagt in 2011. In de politie-systemen komt echter maar 6 miljoen voor. Hoewel de financiële schade nog ver verwijderd lijkt van het niveau ten tijde van het Apollo-project, is het belangrijk om meer inzicht te verwerven in de aard en omvang van dit fenomeen.

Gezien de criminaliteitsbevorderende factoren lijkt dit extra belangrijk aangezien op basis van deze ontwikkelingen het te verwachten is dat voorschotfraude de komende jaren zeker niet zal afnemen. Er is op dit moment echter te beperkt zicht op de omvang om van een toename uit te gaan.

Met betrekking tot de ernst zijn geen veranderingen te verwachten. Voorschotfraude heeft zowel financieel als emotioneel ernstige gevolgen voor de slachtoffers. Dit zal de komende jaren niet wijzigen.

4.3.7 Aanpak

Vanwege de ernst werden in het Nationaal dreigingsbeeld van 2008 voorschotfraude en beleggingsfraude tot dreiging gekwalificeerd. Deze kwalificaties zijn echter nooit omgezet in concreet beleid of een hernieuwde aanpak van de problematiek. In 2009 gaf het OM opdracht aan de Dienst IPOL om de Nigerianen-problematiek in kaart te brengen, en ook de resultaten uit dat rapport hebben niet geleid tot een herziene aanpak. Hieruit kan worden afgeleid dat sinds het stopzetten van het project Apollo niets meer is gedaan aan voorschotfraude. Omdat dit voor alle hoofdvormen van fraude in meer of mindere mate geldt, verwijzen wij in dezen naar een voorstel voor een aanpak van fraude dat omschreven wordt in hoofdstuk 6.

4.4 Acquisitiefraude

Huisman en Van de Bunt (2009) rapporteerden uitvoerig over de aard, omvang en ernst van acquisitiefraude, en over de knelpunten die bij de aanpak worden ervaren. De opstellers van het rapport hebben zich vooral gericht op groeperingen die in Nederland actief zijn. Dit rapport is nog steeds actueel en zal in dit deelrapport gebruikt worden om de Nederlandse situatie samen te vatten; de internationale situatie zal geschetst worden op basis van een interview met de directeur van het Steunpunt Acquisitiefraude (SAF) en literatuur.

4.4.1 Aard

Acquisitiefraude wordt door het SAF als volgt gedefinieerd:

Acquisitiefraude is het stelselmatig benaderen van aan het economische verkeer deelnemende organisaties (bedrijfsleven, overheid, non-profit sector), door malafide advertentiebureaus, uitgeverijen, adviesbureaus of personen handelend in opdracht van dit soort bedrijven, met als doel het onder valse voorwendselen

verkrijgen van (advertentie) opdrachten door het misleiden van werkzame personen binnen die organisaties, teneinde daar een financieel voordeel mee te behalen.

Huisman en Van de Bunt (2009) stellen dat in Engelstalige literatuur *“misleidende handelspraktijken tussen ondernemingen in het buitenland worden aangeduid als ‘business scams’.* Deze scams doen zich voor op allerlei terreinen, niet alleen bij het aanbieden van advertenties in tijdschriften of vermeldingen op internet, maar net zo goed bij de verkoop van kantoorproducten of diensten van *‘consultants’.* Het begrip *‘scam’* drukt veel beter dan het begrip *‘fraude’* uit dat de handelspraktijken balanceren tussen slim, agressief zakendoen en onrechtmatig handelen” (p. 4).

Bedrijven worden op twee manieren benaderd, via massale mailings of persoonlijk. Bij een massale aanpak krijgt een groot aantal ondernemers een document opgestuurd met daarin een aanbod, verhuuld in de vorm van een factuur (ook wel spookfactuur of spooknota genoemd). De misleiding bestaat eruit dat aanbieders proberen bedrijven te laten denken dat zij een factuur moeten betalen, terwijl zij door te betalen een document tekenen dat kan doorgaan voor een rechtsgeldige overeenkomst. De fraudeurs speculeren erop dat potentiële gedupeerden de kleine lettertjes over het hoofd zien en dit wordt in de hand gewerkt door aan te sluiten op de huisstijl van gerenommeerde organisaties. Zo stuurde een malafide bedrijf een mailing aan 350.000 ondernemingen waarin de huisstijl leek op die van de Kamer van Koophandel; de afkorting KvK werd gehanteerd, die in dit geval stond voor Kantoor voor Klanten en niet voor Kamer van Koophandel.

De malafide bedrijven hebben allemaal een eigen website en geven een fysieke gids of een krantje uit om de schijn op te houden dat het om een bonafide bedrijf gaat. De adverteerder krijgt wel een ‘bewijsexemplaar’ opgestuurd, maar de doelgroep (potentiële klanten) wordt nooit bereikt. De slachtofferbedrijven worden weliswaar gemeld op de online gids, maar het zijn altijd onbekende gidsen die geen waarde voor adverteerders hebben, omdat ze niet via de reguliere weg op internet te vinden zijn. Met andere woorden, er wordt niet geïnvesteerd in naamsbekendheid, zoals de Gouden Gids en anderen wel doen.

Recent is een nieuwe modus operandi waargenomen. Begin februari 2012 kregen naar schatting tienduizenden klanten een vervalste factuur met het echte logo van de Telefoongids en de Gouden Gids, waarin ook echte gegevens en het logo van de Kamer van Koophandel stonden. Het was de eerste keer dat vervalste facturen werden verstuurd met echte logo’s erop; meestal gaat het om

gelijkende logo's en andere gegevens. De fraudeurs maakten hiervoor vermoedelijk gebruik van het adressenbestand van het bedrijf dat beide gidsen uitgeeft.

Bij een persoonlijke (vaak telefonische) benadering proberen fraudeurs op verschillende manieren vertrouwen te wekken en een positieve verwachting te kweken. Aanbieders suggereren bijvoorbeeld dat er al een zakelijke relatie bestaat of dat een collega al akkoord is gegaan met een opdracht. Er hoeft alleen nog een gegevenscontrole plaats te vinden en een handtekening gezet te worden. Ze noemen bijvoorbeeld terloops een jaarbedrag terwijl het om een maandbedrag gaat. De aandacht wordt afgeleid van de kleine lettertjes, waarin de juiste voorwaarden meestal wel staan omschreven. De fraude is hierdoor moeilijk aan te vechten. De misleiding bestaat eruit dat aanbieders proberen bedrijven een document te laten tekenen dat kan doorgaan voor een rechtsgeldige overeenkomst en waarvan de inhoud lijkt op wat besproken is, maar in de kleine lettertjes een contract bevat.

Bij beide benaderingen wordt onder het mom van gegevenscontrole een fax gestuurd. Bij spooknota's wordt de suggestie gewekt dat de klant een betalingsverplichting heeft, terwijl in de kleine lettertjes staat dat het om een offerte gaat. De tegenprestatie is altijd nihil. Wanneer de klant een eerste factuur ontvangt, of al betalingen heeft gedaan, komt hij er vrij snel achter dat de overeenkomst malafide is. Doordat is getekend voor akkoord, is het erg moeilijk om de overeenkomst te ontbinden.

Er bestaan verschillende modi operandi om slachtoffers te misleiden. Het kan voorkomen bij het aanbieden van advertenties op websites of in fysieke uitgaven (bijvoorbeeld een telefoongids). Er wordt verwarring gezaaid over het registreren van domeinnamen²⁹. Er kunnen vervalste facturen van echt lijkende bedrijven gestuurd worden voor zogenaamd geleverde diensten of producten, bijvoorbeeld software. Het kan gaan om een eenmalige betalingsopdracht of een jaarcontract met periodieke betalingen. Wanneer niet wordt voldaan aan de betalingsverplichting, schakelen de malafide aanbieders zonder pardon incassobureaus in of voeren civiele acties tegen wanbetalers of tegen personen die het wagen hun 'goede naam' in diskrediet te brengen.

²⁹ Bedrijven worden telefonisch gewaarschuwd dat een mogelijke concurrent een soortgelijke domeinnaam heeft aangevraagd. Vervolgens bieden de fraudeurs aan om, tegen betaling, snel het desbetreffende domein te registreren.

Op de website van het SAF staat een lijst van bedrijven die verschillende (niet bestaande) producten aanbieden, zoals de Bedrijvengidsonline, de Gouden-telefoongids.nl, Heritage Software, de Nationale Telefoongids en T.I.D. Elektrotechniek. Malafide ondernemingen verschillen nauwelijks van bonafide, ze staan ingeschreven bij de Kamer van Koophandel, hebben een professioneel ogende website (waarop een afbeelding van een prachtig bedrijfspand staat) en goed vormgegeven nota's.

Alle branches kunnen slachtoffer zijn. Tot een aantal jaren geleden waren vooral kleine ondernemingen de dupe, maar de fraudeurs hebben hun praktijken verspreid over allerlei bedrijven en organisaties, zoals ziekenhuizen, multinationals, scholen en gemeenten.

4.4.2 Omvang

Het SAF kreeg tot en met 2009 gemiddeld 3000 meldingen per jaar van bedrijven in Nederland die met acquisitiefraude in aanraking waren gekomen. Een bedrijf kan meerdere meldingen doen, waardoor het aantal meldingen hoger ligt dan het aantal gedupeerde organisaties. In 2010 was het aantal meldingen gestegen naar 8200. Deze enorme stijging is toe te schrijven aan de spooknota's, die vanaf dat jaar ook als melding werden meegenomen. In 2011 was het aantal meldingen 11.000. Het SAF stimuleert melderders om ook aangifte te doen, omdat dit een zaak sterker maakt wanneer deze voor de rechter komt. Het aantal aangiften blijft echter ruimschoots achter bij het aantal meldingen bij het SAF. Uit de analyse van de aangiften (hoofdstuk 3) blijkt dat slechts 255 keer aangifte is gedaan van acquisitiefraude en spooknota's en dat is 2,4 procent van het totaal. Op verschillende plaatsen in dit rapport is aangegeven dat de aangiftebereidheid in het algemeen laag is, en dit is met name het geval voor slachtoffers van acquisitiefraude. Het doen van aangifte kost veel moeite en daar staat tegenover dat de kans dat een zaak voor de rechter komt erg klein is.

Huisman en Van de Bunt (2009) trokken een steekproef van 200 uit een totaal van 5000 meldingen die bij het SAF zijn gedaan (in een periode van vijftien maanden tussen 2007 – 2008) en analyseerden deze. Ook onderzochten zij 28 bankrekeningen van malafide aanbieders en werden 24 experts geïnterviewd. Een kwart van de meldingen ging over een massale aanpak van bedrijven, het merendeel was het resultaat van een persoonlijke benadering. Een kwart van de meldingen had betrekking op plaatsing van een advertentie in een fysieke fake-uitgave, bijna de helft (43,5%) op een internetgids, een tiende op domeinnaamfraude en ruim tien procent op spooknota's.

Van de 200 meldingen was 72 procent afkomstig van kleine bedrijven, 20 procent van middelgrote bedrijven en 8 procent van zeer grote bedrijven (onder meer ziekenhuizen en zorginstellingen). Het aantal meldingen wordt door Huisman en Van de Bunt het topje van de ijsberg genoemd, vanwege de lage aangiftebereidheid van de gedupeerden. Ondernemers schamen zich, de politie is afhoudend bij het opnemen van aangiften over acquisitiefraude (zo bleek uit een proef van Huisman en Van de Bunt), en niet altijd realiseren ondernemers zich dat ze misleid zijn of worden.

In samenwerking met vier banken keken Huisman en Van de Bunt ook naar 28 bankrekeningen van malafide bedrijven. Op deze rekeningen werden in totaal 9.558 overboekingen gedaan, waarbij de fraudeurs gezamenlijk 5,7 miljoen euro aan wederrechtelijk voordeel genoten. De perioden waarbinnen overboekingen werden gedaan, verschilden van één tot veertien maanden en ook het aantal overboekingen binnen die perioden vertoonde grote verschillen. Zo deden in zeven maanden 3782 gedupeerden overboekingen naar één aanbieder voor vermelding op een website. Deze incasseerde aldus ruim 2,5 miljoen euro. Een andere aanbieder kreeg binnen veertien maanden slechts één overboeking van 4486 euro. De gemiddelde bedragen die overgeboekt werden, lagen tussen de 100 en 4700 euro. Huisman en Van de Bunt vergeleken deze gegevens met de meldingen die het SAF kreeg met betrekking tot dezelfde aanbieders, en vonden daarin ook enorme verschillen. De malafide aanbieder die in veertien maanden tijd één overboeking ontving, leverde het SAF dertien meldingen voor een (betwist) schadebedrag van afgerond 172.000 euro. Er werden geen overboekingen gedaan; betwist wil zeggen gedeclareerd door malafide bedrijven, maar niet daadwerkelijk betaald door potentieel gedupeerden.

Huisman en Van de Bunt waagden zich niet aan een schatting van de financiële schade, maar het SAF deed wel uitspraken over de jaarlijkse schade van acquisitiefraude voor het bedrijfsleven, de overheid en de gesubsidieerde sector. Een aantal jaren geleden schatten MKB-Nederland, de Kamer van Koophandel en organisaties voor verantwoord ondernemen de schade op 400 miljoen gulden, omgerekend 180 miljoen euro. De schade voor de overheid en de gesubsidieerde sector was daar niet in meegenomen, omdat deze sectoren er vaak niet van op de hoogte waren dat ze slachtoffer van fraude waren, maar wel hoge bedragen overmaakten. Toen dit bekend werd, heeft het SAF het geschatte bedrag verdubbeld en afgerond op 400 miljoen euro.

Van deze cijfers is echter geen goede onderbouwing bekend, en het lijkt aan de hoge kant. Er wordt namelijk veel aan preventie gedaan, waardoor het fenomeen acquisitiefraude beter bekend is geworden. Daardoor is het waarschijnlijk dat

ondernemers en bestuurders meer beducht zijn op deze vorm van fraude. Veel bedrijven krijgen wel rekeningen, maar betalen vaak niet.

Tot slot is er nog het gemiddelde schadebedrag dat in rekening wordt gebracht in verhouding tot de totale schade. Volgens opgave van de Fraudehulpdesk werd over de periode februari tot en met december 2011 gemiddeld 641 euro per melder in rekening gebracht. Uitgaande van de geschatte 400 miljoen euro schade zou het aantal gedupeerden dan 700.000 moeten zijn. Dat lijkt niet reëel op basis van het aantal meldingen dat bij het SAF wordt gedaan en al jaren stabiel is (in 2010 was dat 8200, doordat spooknota's werden meegenomen). De bij het SAF gemelde schade ligt veel lager dan de geschatte schade. In de periode 2003 – 2011 werd voor een bedrag van (afgerond) 48 miljoen euro gemeld, dat is gemiddeld 5 miljoen euro per jaar. Het gaat hier om betwiste contracten, de melders hebben minder betaald en worden door het SAF geholpen in het tegenhouden van geldstromen richting oplichters. Of het aantal meldingen en de totaal gemelde schade de werkelijkheid weerspiegelen is nauwelijks te zeggen. Middelgrote en grote organisaties merken namelijk niet of niet snel dat ze opgelicht worden, waardoor schadebedragen enorm kunnen oplopen. De meldingen worden, zoals hiervoor al uiteengezet, vooral gedaan door kleine bedrijven. Daardoor kan de gemelde schade lager zijn dan wanneer de schade van grote bedrijven en organisaties bekend zou zijn en meegenomen zou worden. Dit betekent dat aan deze ontwikkelingen en het aantal meldingen geen uitspraken over de omvang en financiële schade ontleend kunnen worden.

4.4.3 Criminele samenwerkingsverbanden

De criminele samenwerkingsverbanden (csv's) die zich bezighouden met acquisitiefraude, zijn onder te verdelen in twee soorten: enerzijds csv's van autochtone afkomst, gevestigd in Nederland die zich richten op Nederlandse ondernemingen en organisaties. Anderzijds buitenlandse csv's, die in verschillende landen actief zijn en hun frauduleuze producten via internet wereldwijd aanbieden.

De Nederlandse csv's zijn voornamelijk geconcentreerd in het noordoosten van het land. In de jaren tachtig hield een tweetal broers zich vanuit het noordoosten van het land bezig met misleidende acquisitie. Verschillende malafide ondernemers die nu actief zijn, zouden bij deze broers hebben gewerkt en later voor zichzelf zijn begonnen. Advertentieverkopers werden niet alleen opgeleid, maar ook gestimuleerd om hun eigen bedrijven op te richten om hun werkzaamheden uit te voeren. De organisatiestructuur die op deze manier ontstaat, een netwerk van malafide bedrijven, is kenmerkend voor de handelswijze van

dergelijke actoren. Daarbij blijft onduidelijk wie de daders zijn, omdat ze zich verschuilen achter ingewikkelde constructies van Nederlandse en buitenlandse vennootschappen (Kabki, Van Koningsveld, Staat & Westerbeek, 2011).

De schatting is dat in totaal 250 aanbieders zich bezighouden met acquisitie-fraude. Het aantal aanbieders is niet gelijk aan het aantal actieve csv's: één csv kan meerdere aanbieders aansturen. Het SAF schat dat in Nederland dertig tot vijftig csv's actief zijn met het aanbieden van advertenties en domeinnamen, en daarnaast twintig die zich bezighouden met het verzenden van spooknota's. Huisman en Van de Bunt (2009) kwamen op 62 malafide organisaties die leefden van dit soort fraude, maar harde gegevens hierover ontbreken.

De omvang van de malafide bedrijven loopt uiteen van eenmanszaakjes en bedrijfjes van twee à drie werknemers tot grote georganiseerde netwerken, die bestaan uit een overkoepelend bedrijf met verschillende leidinggevendende kleinere uitvoerende bedrijven onder hun hoede hebben. Werknemers zijn er niet altijd van op de hoogte dat ze bij bedrijven werken die frauduleuze activiteiten verrichten: soms worden ze geworven uit re-integratieprojecten of gaat het om schoolverlaters. Door steeds nieuwe bv's op te richten schermen de fraudeurs de feitelijk betrokken medewerkers en bestuurders van het bedrijf effectief af (Kabki et al., 2011). Bij het registreren in het handelsregister en het openen van bankrekeningen wordt veelal gewerkt met katvangers, waardoor onduidelijk blijft wie er daadwerkelijk leiding geeft aan het bedrijf. Zo kwam in het geval van de *World Business Guide* een Nederlands echtpaar in beeld dat een postbus en een bankrekeningnummer beheerde, waarop betalingen binnenkwamen die via moneytransfers werden doorgeboekt naar andere landen. Zij ontvingen in twee maanden tijd 650 overboekingen met een totale waarde van 400.000 euro.

Frauduleuze bedrijven werken meer specialistisch dan generalistisch, ze worden niet groter en ontwikkelen geen andere activiteiten. De csv's erachter zijn nauwelijks aan te pakken, omdat ze gebruikmaken van internet, en zich verschuilen achter talloze rechtspersonen in binnen- en buitenland. Door de verspreiding over meerdere landen, is het daarom een groot internationaal probleem. Buitenlandse aanbieders betreden in toenemende mate de Nederlandse markt. Naar schatting zijn in het buitenland vijf csv's actief die wereldwijd slachtoffers maken. Ze opereren onder meer vanuit Zweden, Zwitserland, Duitsland, Spanje en België. Vanuit Zweden werd fraude met domeinnamen gepleegd, waarbij in twee maanden tijd ruim 700.000 euro werd overgeboekt. Vanuit Zwitserland zijn aanbieders van de *European Business Guide* al twintig jaar actief. Op de website van het SAF is te lezen:

“World Business Guide is het zusje van EU Company Directory is het zusje van EU Business Guide is het zusje van Euro Business Guide is het zusje van EU Business Services is het zusje van European City Guide etcetera etcetera.”

In totaal 140 meldingen kwamen uit Duitsland over de Gele Bedrijvengids; de fraudeurs hierachter zijn Duitsers die zich gevestigd hebben in Spanje en Florida, en die investeren in vastgoed, pornografie en zoekmachines.

Eén crimineel samenwerkingsverband, dat voorheen vanuit Heerhugowaard opereerde, heeft zijn activiteiten verplaatst naar Duitsland en België. Waarschijnlijk richten de leden hun activiteiten nu op die landen en niet specifiek op Nederland. Verdere gegevens over de samenstelling van zowel Nederlandse als buitenlandse csv's ontbreken.

4.4.4 Maatschappelijke gevolgen

Bij acquisitiefraude is sprake van het zogenoemde *many-little-principe*: veel slachtoffers, relatief lage bedragen en een laag risico. Bedrijven (meestal kleine en middelgrote bedrijven) zijn zich vaak niet bewust van de oplichting en soms worden ze dat nooit, en gaat de fraude jarenlang door.

De omvang van de financiële schade is onbekend, maar ligt waarschijnlijk tussen enkele en tientallen miljoenen euro's per jaar. Naast financiële schade is er ook emotionele schade. Wanneer mensen door acquisitiefraude worden opgelicht, zijn ze over het algemeen geschokt en kunnen niet geloven dat ze erin getrappt zijn. Ze zijn opgelicht terwijl ze zich veilig waanden. De verdere gevolgen hangen af van de hoogte van het schadebedrag. Sommige mensen krijgen behoorlijke emotionele problemen, anderen zijn laconieker, maar kunnen problemen krijgen als ze er nog een keer intrappen. De gevolgen van de fraude, het doen van aangifte of het verwerken van de emotionele problemen, kost tijd en dat is tijd die ze dan niet in het bedrijf kunnen steken. Handel berust in belangrijke mate op vertrouwen en dit type fraudezaken ondermijnt het vertrouwen in het handelsverkeer.

4.4.5 Criminaliteitsrelevante factoren

De juridische aanpak en bestrijding van acquisitiefraude loopt in Nederland moeillijk. Malafide bedrijven weten de mazen van de wet te vinden door samen te werken met juristen en belastingadviseurs (Fleuren, 2009). Ook wordt de schuld afgewenteld op de gedupeerden, zij hadden de kleine lettertjes immers kunnen lezen, zoals een uitspraak door het Gerechtshof Den Bosch in 2008 liet

zien ('van bedrog in strafrechtelijke zin kon geen sprake zijn'). Acquisitiefraude is niet strafbaar gesteld en wanneer vervolging plaatsvindt, is dat op basis van valsheid in geschrifte (art. 225 sr), verduistering en bedrog. Daarmee raakt het niet de kern van het probleem, omdat het gebruik van valse geschriften slechts een manier is waarop ondernemers worden misleid. Het ligt meer voor de hand om strafrechtelijk te vervolgen op basis van oplichting (art. 326 sr), omdat deze strafbepaling zich meer richt op bedrog bij de totstandkoming van de overeenkomst en het afdwingen van de betalingen. Tijdens het telefonisch contact tussen fraudeur en potentieel slachtoffer is bijvoorbeeld sprake van leugens en verzwijgingen, bij de fysieke uitgaven van gidsen en bij de internetgidsen en/of websites is sprake van het toezenden van een misleidende fax, en bij fysieke printuitgaven en domeinnaamfraude is sprake van het aannemen van een valse naam. Bovendien wordt een valse hoedanigheid aangenomen door het malafide bedrijf (Fleuren, 2009). De bewijslast is moeilijk en een proefproces hieromtrent is nooit gevoerd. Wanneer deze situatie gehandhaafd blijft, wordt fraudeurs weinig in de weg gelegd bij de voortzetting van hun frauduleuze praktijken.

Het zijn vaak de malafide bedrijven die een rechtszaak starten om de gedupeerden die niet betalen tot betaling te dwingen. Het malafide bedrijf dat door het Gerechtshof Den Bosch werd vrijgesproken van bedrog, ging in hoger beroep bij het Gerechtshof 's Gravenhage waar de uitspraak luidde dat er wel sprake was van bedrog. Weinig zaken komen echter voor de rechter. Een civiele procedure starten is mogelijk, maar dan is het aan de slachtoffers om te bewijzen dat ze misleid zijn. Een aantal aanbieders gaat op deze manier al jarenlang zijn gang; zo houdt de belanghebbende/bestuurder van Holland Internet Group (voorheen Website Services BV, aanbieder van diverse internetgidsen en domeinnamen), de Telefoongids.com en Infosite BV zich al ruim twintig jaar in Nederland met dubieuze praktijken bezig. Het is niet te verwachten dat de komende jaren in de omvang van acquisitiefraude verandering optreedt, als er niets verandert in de wetgeving.

4.4.6 Verwachtingen

Het SAF verwacht geen belangrijke verschuivingen; acquisitiefraude in Nederland zal niet groter worden, er zullen geen andere (nieuwe) vormen op de markt komen.

4.4.7 Aanpak

MKB-Nederland heeft in juli 2011 een civielrechtelijk proces aangespannen tegen de belanghebbende/bestuurder van Holland Internet Group (zie paragraaf

4.4.5), vanwege de grote hoeveelheid klachten en meldingen. MKB-Nederland heeft de rechtbank niet alleen gevraagd om de fraude te doen stoppen, maar ook om een principiële uitspraak te doen over de Wet oneerlijke handelspraktijken³⁰. MKB-Nederland heeft de rechter gevraagd de wet, die nu alleen voor consumenten geldt, ook van toepassing te laten zijn voor kleine en middelgrote ondernemingen. Daardoor worden ondernemers beter tegen acquisitiefraude beschermd.

De Europese richtlijn waarop de Nederlandse Wet oneerlijke handelspraktijken is gebaseerd, laat expliciet de ruimte om ondernemers die bescherming te bieden. In andere lidstaten is de wet al aangepast. Inmiddels staat in Europees verband acquisitiefraude hoog op de agenda; het Europees Parlement heeft in juni 2011 een resolutie aangenomen tot striktere naleving van de richtlijn Misleidende reclame. Het Europees Parlement doet een beroep op de Europese Commissie om de naleving van de richtlijn actief af te dwingen, te bespoedigen dat relevante wetgeving wordt aangepast en in geval van handhaving waar nodig corrigerend op te treden.

Tot slot is een integrale aanpak van belang (zie ook hoofdstuk 6). Primair is die aanpak gericht op preventie door voorlichting te geven en een beroep te doen op de eigen verantwoordelijkheid van ondernemers. Verder zijn maatregelen gericht op tegenhouden nodig, zoals het blokkeren van bankrekeningen waarop criminele gelden worden ontvangen. Daarnaast zijn civielrechtelijke acties van belang. De inzet van het strafrecht vormt het sluitstuk en komt om de hoek in geval van ernstige vormen van oplichting, bijvoorbeeld als het gaat om hoge bedragen of stelselmatige fraude door criminele organisaties. Bij een integrale aanpak zouden overigens alle vormen van fraude gebaat zijn.

4.5 Hypotheekfraude

Voor dit hoofdstuk zijn twee experts geïnterviewd en is gebruik gemaakt van twee oudere rapporten over vastgoedfraude (FEC, 2008; Ferwerda, Staring, De Vries Robbé & Van de Bunt, 2007). Geen toestemming werd gekregen om uit een recent (vertrouwelijk) rapport van het Financieel Expertise Centrum (FEC) over hypotheekfraude te citeren.

³⁰ Burgerlijk Wetboek, Boek 6, Titel 3, Afdeling 3A Oneerlijke handelspraktijken.

4.5.1 Aard

Hypotheekfraude wordt gepleegd met het doel vastgoed te verwerven op onrechtmatige gronden. Als hypotheekfraude is aan te merken:

- Het vervalsen of valselijk opmaken van formulieren, zoals valse en vervalste loon- en inkomensgegevens, taxatierapporten, werkgeversverklaringen, belastingaangiften, uittreksels van de Kamer van Koophandel en identiteitsbewijzen.
- Het gebruikmaken van deze formulieren en het geven van een verkeerde voorstelling van zaken bij de totstandkoming en/of uitvoering van een hypothecaire financiering.
- Het opzettelijk (of een poging daartoe) benadelen of misleiden van hypothecaire financiers, evenals het oneigenlijk gebruik van het stelsel van hypothecaire financieringen door personen of instanties die zijn betrokken bij de totstandkoming en/of uitvoering van hypothecaire financieringen.

Bij hypotheekfraude is altijd sprake van identiteitsfraude. Behalve van hypotheekfraude is vaak ook sprake van belastingfraude, afpersing en overige commune delicten. Om vastgoedtransacties uit te voeren wordt de hulp ingeroepen van allerlei financiële ondernemingen en dienstverleners, die al dan niet verwijtbaar betrokken zijn. (FEC, 2008).

Hypotheekfraude wordt niet alleen gebruikt voor het verwerven van vastgoed, maar ook voor het genereren van inkomsten. Naast een wijze om geld wit te wassen met het aangekochte vastgoed, zijn er verschillende manieren om inkomen te genereren. Ferwerda et al. (2007) maken onderscheid tussen fraude met betrekking tot exploitatie enerzijds en speculatie anderzijds. Bij malafide exploitatie van het vastgoed komen drie verschijningsvormen voor:

De eerste vorm is *onrechtmatige bewoning* waarbij sprake is van illegale (door)verhuur aan legaal of illegaal in ons land verblijvende personen.³¹

De tweede vorm bestaat uit *onregelmatigheden rond de verhuur* van particuliere woningen, waarbij de traditionele huisjesmelker zijn huurders uitbuit.

³¹ Deze personen betalen vaak een hoge huur en worden gebruikt om tegen een schamel salaris in kassen en kwekerijen te werken.

Tot slot is er bij de derde vorm sprake van *onrechtmatig gebruik*. Binnen deze vorm wordt de woning voor andere doeleinden gebruikt dan reguliere huisvesting. Dit kan uiteenlopen van illegale pensions tot het gebruik van de woning als dekmantel voor criminele activiteiten, zoals hennepteelt, mensenhandel, witwaspraktijken en illegale prostitutie.

Exploitatievormen verschillen per stad of regio. Amsterdam en Utrecht kampen vooral met illegale onderhuur, terwijl de problematiek in Rotterdam en Den Haag zich concentreert op uitbuiting van illegalen, huisjesmelkers, verkrotting en overbewoning van panden die veelal privaats eigendom zijn (Ferwerda et al., 2007).

Het Openbaar Ministerie in Den Haag heeft vandaag in een groot onderzoek van politie Haaglanden en het OM naar witwassen, valsheid in geschrifte, overtreding van de woningwet en hypotheekfraude beslag gelegd op 30 panden in Den Haag met een aankoopwaarde van meer dan drie miljoen euro's. Er is ook beslag gelegd op honderdduizenden euro's op diverse bankrekeningen. De hoofdverdachte wordt ervan verdacht dat hij de 30 panden heeft gefinancierd met crimineel geld uit het verleden, dat onder meer is verkregen door belastingfraude, valsheid in geschrifte en oplichting. Hij wordt er van verdacht de woningen op naam van zogenaamde katvangers te hebben gezet, om zo zelf buiten beeld te blijven van de autoriteiten. De woningen zijn veelal verhuurd (huisjesmelkerij).

Website Openbaar Ministerie, 10 januari 2012

Naast malafide activiteiten in panden, wordt er ook gespeculeerd met panden, bijvoorbeeld door middel van ABC-transacties, waarbij panden in een korte periode tegen steeds hogere prijzen worden doorverkocht. De bij deze transacties betrokken personen werken samen en delen de winst uit de steeds hogere verkoopprijs of gebruiken de winst om criminele schulden en vorderingen te verrekenen. De hypotheekverstrekker moet het pand vervolgens op een executieveiling tegen een lage prijs verkopen en draait verlies. Er is sprake van verkoopcarrouzels wanneer een stroman het pand koopt, en dan doorverkoopt aan een andere stroman die het pand voor meer geld wil kopen met behulp van een vervalste hypotheekaanvraag. Op het moment dat het pand is betaald, is de winst binnen en wordt de hypotheek niet meer afgelost (Ferwerda et al., 2007).

Een bijzondere vorm van hypotheekfraude is fraude met bouwdepots. Een bouwdepot wordt afgesloten bij een hypotheek wanneer het hypotheekbedrag of een gedeelte daarvan bestemd is voor bouw. Een bouwdepot is een soort

rekening waar geld op staat, om daaruit kosten te betalen voor de bouw van een woning. Dat kan gaan om nieuwbouw of om verbouw van een bestaande woning. Met behulp van valse facturen van bouwbedrijven kunnen bouwdepots leeggehaald worden voor andere doeleinden dan bouw of verbouwing.

In tegenstelling tot de meeste andere vormen van horizontale fraude, die grensoverschrijdend zijn, vindt hypotheekfraude voornamelijk op Nederlands grondgebied plaats.

4.5.2 Omvang

Over de aard, omvang en geleden schade van hypotheekfraude bestaat geen uitgebreide rapportage. De Stichting Fraudebestrijding Hypotheken (SFH) heeft zich ten doel gesteld om in het jaar 2012 te werken aan een kwalitatieve en kwantitatieve analyse van hypotheekfraude.

De SFH maakt sinds 2004 gebruik van het Incidentenwaarschuwingssysteem Financiële Instellingen. Jaarlijks worden hierin 500 à 600 (rechts)personen door de banken geregistreerd die hypotheekfraude hebben gepleegd. Ten opzichte van de eerste jaren is het aantal registraties afgenomen. Dit is het gevolg van preventieve maatregelen die zijn genomen door de hypotheekverstrekkers. Daarnaast zijn de eisen vanuit het College Bescherming Persoonsgegevens (CBP) aangescherpt. Ieder incident dat wordt geregistreerd, moet ook worden gemeld aan het CBP. Ook heeft de Hoge Raad bepaald dat altijd een aangifte nodig is voordat gegevens met andere banken mogen worden uitgewisseld. Bij de SFH is niet bekend hoe vaak aangifte wordt gedaan van hypotheekfraude. De analyse van de aangiften die wij zelf hebben uitgevoerd (hoofdstuk 3), leverde 253 aangiften op, waarvan het merendeel over hypotheekfraude (234) ging en een klein deel over fraude met bouwdepots (46). Deze aangiften staan niet los van elkaar; daar waar sprake is van bouwdepotfraude is nagenoeg altijd sprake van hypotheekfraude. Twee groeperingen konden worden onderscheiden die verantwoordelijk waren voor vijf of meer aangiften.

Het aantal ABC-transacties is afgenomen doordat notarissen een meldingsplicht of onderzoeksplicht hebben bij ongebruikelijke transacties. Ook fraude met bouwdepots neemt af doordat sinds kort nieuw op de markt komende bouwbedrijven worden doorgelicht. Depotfraude wordt door de dalende markt eerder zichtbaar. Onder andere door de economische crisis vinden meer executie-veilingen plaats, waardoor zichtbaar wordt dat een depot is leeggehaald voor andere doeleinden dan bouw of verbouwingen.

4.5.3 Criminele samenwerkingsverbanden

Bij hypotheekfraude gaat het nagenoeg altijd om georganiseerde criminaliteit, maar exacte details over het aantal criminele samenwerkingsverbanden dat zich hiermee bezighoudt en de samenstelling ervan, ontbreken. Wel is bekend dat veel verschillende partijen betrokken zijn die ingezet worden door criminele organisaties. Financiële ondernemingen, makelaars, taxateurs, notarissen, belastingadviseurs, trustkantoren, advocaten, accountants en stromannen. De betrokkenheid varieert van geen vragen stellen door een notaris, via het vormen van een cruciale schakel in het proces (valse taxaties afgeven door een taxateur op initiatief van een accountmanager van een bank) tot het compleet orkestreren en (doen) uitvoeren van constructies door een belastingadviseur en een advocaat. Omdat meerdere partijen in de keten zich op zijn minst discutabel gedragen, ontstaat door de stapeling van dergelijke gedragingen een geleghedenstructuur. Ook is vastgesteld dat als een van de financiële ondernemingen of zakelijke dienstverleners zijn diensten weigert, de criminelen gaan 'shoppen' bij anderen. Er is bij hypotheekfraude al snel sprake van verwevenheid tussen onder- en bovenwereld.

Naast allerlei dienstverleners worden katvangers gebruikt om voor een bescheiden bedrag (binnen- en buitenlandse) rechtspersonen of hypotheek op naam te zetten. Het gaat hier meestal om kwetsbare mensen die verslavingsproblemen en schulden hebben.

Een van de geïnterviewde experts geeft aan dat fraudeurs steeds slimmer te werk gaan. Als bij twijfel de bankafschriften bijvoorbeeld tot zes maanden terug worden gecontroleerd, dan zorgen de fraudeurs ervoor dat er zes maanden lang (fictief) salaris is gestort. Daar kan een werkgever bij betrokken zijn, die (uiteraard) iedere vorm van betrokkenheid ontkent. Door deze werkwijze hebben fraudeurs ook nog recht op een WW-uitkering, waardoor ook het Uitkeringsinstituut Werknemersverzekeringen (UWV) schade lijdt. Op internet is het mogelijk om vervalsingen te maken van de benodigde paperassen.

4.5.4 Maatschappelijke gevolgen

Het aantal geregistreerde (rechts)personen dat hypotheekfraude pleegt, is jaarlijks 500 à 600. Aangezien de bedragen die met hypotheek gemoeid zijn, hoog zijn, zal de omvang van hypotheekfraude ook hoog zijn. De financiële schade treft vooral de geldverstrekkers, wanneer niet meer aan de hypotheekverplichtingen wordt voldaan. Het hangt er dan vanaf hoeveel het vastgoed nog voor de bank opbrengt. De schade kan nog verder oplopen wanneer panden

voor de hennepsteelt zijn gebruikt. Daarnaast lijdt de overheid schade, die belastinginkomsten mist, mede doordat ten onrechte gebruik wordt gemaakt van de hypotheekrenteaf trek. Het is niet bekend of particulieren lijden onder de prijsopdrijving die het gevolg is van de geschetste malafide activiteiten.

De maatschappelijke schade wordt voornamelijk veroorzaakt door de criminele activiteiten die zich bij hypotheekfraude voordoen, zoals hennepsteelt, verhuur aan illegalen, mensenhandel en prostitutie. Hierdoor wordt de leefbaarheid van buurten aangetast.

4.5.5 Criminaliteitsrelevante factoren

Banken hebben beperkte mogelijkheden om te controleren: de regelgeving bij het UWV en de voorschriften bij de belastingdienst maken dat geen controle op inkomsten kan/mag plaatsvinden (zelfs niet na toestemming van een cliënt). Dit bemoeilijkt fraudebestrijding door banken.

Eén van de geïnterviewde experts noemt de informatie-uitwisseling met de politie moeizaam. De uitzondering hierop vormen de convenanten die in de gemeenten Den Haag en Rotterdam zijn afgesloten om de samenwerking en uitwisseling tussen gemeenten, politie, OM en private partijen te bevorderen. Een uitbreiding van deze aanpak kan bijdragen aan het indammen van hypotheekfraude.

Een andere criminaliteitsbevorderende factor is het te koop aanbieden van huurwoningen door woningcorporaties. Dit gebeurde vanaf 2007-2008. Het ging vaak om slecht onderhouden woningen in achterstandswijken. Dit levert nog steeds voor fraudeurs en andere criminelen een interessante markt van goedkope woningen op. Zij kunnen veel panden aanschaffen en doorverkopen aan stromannen, die de panden aankopen door gebruikmaking van vervalste inkomensgegevens. Naast fraude met hypotheekleningen sluiten ze bouwdepots af en halen deze leeg. Veel van deze panden worden op verschillende wijzen geëxploiteerd voor criminele activiteiten.

4.5.6 Verwachtingen

Het aantal (rechts)personen dat hypotheekfraude pleegt, is al jaren stabiel. Fraude met bouwdepots wordt, ondanks de afname, als een groeiend probleem gezien, waar vermoedelijk criminele organisaties bij betrokken zijn. Ook wordt geconstateerd dat vaker tussenpersonen betrokken zijn bij hypotheekfraude.

Ondanks een dalend aantal meldingen verwacht een expert dat de omvang onverminderd hoog zal blijven en er weinig zal veranderen.

4.5.7 Aanpak

De Stichting Fraudebestrijding Hypotheken is opgericht in 1999 om hypotheekfraude te signaleren, te voorkomen en te bestrijden. Bij de SFH zijn rond de veertig Nederlandse hypotheekverstrekkers aangesloten, waarmee de gehele Nederlandse hypotheekmarkt gedekt is. Het fraudeloket van de SFH valt onder beheer van de Nederlandse Vereniging van Banken (NVB). Doel van het loket is het uitwisselen van ervaringen en samenwerken aan onderzoeken naar hypotheekfraude.

De bancaire sector is er veel aan gelegen om fraude te voorkomen. De laatste jaren is ingezet op:

- Verbeterde samenwerking tussen hypothecair financiers onderling;
- Gezamenlijke aanbevelingen van hypotheekverstrekkers;
- Samenwerking met betrokken partijen in de keten van financiers, makelaars, taxateurs, notarissen, politie en het OM;
- Het inrichten van afdelingen specifiek gericht op het bestrijden van hypotheekfraude;
- Het monitoren van de portefeuilles van tussenpersonen en het plaatsen van fraudeurs op een waarschuwingslijst voor een periode van acht jaar.

Het Financieel Expertise Centrum (FEC) is ingesteld bij besluit van 31 december 1998 van de ministers van Financiën en Justitie en de staatssecretaris van Financiën. De aanleiding daarvoor was de *Nota integriteit financiële sector* van december 1997. In het FEC zijn de volgende partners vertegenwoordigd: Autoriteit Financiële Markten (AFM), Algemene Inlichtingen- en Veiligheidsdienst (AIVD), de belastingdienst, De Nederlandsche Bank (DNB), FIOD-ECD, Openbaar Ministerie en de politie. Het gezamenlijke doel is het versterken van de integriteit van de financiële sector. Op 2 februari 2012 heeft het FEC aangekondigd zich de komende jaren te richten op witwassen, met blijvende aandacht op onder andere hypotheek- en beleggingsfraude.

4.6 Telecomfraude³²

In 2006 heeft TNO onderzoek gedaan naar telecomfraude in Nederland (Kerkdijk, Knobbe, Helmus & Van Staden, 2006). Het beeld dat in het rapport wordt geschetst is nog steeds actueel, aldus de experts, en daarom wordt dit gebruikt voor de beschrijving van onder andere de aard en omvang. Deze informatie wordt aangevuld door interviews met experts van de Bovenregionale Recherche Noord- en Oost-Nederland (BRNON) en literatuur.

4.6.1 Aard

Van het begrip telecomfraude zijn diverse definities en omschrijvingen in omloop. De meest gangbare³³ is de werkdefinitie die door het Landelijk Expertisecentrum Telecommunicatiefraude is opgesteld. Deze luidt als volgt (Benedick, 2002):

"Elke vorm van misbruik van een telecommunicatievoorziening, waardoor de integriteit van de telecommunicatie infrastructuur wordt of kan worden aangetast dan wel het verrichten van enige frauduleuze handeling teneinde een telecommunicatie dienstverlening te verkrijgen, waardoor enig nadeel kan ontstaan en waarbij de gedragingen of het nalaten is te kwalificeren als een overtreding van het wetboek van strafrecht en/of een bijzondere wet."

Telecomfraude heeft veel verschijningsvormen, zowel bij vaste als mobiele telecommunicatie. De vormen die daarbij het meest in het oog springen, zijn:

PABX-fraude

Bij deze vorm van telecomfraude hacken fraudeurs bedrijfstelefooncentrales. Eenmaal gehackt worden er via deze centrales telefoonverbindingen opgezet naar dure buitenlandse nummers of *premium rate service*-nummers (PRS). Daarnaast worden gehackte centrales ook gebruikt door dubieuze dienstverleners (zoals belwinkels) om gesprekken, via de gehackte telefooncentrale, goedkoop af te handelen. De gesprekskosten komen dan voor rekening van de eigenaar van de gehackte telefooncentrale.

³² In dit rapport beschrijven we telecomfraude, ondanks het feit dat vanaf 2004 deze term vervangen is door de term elektronische communicatiefraude. Reden hiervoor is de bredere bekendheid van de term telecomfraude bij het publiek.

³³ Deze werkdefinitie is onder andere opgenomen in het Handhavingssarrangement tussen het Openbaar Ministerie, het ministerie van Verkeer en Waterstaat en de verschillende mobiele telecomoperators die in Nederland gevestigd zijn.

PRS-fraude

Bij deze vorm van telecomfraude worden grote hoeveelheden telefoonverkeer gegenereerd naar dure servicenummers. Dit leidt tot grote inkomsten voor de serviceaanbieder of nummerhouder³⁴. De schade van deze praktijken uit zich, afhankelijk van de wijze waarop het telefoonverkeer wordt gegenereerd, in extreem hoge telecomnota's voor eindgebruikers en/of inkomstenderving voor de telecomaandbieder.

Premium sms-fraude

Bij deze vorm van telecomfraude worden grote aantallen sms-berichten gegenereerd met een hoog tarief. Meestal meldt een klant zich voor een dergelijke sms-dienst aan door een sms met een korte tekst naar een bepaald nummer te sturen, waarna vervolgens zeer veel *premium* sms-berichten worden verstuurd richting de klant. Afmelding voor dergelijke diensten wordt vervolgens erg lastig gemaakt. De schade van deze praktijken uit zich, afhankelijk van de wijze waarop het sms-verkeer wordt gegenereerd, in extreem hoge telecomnota's voor eindgebruikers en/of inkomstenderving voor de telecomaandbieder.

Abonnementsfraude

Bij deze vorm van telecomfraude worden abonnementen voor telefonie afgesloten met onjuiste gegevens. Dit gebeurt meestal door middel van vervalste identiteitsbewijzen (identiteitsfraude)³⁵. Ook wordt gebruikt gemaakt van personen die door middel van (georganiseerde) ronselpraktijken bereid worden gevonden een abonnement op hun eigen naam af te sluiten en dit aan de fraudeur ter beschikking te stellen. Het verworven abonnement wordt vervolgens bovenmatig gebruikt door de fraudeur.

Telecomfraude is een dynamisch fenomeen. Naast de genoemde verschijningsvormen komen met enige regelmaat nieuwe vormen aan het licht of steken vormen die ingedamd leken te zijn weer de kop op. Een voorbeeld hiervan is PABX-fraude. Deze vorm leek na een afname ten opzichte van een initiële piek, gedurende een aantal jaar een *manageable risk* te zijn geworden (Kerkdijk et al.,

³⁴ De fraudeur onderhoudt in dergelijke scenario's meestal een relatie met de nummerhouder van de PRS-dienst. Vaak betreft het zelfs één en dezelfde partij.

³⁵ In de afgelopen jaren heeft de telecomsector bij de aanvraag van een nieuw abonnement het één cent pinnen geïntroduceerd waarmee klanten zich dienen te identificeren (CMI, 2012). Hierdoor is het plegen van identiteitsfraude met valse documenten ten koste van onwetende slachtoffers een stuk moeilijker gemaakt.

2006). Experts geven aan dat deze vorm van telecomfraude alweer enige tijd frequent voorkomt.

Telecomfraude komt er in de kern op neer dat fraudeurs wel op grote schaal diensten voor telefonie of producten afnemen, maar daar niet voor willen betalen (Kabki et al., 2011). Schade voor telecomaanbieders ontstaat in deze gevallen door het niet kunnen innen van de abonnementsgelden of *prepaid* tegoeden waar wel gebruik tegenover staat.

Bij bedrijven die PRS-nummers of *premium* sms-diensten exploiteren, werkt het anders. Bij fraude met deze diensten wordt het businessmodel van de kick-backregeling misbruikt. Bij verrekening met een kick-backregeling wordt een deel van het aan de consument in rekening gebrachte tarief afgedragen aan de 0900-exploitant (Kerkdijk et al., 2006). Uitbaters van dure PRS-servicediensten hebben door de genoemde kick-backregeling baat bij het genereren van zoveel mogelijk verkeer via hun nummer- of sms-diensten. Het misbruik van deze betaaldiensten komt tot stand doordat exploitant en beller met elkaar samenwerken om zo veel mogelijk telecomverkeer richting de betaaldienst tot stand te brengen. Door dit 'gearrangeerde' telecomverkeer ontstaan extreem hoge telecomnota's voor eindgebruikers en/of inkomstenderving voor de telecomaanbieder.

Omdat rekeningen meestal maandelijks of tweemaandelijks naar eindgebruikers worden verzonden, blijkt pas (veel) later dat er sprake is van niet-inbare kosten. Dit komt mede doordat de beller op frauduleuze wijze een abonnement heeft weten te verkrijgen, dan wel doordat een technische ingreep een 090X-nummerverbinding tot stand is gebracht via een nietsvermoedende abonnee. Voor de exploitant levert het echter grote winst op, omdat hij via de kick-backregeling zijn (gefingeerde) inkomsten al heeft opgestreken.

4.6.2 Omvang

TNO komt tot de conclusie dat de absolute financiële omvang van telecomfraude in Nederland vermoedelijk minimaal 40 miljoen euro bedraagt (Kerkdijk et al., 2006). Verreweg het grootste deel van deze schade komt voor rekening van de telecomaanbieders. Hoewel het een omvangrijk bedrag betreft, is het verlies ten opzichte van de totale omzet in de telecomsector beperkt en vormt het geen directe bedreiging voor de telecombranche.

Hierbij dient te worden vermeld dat deze schatting een momentopname van het jaar 2005 betreft. Schade als gevolg van telecomfraude kan erg fluctueren. Zo

hebben ontwikkelingen op internet en op het gebied van voice-over IP fraudeurs meer handvatten gegeven om telecomfraude op te zetten (Kerkdijk et al., 2006). De branchevereniging ICT-Office heeft bijvoorbeeld een schatting gemaakt van de omvang van fraude met zakelijke abonnementen. Daar kwam uit naar voren dat ongeveer één procent van de zakelijke abonnementen op naam van een plof-BV³⁶ wordt afgesloten. In totaal zou de schade hiervan tussen de zes en tien miljoen euro bedragen (Kabki et al., 2011). De schattingen van de schade als gevolg van telecomfraude zijn in de meeste gevallen een ondergrens. De werkelijke omvang zal waarschijnlijk hoger uitvallen.

Op basis van de analyse van de aangiften (hoofdstuk 3) lijkt de omvang van telecomfraude in de afgelopen jaren redelijk stabiel te zijn gebleven. Tussen 2008 tot en met 2011 vormde telecomfraude tussen de 0,6 en 1,6 procent van de aangiften die onder oplichting geregistreerd staan. In 2011 is in Nederland 172 keer aangifte gedaan van een vorm van telecomfraude. Van deze aangiften gaat het in 89 gevallen om fraude met abonnementen³⁷. Daarna komt PABX-fraude met 41 gevallen. Hierbij kraken fraudeurs de beveiliging van een telefooncentrale, waarna via deze telefooncentrales veel telefoonverkeer, vooral naar het buitenland en dure betaalnummers, wordt gegenereerd.

Sinds 2009 zijn er aanwijzingen dat PABX-fraude aan het toenemen is³⁸. En hoewel hier overeenstemming over lijkt te zijn, lopen de schattingen op basis van meldingen uiteen. Zo kreeg KPN in 2009 hooguit één melding per week, maar inmiddels zouden drie à vier bedrijven per week van deze praktijken de dupe worden. Kleinere aanbieders, zoals Tele2 en Ziggo, hebben met een à twee meldingen per maand beduidend minder gevallen (bron: www.Nos.nl). Experts spreken echter van ongeveer 200 aangiften in het afgelopen jaar, maar tekenen daarbij aan dat het werkelijke aantal aanzienlijk hoger ligt. Onderzoek namens het MKB in 2009/2010 heeft uitgewezen dat het jaarlijks om ruim 700 gevallen gaat (Telegraaf, 2010).

Gedeeltelijk kunnen deze verschillen voortkomen uit het feit dat niet iedereen die slachtoffer wordt van PABX-fraude aangifte doet. Bovendien wordt tele-

³⁶ Op naam van dit soort 'bedrijven' wordt voor veel geld zakelijke abonnementen gekocht, maar blijft betaling uit. Vaak blijkt de 'onderneming' te zijn verdwenen op het moment van incasso.

³⁷ Abonnementenfraude is vaak een opstap om andere criminele activiteiten te plegen zoals PRS-fraude of witwassen.

³⁸ PABX-fraude was in 2001 verantwoordelijk voor een piek in schadecijfers voor de telecombranche, toen was deze vorm van fraude goed voor een miljoenschade onder Nederlandse en West-Europese bedrijven.

comfraude, wanneer wel aangifte is gedaan, vaak onder onjuiste codes weggeschreven waardoor het als zodanig niet terug te vinden is. Alles overziend lijkt het aannemelijk dat jaarlijks zeker 100 bedrijven slachtoffer worden van deze vorm van fraude.

De gemiddelde schade voor een bedrijf als gevolg van deze PABX-fraude loopt van ongeveer duizend euro tot enkele tienduizenden euro's. Uitschieters in schadebedragen kunnen oplopen tot 60.000 euro in één weekend. Sommige bedrijven dreigen daardoor failliet te gaan. De schade als gevolg van alleen PABX-fraude loopt daarmee in totaal in de miljoenen euro's.

4.6.3 Criminele samenwerkingsverbanden

Het grootste deel van de schade is het gevolg van georganiseerde criminaliteit. Hieruit kan echter niet worden geconcludeerd dat het gros van de waargenomen incidenten georganiseerd van aard is. In dit verband schetsen experts een beeld van een zeer beperkte groep criminele organisaties, minder dan vijf procent van de daders, die verantwoordelijk zou zijn voor het overgrote deel van de geleden schade, ongeveer 95 procent (Leipoldt & Laning, 2006, Kerkdijk et al., 2006).

De georganiseerde groepen die zich bezighouden met telecomfraude zijn naar verluidt sterk internationaal van aard en hebben vertakkingen naar een groot aantal individuen en kleine bedrijfjes, de laatste vaak met een beperkte levensduur. Deze organisaties kennen een sterk gelaagde structuur³⁹, wat ervoor zorgt dat hoofddaders grotendeels buiten schot weten te blijven. Ronselaars, die katvangers benaderen, worden aangestuurd door lokale coördinatoren, die bijvoorbeeld verantwoordelijkheid dragen voor een specifiek geografisch gebied. Indien er sprake is van een omvangrijke organisatie kan boven dit niveau sprake zijn van verdere gelaagdheid. Op het hoogste niveau zit een kleine groep organisatoren. Zij dragen de uiteindelijke verantwoordelijkheid over het geheel aan gebezigde fraudepraktijken. Er bestaan sterke aanwijzingen dat veel groepen worden ondersteund door een of enkele zogenaamde domeinexperts. Dit wordt onder andere afgeleid uit het feit dat ze op de hoogte zijn van uiterst gedetailleerde kennis ten aanzien van telecomdiensten, infrastructuur,

³⁹ De geïnterviewde experts geven aan dat sprake is van complexe, internationale organisaties met een groot aantal actoren op alle niveaus. Op het niveau van organisatoren zijn voldoende middelen beschikbaar om waar nodig substantiële voorinvesteringen te doen. De sterk gelaagde structuur zorgt er bovendien voor dat hoofddaders meestal buiten schot blijven (Kerkdijk et al., 2006).

businessmodellen en interne bedrijfsprocessen. Mogelijk zijn deze experts op enig moment werkzaam geweest in de telecombranche (Kerkdijk et al., 2006).

Een en ander wordt bevestigd door experts en bestuurlijke rapportages (Politie IJsselland, BRNON, 2008). Uit de opsporingsonderzoeken kwam het volgende beeld naar voren: de personen die zich met telecomfraude bezighouden zijn van zowel autochtone als allochtone afkomst. Opvallend is dat verdachten met een Pakistaanse⁴⁰ herkomst relatief vaak voorkomen, en het gaat hier dan veelal om hooggeschoolde ICT'ers. Een groep is georganiseerd in cellen met een hoofd, twee secondanten en een aantal katvangers. Deze groep verleent de organisatie hand- en spandiensten door met valse identiteitsbewijzen abonnementen af te sluiten in allerlei landen. Het werkgebied is internationaal: de groepen werkten onder anderé in Duitsland, Spanje, Frankrijk, België en Slowakije.

Op individueel niveau gaat het vaak over katvangers die gebruikt worden bij verschillende fraudeconstructies. De katvangers worden meestal actief benaderd door ronselaars die hen onder dwang of tegen een geringe vergoeding een abonnement laten afsluiten. De telefoon en simkaart worden dan bij een ronselaar ingeleverd zodat deze voor grootschalige exploitatie kan worden ingezet. Hierbij richt men zich voornamelijk op jongeren, vaak scholieren die net 18⁴¹ zijn geworden, en verslaafden. Deze doelgroepen zijn in de meeste gevallen niet bekend bij de Stichting Preventel⁴², waardoor zij bij het afsluiten van een abonnement nauwelijks op hindernissen stuiten (Kerkdijk et al., 2006).

Naast het afsluiten van een telefoonabonnement worden deze groepen ook bewogen om bankrekeningen te openen om er crimineel geld op te zetten. Het afsluiten van de abonnementen gebeurt met valse of echte identiteitspapieren. In het laatste geval doen katvangers na hun abonnementsaanvraag geregeld aangifte van verlies of diefstal van bedrijfspapieren. Zij krijgen het advies aan te geven dat zij door bedreiging of afpersing gedwongen waren om abonnementen af te sluiten. Dit bleek in de onderzochte gevallen vaak niet te

⁴⁰ Voorbeelden van betrokkenheid van specifieke Pakistaanse csv's zijn de Griekenlandzaak in 1999/2000, het simkaart fraude-onderzoek in 2001, het PABX-fraude onderzoek in 2005 en het Jupiter-onderzoek in 2007.

⁴¹ Voor het aanvragen van een abonnement geldt een minimumleeftijd van 18 jaar. Personen jonger dan 18 jaar dienen bij de aanvraag een schriftelijke machtiging van ouders of verzorgers te overhandigen.

⁴² De stichting Preventel is een samenwerkingsverband tussen aanbieders van telecommunicatiediensten en dient een maatschappelijk belang: het voorkomen dat personen en bedrijven verplichtingen voor het gebruik van telecommunicatiediensten aangaan die zij niet kunnen dragen (bron: www.preventel.nl).

kloppen. Op deze wijze werden door een organisatie honderden abonnementen afgesloten in binnen- en buitenland. Naast het ronselen van katvangers wordt er binnen telecombedrijven naar handlangers gezocht.

Met de verkregen simkaarten wordt vooral in het weekend, in eigen beheer en in georganiseerd verband, gebeld naar diverse 090X- betaalnummers, dat zijn betaalde servicenummers. Deze nummers, die via de OPTA worden verkregen⁴³, zijn direct of indirect in beheer van dezelfde organisatie. Om de criminele activiteiten af te schermen switcht de organisatie regelmatig van platformhouder, 090X-betaalnummer-exploitant (nummerhouder) en van 090X-betaalnummer. Wanneer de telecomoperators constateren dat simkaarten excessief belgedrag naar 090X-betaalnummers vertonen en vastgesteld wordt dat er sprake is van frauduleus verkregen simkaarten, worden deze geblokkeerd.

Telecomfraude kan in zijn meest eenvoudige vorm ook als solopraktijk plaatsvinden. In deze gevallen betreft het doorgaans incidentele fraudeurs, die voor eigen gebruik telecomdiensten proberen te verkrijgen zonder hiervoor te betalen. Daarbij maken zij meestal gebruik van abonnementsfraude. Uit interviews met experts maken wij op dat solopraktijken maar een klein aandeel vormt van de totaal geleden schade.

Bij telecomfraude wordt gebruik gemaakt van onjuiste uittreksels van de Kamer van Koophandel of wordt een bedrijf gebruikt dat inmiddels failliet is vanwege het niet voldoen aan de betalingsverplichting. Voor telecomaanbieders is het lastig om hier het hoofd aan te bieden, omdat het op dit moment niet controlebaar is of achter een uittreksel een bonafide of malafide bedrijf zit. Dit probleem is door het verdwijnen van de woonadresgegevens uit het uittreksel vergroot, omdat de telecomaanbieders de bestuurders achter een bedrijf nu niet meer kunnen controleren in de bestaande fraudesystemen (Kabki et al., 2011).

Daders van telecomfraude lijken in veel gevallen ook betrokken bij andere vormen van criminaliteit (Leipoldt & Laning, 2006). Meest in het oog springend zijn heling en witwaspraktijken. Het witwassen via telecomdiensten kan op verschillende manieren plaatsvinden. Een voorbeeld hiervan is het aankopen van grote hoeveelheden beltegoed en deze vervolgens via een PRS-constructie incasseren. De mobiele toestellen die bij de abonnementen worden geleverd,

⁴³ De meeste aanvragen van 0900-nummers lopen in de praktijk via de platformhouder die ook de technische en administratieve afhandeling verzorgt. Zij vragen de 0900-nummers in blokken aan, waardoor zij een reeks van deze nummers op de plank hebben liggen. Dit maakt het voor de feitelijke nummergebruiker mogelijk om controle door de OPTA te omzeilen.

verdwijnen voor een groot deel in het gangbare helingcircuit. Verder zijn frauduleus verkregen telecomabbonementen gewild bij criminelen vanwege de anonimiteit die deze hen verschaffen. Ook wordt al enige tijd gesuggereerd dat telecomfraude vaak samengaat met drugshandel en zou worden aangewend als financieringsbron voor terroristische activiteiten. Dit laatste kon in het onderzoek van TNO (Kerkdijk et al., 2006) niet worden onderbouwd. In een van de afgesloten zaken werden echter aanwijzingen aangetroffen dat een aantal van de verdachte Pakistani betrokken waren bij de aanslag in Mumbai en de financiering van Al Qaida. In dit samenwerkingsverband werd door een aantal beluizen in Noord-Italië gebeld via gehackte centrales in Nederland en bleek een van de verdachten te beschikken over een wisselkantoor.

Voor een indicatie van de opbrengsten van een georganiseerde telecomfraude kan de zaak Jupiter als voorbeeld dienen (Politie IJsseland, BRNON, 2008). In Nederland is er in totaal voor een bedrag van vijf miljoen uitbetaald aan criminelen. Dit is slechts het topje van de ijsberg, omdat deze groep wereldwijd actief was en in vele landen inkomsten genereerde. Een van de hoofdverdachten van het samenwerkingsverband had een huis van zes ton, dat contant was betaald. Daarnaast had de groep luxegoederen, zoals sieraden, in zijn bezit ter waarde van 1 miljoen euro.

4.6.4 Maatschappelijke gevolgen

De financiële omvang van telecomfraude in Nederland wordt geschat op minimaal 40 miljoen euro. Verreweg het grootste deel van deze schade komt voor rekening van de telecoomaanbieders. De directe schade die zij ondervinden bestaat voornamelijk uit inkomstenderving als gevolg van rekeningen die niet geïnd kunnen worden of betalingen die zij moeten verrichten als gevolg van internationale interconnectieafspraken tussen telecomoperators⁴⁴. Indirect is telecomfraude schadelijk voor het imago van de sector. Hoewel het een omvangrijk bedrag betreft, kunnen de gevolgen voor de telecomsector niet als ernstig worden beschouwd, omdat het verlies ten opzichte van de totale omzet beperkt is.

Dit ligt anders bij bedrijven en particulieren. Bedrijven kunnen als gevolg van telecomfraude opdraaien voor flinke verliezen, en zelfs failliet gaan. Een

⁴⁴ Deze verplichting bestaat als gevolg van de afspraak dat (internationale) telecomoperators de gemaakte kosten aan elkaar vergoeden. Deze kosten worden gemaakt wanneer telefoonverkeer wordt overgedragen naar een volgende partner in de keten.

soortgelijk beeld is te zien bij particulieren die zijn geronseld om telefoon-abonnementen af te sluiten. Zij blijven als katvanger vaak zitten met fikse telefoonrekeningen. De impact van telecomfraude op bedrijven en particulieren kan in sommige gevallen ernstig zijn.

4.6.5 Criminaliteitsrelevante factoren

Binnen telecomfraude is, zoals bij zoveel fenomenen, een verschuiving naar het internet waar te nemen. In de afgelopen jaren zijn veel meer telefooncentrales aangesloten op het internet. Dit heeft bijgedragen aan de recente stijging van PABX-fraudes, aangezien het hacken van telefooncentrales steeds meer via het internet plaatsvindt. Wanneer deze ontwikkeling doorzet, zal dit mogelijk⁴⁵ leiden tot een toename van telecomfraude.

In de toekomst zal betalen via mobiele telefoons een impact hebben op telecomfraude. Telefonie en betalingsverkeer komen daardoor steeds meer in elkaars verlengde te liggen. Fenomenen als phishing, cybercrime en telecomfraude vertonen daardoor steeds meer overlap. Op dit moment is niet duidelijk in welke richting zich dit gaat ontwikkelen en of het tot een toename van een of meerdere vormen van fraude gaat leiden.

Tot slot zal de economische crisis ook mogelijkheden scheppen voor fraudeurs. Als gevolg van de oplopende werkeloosheid⁴⁶, met name onder jongeren, kunnen meer mensen in geldnood komen. Telecomfraudeurs zullen hierdoor waarschijnlijk makkelijker katvangers kunnen ronselen die voor een klein bedrag een abonnement voor hen afsluiten.

4.6.6 Verwachtingen

Er is weinig zicht op de omvang van telecomfraude, dat in 2006 werd geschat op minimaal 40 miljoen euro. Sindsdien zijn weinig cijfers beschikbaar die wijzen op een toe- of afname van deze criminaliteitsvorm. Volgens experts is het fenomeen echter zeker niet afgenomen de afgelopen jaren. Voor de toekomst verwachten zij zelfs een stijging.

⁴⁵ Dit is daarnaast nog afhankelijk van andere factoren zoals de mate van beveiliging. Hier zullen ook ontwikkelingen plaatsvinden zowel hard- en softwarematig als in het bewustzijn van gebruikers.

⁴⁶ Voor een onderbouwing hiervan, zie paragraaf 4.2.5.

Een verdere verplaatsing van (traditionele) telecomdiensten richting het internet, de invoering van het mobiel betalen en de impact van de economische crisis ondersteunen deze verwachting ten dele. Hoewel deze ontwikkelingen nieuwe mogelijkheden voor fraudeurs creëren, is moeilijk te bepalen of dit tot een (blijvende) stijging of slechts een verschuiving van telecomfraude zal gaan leiden. Het is daarom de verwachting dat telecomfraude de komende jaren minimaal gelijk zal blijven, zowel in omvang als in ernst.

4.6.7 Aanpak

De aanpak van telecomfraude gebeurt op dit moment voornamelijk vanuit de private sector. De sector richt zich zo veel mogelijk op preventie van fraude of het (vooraf) bepalen van kwetsbaarheden van nieuwe diensten. Het dynamische karakter van het fenomeen telecomfraude stelt beperkingen aan de mate waarin preventieve fraudebestrijdingsmaatregelen tot resultaat kunnen leiden. Bij de ontwikkeling van nieuwe diensten zijn de frauderisico's niet altijd goed te voorspellen. Bestrijding van telecomfraude zal dan ook altijd tot op zekere hoogte een reactief karakter hebben.

De aanpak is gebaat bij een nauwere samenwerking tussen marktpartijen, politie en overheid. Tot nu toe zijn afspraken om te komen tot een gezamenlijke aanpak vervat in het Handhavingsarrangement 2002 dat ondertekend is door de telecomoperators, het Parket-Generaal en het ministerie van Economische Zaken. Op dit moment (begin 2012) zijn gesprekken gaande om tot een herziening van dit convenant te komen naar voorbeeld van het onlangs afgesloten Verzekeringsconvenant. Het effect hiervan zal in de toekomst moeten blijken.

4.7 Verzekeringsfraude

De informatie in deze paragraaf is afkomstig uit interviews met vertegenwoordigers van het Verbond van Verzekeraars en het Fraudemeldpunt Noord- en Oost-Nederland. Daarnaast is gebruikgemaakt van brochures en een rapport van het Verbond van Verzekeraars, waarin omzet en fraudecijfers zijn gepubliceerd, en een Verzekeringsfraudebeeld dat recent door de BRNON is opgesteld.

4.7.1 Aard

Bij alle schade-, levens- en zorgverzekeraars, natura uitvaartverzekeraars en spaarkasbedrijven vindt fraude plaats. Verzekeringsfraude is het handelen met de opzet een verzekeraar te misleiden. Het kan op twee manieren plaatsvinden:

ten eerste bij het aanvragen van een verzekering. De fraudeur geeft een onjuiste voorstelling van de feiten, omdat anders de verzekeraar de verzekering niet of niet onder dezelfde voorwaarden/premie zal accepteren. Ten tweede bij het indienen van een claim. De fraudeur misleidt de verzekeraar, waardoor deze een uitkering doet die niet zou worden verstrekt bij een juiste opgave van de feiten.

Er bestaan verschillende vormen van misleiding. Fraudeurs claimen meer dan waar ze daadwerkelijk recht op hebben (majoreren), ze doen alsof de omstandigheden zodanig zijn dat deze onder de dekking vallen (fingeren), ze creëren opzettelijk omstandigheden die tot een uitkering leiden (ensceneren), of, tot slot, ze voldoen niet aan de mededelingsplicht, dat wil zeggen het doen afsluiten van een verzekering op grond van verkeerde of onvolledige informatie (Verbond van Verzekeraars, 2008). Onterechte claims leiden jaarlijks tot vele onterechte uitkeringen door verzekeraars.

4.7.2 Omvang

De geschatte omvang moet in het licht worden gehouden van de cijfers over verzekeringen. De Nederlandse verzekeraars hadden in 2009 een premieomzet van 78 miljard euro en keerden in totaal 70 miljard euro uit aan personen en bedrijven. Dit betekent dat de fraude afgerond 1,3 procent uitmaakt van hetgeen totaal is uitgekeerd.

Het Verbond van Verzekeraars schat dat 10 procent van de Nederlanders fraudeert en dat daardoor 900 miljoen euro per jaar ten onrechte wordt uitgekeerd: 400 miljoen per jaar bij fraude met particuliere motorrijtuigen, 300 miljoen per jaar aan bedrijfsverzekeringen, 135 miljoen aan inboedel- of opstalverzekeringen (particulier), 50 miljoen aan reisverzekeringen (particulier) en 15 miljoen aan overige verzekeringen (particulier) (Verbond van Verzekeraars, 2011). Deze cijfers lopen in de pas met andere Europese landen, zoals Groot-Brittannië en Duitsland.

Bij het Fraudemeldpunt Noord- en Oost-Nederland werd in 2010 totaal 25 miljoen euro fraude met verzekeringen gemeld. Maar daar komen alleen meldingen binnen van fraudezaken die daadwerkelijk gedetecteerd zijn, dit betekent dat lang niet alle fraudegevallen worden gemeld. Uit een in 2011 uitgevoerd dossieronderzoek naar fraude door blikschadeherstellers bleek dat in deze sector de schade alleen al 70 miljoen euro bedraagt. Hoewel dit een indicatie is dat verzekeraars meer schade hebben dan strikt wordt gemeld, blijft het geschatte bedrag door het Verbond van Verzekeraars moeilijk te onderbouwen op basis van werkelijke zaken (BRNON, 2012). Zoals het Verbond van

Verzekeraars schetst 'alleen het topje van de ijsberg is zichtbaar, onzichtbaar blijft het deel onder water'.

De omvang wordt in het *Verzekeringsfraudebeeld* (BRNON, 2012) fors maar stabiel genoemd; er zijn geen onbetwiste cijfers beschikbaar over de schade door verzekeringsfraude. Het grote aantal soorten verzekeringen en de vele vormen van fraude bemoeilijken het bepalen van de omvang van verzekeringsfraude. Tromp et al, (2010) kwamen tot een soortgelijke conclusie op basis van onderzoek naar het voorkomen van een aantal vormen van fraude, waaronder verzekeringsfraude.

4.7.3 Criminele samenwerkingsverbanden

Verzekeringsfraude speelt zich, in vergelijking tot andere hoofdvormen van fraude, voornamelijk af op Nederlands grondgebied, uitgevoerd door in Nederland wonende daders.

Zowel individuele consumenten als criminele samenwerkingsverbanden bezondigen zich aan fraude. Op basis van onderzoek in opdracht van het Verbond van Verzekeraars zou iets minder dan de helft van de omvang bij schadeverzekeringen uit georganiseerde criminaliteit ontstaan. Iets meer dan de helft wordt veroorzaakt door gelegenheidsfraudeurs. Het gaat hier om geschatte aantallen (CMC, 2005). Het Verbond van Verzekeraars keek in 2006 naar 100 werkelijk uitgevoerde fraudes met schadeverzekering en komt lager uit voor de georganiseerde criminaliteit (ongeveer 20%). Het gaat hier dan om de aantallen die, zoals ze zelf aangeven, zichtbaar zijn; wat onder water zit, blijft onzichtbaar. Een kenmerk van deze criminele samenwerkingsverbanden is dat het, zoals één van de experts bevestigde, meestal om slimmere fraudeurs gaat, maar details daarover ontbreken. Ook is geconstateerd dat misbruik wordt gemaakt van katvangers, jonge studenten, zoals ook bij veel andere vormen van fraude.

Uit de analyse van de 30.000 aangiften, die wij zelf uitvoerden (hoofdstuk 3), komen 142 aangiften naar voren die betrekking hebben op verzekeringsfraude. Eén cluster van vijf aangiften is terug te voeren op een groep daders die fraudeerde met voertuigen en elektrische fietsen. Details over het samenwerkingsverband komen in deze aangiften niet voor.

4.7.4 Maatschappelijke gevolgen

De financiële omvang van fraude bij schadeverzekeringen wordt geschat op 900 miljoen euro per jaar. Ofschoon dit een fors bedrag is, is het gering in verhouding tot hetgeen wordt uitgekeerd. Het frequent voorkomen van verzekeringsfraude heeft echter ook maatschappelijke gevolgen. Het kan leiden tot een vervagend normbesef, waardoor voor sommige mensen de drempel om tot fraude over te gaan, wordt verlaagd. Deels dragen verzekeringsmaatschappijen zelf bij aan deze gevolgen door fraudegevoelige producten in de markt te zetten. De financiële schade die verzekeraars lijden, wordt doorberekend in de vorm van premieverhogingen of verhogingen van het eigen risico voor alle verzekerden. Hierdoor komen de financiële gevolgen uiteindelijk bij de verzekerden te liggen, en dat kan op termijn ondermijnend werken.

4.7.5 Criminaliteitsrelevante factoren

Een criminaliteitsbevorderende factor is de lage pakkans. Jaarlijks worden 3000 tot 4000 zaken door de verzekeraars gemeld aan het Verbond van Verzekeraars. Deze zaken worden geselecteerd door een systeem van indicatoren dat gezamenlijk door verzekeraars wordt gehanteerd, of verzekeraars maken zelf een selectie op basis van eigen criteria. De geselecteerde zaken gaan via het Verbond van Verzekeraars door naar het OM in de vorm van een melding, en vijftien tot twintig van deze zaken worden strafrechtelijk afgedaan. Bij de politie is te weinig prioriteit en capaciteit om alle zaken op te pakken. Hierdoor blijven veel zaken liggen of worden niet goed uitgezocht. De pakkans is in 1994 berekend op minder dan één procent (CMC, 2005).

Verzekeraars geven aan dat veel problemen kunnen worden voorkomen wanneer ze inzicht zouden krijgen in de Gemeentelijke Basis Administratie, zodat ze kunnen controleren of naam en adres overeenkomen. Daarnaast heeft internet, zoals bij andere vormen van fraude, frauderen gemakkelijker gemaakt, terwijl frauderen met verzekeringen al heel gemakkelijk wordt genoemd door een expert. Via internet kunnen verzekeringen afgesloten worden waar nog minder dan voorheen controle op plaatsvindt (bv. op identiteitsgegevens). Volgens een expert wordt dit versterkt doordat te weinig controle wordt uitgeoefend door verzekeringsmaatschappijen. Bij schadeverzekeringen doet de tegenstrijdige situatie zich voor dat verzekeraars minder winst maken op schades en daardoor minder investeren op betere risicoanalyses (De Vos, 2011).

Om de aanpak te verbeteren hebben de politie, het OM, Zorgverzekeraars Nederland en het Verbond van Verzekeraars in maart 2011 het Convenant

Aanpak Verzekeringsfraude afgesloten ten behoeve van het uitwisselen van informatie, het stellen van prioriteiten en het opzetten van interventie-strategieën. De mogelijkheden om op te treden waren tot nu toe beperkt. Bovendien bestaat het beeld dat keurige mensen niet frauderen, en staat fraudedetectie nog in de kinderschoenen (vergeleken bij de frauderisicoanalyse / profilering bij creditcardmaatschappijen).

In de komende jaren moet blijken of de economische crisis zal leiden tot een toename van het aantal verzekeringsfraudes. In de Verenigde Staten lijkt dat al het geval te zijn: de schade wordt vaker overdreven en er wordt meer geclaimd. Er komen steeds vaker frauduleuze meldingen binnen van autodiefstal en brandstichting. Ook stegen andere soorten claims, zoals van hagelschade, gefingeerde valpartijen en brandschade. Autoschades maakten het grootste deel uit van alle schadeclaims, en ook deze stegen (Tromp et al., 2010).

4.7.6 Verwachtingen

De omvang van verzekeringsfraude wordt hoog maar stabiel genoemd. In de ernst zal de komende jaren weinig veranderen. Trends konden door een fraude-expert van het Verbond van Verzekeraars niet worden benoemd, maar wel werd opgemerkt dat bij sommige verzekeringsmaatschappijen medewerkers op cruciale functies bedragen uitbetalen op door criminelen gedirigeerde rekeningen. Deze rekeningen staan op naam van katvangsters. Er lopen een aantal opsporingonderzoeken, maar er is te weinig capaciteit om een en ander goed uit te zoeken.

Daarnaast wordt fraude met verzuimverzekeringen gemeld als nieuw fenomeen: bedrijven worden opgezet en nemen (op papier) jonge, goed opgeleide mensen in dienst, die vervolgens spoedig ziek worden en waarvoor dan wordt gedeclareerd.

Steeds meer verzekeringsaanvragen en claims zullen via internet worden afgehandeld, dit werkt fraude in de hand. Of de economische crisis het doen van valse claims in de hand werkt, moet nog blijken.

4.7.7 Aanpak

De verzekeraars hebben al diverse maatregelen genomen, zoals de oprichting van een kenniscentrum, het Centrum Bestrijding Verzekeringsfraude (CBV), dat ook als aanspreekpunt fungeert. Verder nemen de verzekeraars deel aan het Nationaal Platform Criminaliteitsbeheersing (NPC), een samenwerkingsverband

tussen overheid en bedrijfsleven (gericht op criminaliteitsvormen waarvan het bedrijfsleven slachtoffer is).

In het Convenant Aanpak Verzekeringsfraude richten de samenwerkende partijen zich meer op de bestrijding van verzekeringsfraude in brede zin (alle sectoren) dan tot nu toe het geval was. Een eerste stap is zicht krijgen op de aard en omvang van verzekeringsfraude. Om dit te verwezenlijken is door de BRNON, het Verbond van Verzekeraars en Zorgverzekeraars Nederland een gezamenlijk verzekeringsfraudebeeld opgesteld (BRNON, 2011). In 2012 verschijnt dit rapport voor de tweede keer. Ook zullen alle fraudemeldingen van de verzekeraars centraal geregistreerd en geanalyseerd worden bij het Fraudemeldpunt Noord- en Oost-Nederland. Daarnaast zullen zij een integrale aanpak ontwikkelen die bestaat uit preventie, bewijsvoering en civiel- en strafrechtelijke afhandeling. Preventie en detectie staan in de aanpak voorop. Veel zaken worden bijvoorbeeld in het stadium van aanvragen al afgewezen. Daarbij handelen verzekeraars lichte fraudegevallen civielrechtelijk af en vindt in beginsel strafrechtelijke afhandeling plaats van zware fraudegevallen (onder andere waar sprake is van georganiseerde criminaliteit).

Op basis van het *Verzekeringsfraudebeeld* (BRNON, 2012) spreken de convenantspartijen af zich de komende jaren op de volgende vormen van georganiseerde verzekeringsfraude te richten (in het rapport worden dit de prioriteitsfenomenen van 2012 genoemd):

Autoschadeherstelfraude: het gaat hier vooral om glasschadeherstelbedrijven, vaak te vinden op parkeerterreinen, die te hoge bedragen opvoeren voor slechte of niet uitgevoerde reparaties: dit is een ontwikkeling van de laatste twee jaar. De frauduleuze inkomsten van een bedrijf werden geschat op 30 miljoen euro.

De Bovenregionale Recherche Noord- en Oost-Nederland (BR NON) hield eind januari vier mannen uit Emmen aan. De Emmenaren zijn de hoofdverdachten in een onderzoek naar verzekeringsfraude. Zij dienden facturen in bij verschillende verzekeringsmaatschappijen voor het herstel van autoruitschade. De BRNON startte het onderzoek naar aanleiding van een fraudemelding van het Verbond van Verzekeraars. Het Verbond zag een sterke stijging in claims op het gebied van autoruitschade en schakelde de politie in. Het daaropvolgende onderzoek leidde in juli 2011 tot doorzoeken in diverse panden in Emmen en Duitsland. Het ging om drie woningen en drie bedrijfspanden. De doorzoeking in Duitsland vond plaats, omdat via dit land geld werd wit gewassen. Tijdens de doorzoeken werd administratie in beslag genomen. Ook werd er beslag gelegd op vijf woningen, twee auto's, geld en goud. In totaal vertegenwoordigen de in beslag genomen goederen een waarde van 1 miljoen euro.

Website Politie Drenthe, 22 februari 2012

Inkomensverzekeringsfraude: bij deze vorm van fraude sluit een onderneming een inkomensverzekering af voor haar werknemers. Vervolgens meldt de onderneming dat een werknemer ziek is en vraagt de inkomensverzekeraar het vaak hoge salaris door te betalen. Men maakt gebruik van een rechtspersoon en fake werknemers.

4.8 Faillissementsfraude

Deze paragraaf is onder meer gebaseerd op het rapport *Fraude en misbruik bij faillissement* (Knegt, Beukelman, Popma, Van Willigenburg & Zaal, 2005). Sinds het verschijnen van dit rapport heeft geen update meer plaatsgevonden. Vorig jaar heeft het CBS het rapport *Faillissement: oorzaken en schulden 2011* gepubliceerd (De Boer & Lalta, 2011), waaruit cijfers over de omvang gedestilleerd konden worden. Informatie in dit hoofdstuk is ook afkomstig uit het rapport *Preventieve maatregelen horizontale fraude* (Tromp, et al., 2010) en een interview met een expert bij de FIOD-ECD Zwolle. Andere experts op dit terrein (BR Zuid-Nederland, Kenniskring Faillissementsfraude Politieacademie en het ministerie van Veiligheid en Justitie) waren nog niet in staat informatie te leveren.

4.8.1 Aard

Onder een faillissement wordt het volgende verstaan:

Ingevolge het eerste artikel van de Faillissementswet (Fw) wordt de schuldenaar die in de toestand verkeert dat hij heeft opgehouden te betalen, hetzij op eigen aangifte, hetzij op verzoek van een of meer zijner schuldeisers, bij rechterlijk vonnis in staat van faillissement verklaard. Door de faillietverklaring verliest de schuldenaar van rechtswege de beschikking en het beheer over zijn tot het faillissement behorend vermogen (artikel 23 Fw). Tijdens de procedure van het faillissement worden de (eventueel) nog aanwezige baten gelijkelijk onder de schuldeisers verdeeld, behoudens de door de wet erkende redenen van voorrang. De curator is belast met het beheer en de vereffening van de failliete boedel (artikel 68 Fw).

Wanneer een faillissement opzettelijk wordt misbruikt om financieel gewin te behalen, is sprake van faillissementsfraude, en de definitie hiervan luidt:

Een opzettelijke handeling vóór of tijdens een faillissement waarbij door het geven van een onjuiste voorstelling van zaken een gepretendeerde rechtvaardiging voor deze handeling ontstaat, waardoor een onrechtmatig voordeel wordt verkregen en faillissementsschuldeisers opzettelijk of culpoos (verwijtbaar) kunnen worden benadeeld (Tromp et al., 2010).

Lang niet altijd zijn alle uitgevoerde handelingen strafbaar of onrechtmatig. Het is vaak het geheel van handelingen dat als onbehoorlijk kan worden aangemerkt, waardoor er bijvoorbeeld sprake kan zijn van onbehoorlijk bestuur. In dat geval kan een aanpak civielrechtelijk zijn (Burgerlijk Wetboek of de Faillissementswet).

Faillissementsfraude kent in principe twee hoofdvormen:

1. Aan de hand van een vooropgezet plan wordt een onderneming opgezet en gefailleerd om de schuldeisers door middel van faillissement te benadelen;
2. Een bedrijf gaat (niet vooropgezet) failliet en vlak voor en/of tijdens het faillissement wordt getracht illegitiem voordeel te behalen door activa aan de boedel te onttrekken. Voorbeelden hiervan zijn verduistering van activa via gefingeerde nota's of verkoop van activa onder de marktwaarde (Knegt, et al., 2005).

De vijf verdachten die door de FIOD-ECD en de BR NON zijn aangehouden zouden in georganiseerd verband van 2008 tot op heden bedrijven opgekocht hebben die nagenoeg bankroet waren. Ze kwamen aan de bedrijven door middel van advertenties in kranten en via internetsites. Ze worden verdacht van faillissementsfraude bij vijf rechtspersonen in Nederland. Het gaat om een slachterij uit 's-Graveland, een groothandel in sanitaire artikelen uit gemeente Haaren, een internationaal transportbedrijf uit Almelo en twee rechtspersonen bij een financieel adviesbureau uit Goes. De verdachten kochten op papier de bedrijven op voor 1 euro, terwijl het vermoeden is dat de eigenaren van de bedrijven tussen de 10.000 en 25.000 euro betaalden aan de verdachten om van hun 'probleem BV's' af te komen. Vervolgens werden de nog aanwezige bezittingen van de bedrijven te gelde gemaakt. Dit ging ten koste van de schuldeisers, die nauwelijks of geen geld meer uit de failliete boedel konden halen.

Website Rijksoverheid (8 juli 2011)

Het hoofddoel van faillissementsfraude is onrechtmatig geld aan een onderneming onttrekken. Daarbij kan gebruik worden gemaakt van de volgende modi operandi:

- *Hoge privéonttrekkingen*

De meest eenvoudige manier is door hoge bedragen te onttrekken aan de bv voor privédoeleinden, en zich daarbij te verschuilen achter een onoverzichtelijke administratie of een die niet aanwezig is. Als de eigenaar vervolgens ook in privé geen verhaal biedt, wordt het lastig om tot aansprakelijkstelling over te gaan.

- *Lage vergoedingen*

Een andere manier is het inhuren van zusterbv's, waarbij te hoge of te lage vergoedingen worden doorberekend, waardoor de ene bv veel winst maakt en de andere failliet gaat. Een inhurende bv betaalt bijvoorbeeld een dubbel uurloon aan werknemers uit een personeels-bv, maar brengt slechts de helft van de gewerkte uren in rekening. Daardoor ontstaat belastingvoordeel, waardoor de inhurende bv minder kosten maakt en dus meer winst, terwijl de ingehuurde bv op termijn failliet gaat.

- *Katvangers*

Een niet ongebruikelijke techniek bij faillissementsfraude is het inschakelen van een 'katvanger'. Een katvanger is een persoon die, veelal tegen betaling, een vennootschap op zijn naam zet of laat zetten en op papier bestuurder is. In de

praktijk wordt het bedrijf dan gerund door een partij achter de schermen. Deze partij bestelt op naam van de katvanger voor veel geld goederen, waarvoor na ontvangst niet wordt betaald (een vorm van flessentrekkerij). Vervolgens laat de bestuurder de bv 'ploffend', en blijft zelf buiten schot, terwijl de katvanger geen vermogen heeft.

- *Postbus-bv's*

In sommige gevallen 'runt' een katvanger een flink aantal postbusbv's. In het rapport van Knecht et al. wordt het voorbeeld genoemd van een postbus waarachter zich 140 bedrijven bevinden. Negentig hiervan waren inmiddels opgeheven of ontbonden.

Dit zijn slechts een aantal modi operandi, er kan niet gesproken worden van één vorm om te frauderen. Knecht et al. geven aan dat er veel verschillende verschijningsvormen van faillissementsfraude zijn en dat in de bestudeerde dossiers de meeste vormen niet meer dan enkele keren voorkwamen. Tromp et al. noemen faillissementsfraude zeer dynamisch, aangezien de fraudeurs de modus operandi steeds veranderen en aanpassen aan de bestaande detectie en repressie.

4.8.2 Omvang

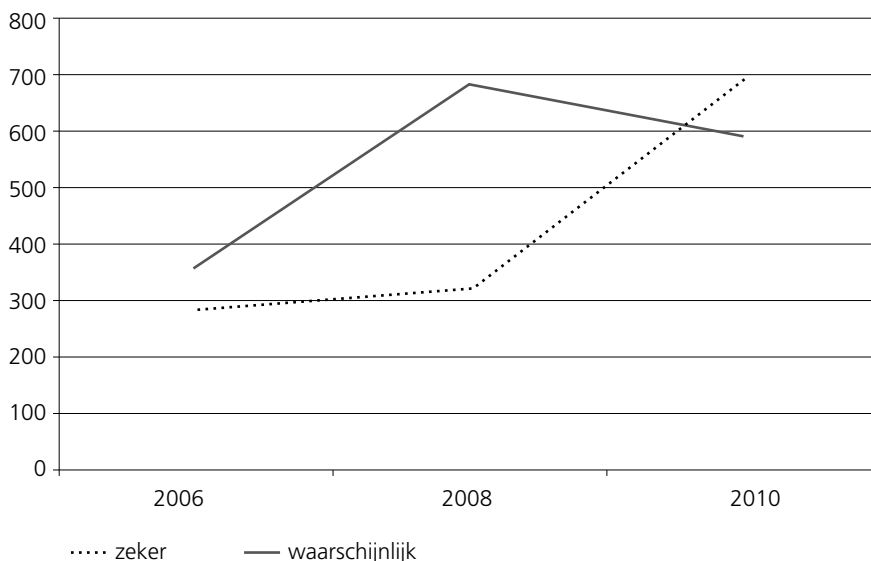
Twee bronnen die inzicht verschaffen in de omvang van faillissementsfraude zijn het CBS en het WODC. Het CBS houdt statistieken van faillissementen bij en registreert of sprake is van fraude. Het WODC analyseerde 868 dossiers, en schreef een rapport over aard en omvang (Knecht et al., 2005).

De cijfers van het CBS (De Boer & Lalta, 2011) zijn gebaseerd op dossiers van curatoren waarop enige actie is ondernomen. In de onderstaande grafiek is te zien hoe de zekere⁴⁷ en waarschijnlijke strafbare benadeling van schuldeisers zich voor de jaren 2006 tot en met 2010 heeft ontwikkeld. Het gaat hier om onbetaald gebleven schulden bij fraude. Deze cijfers moeten in het licht worden gehouden van het totaal aantal faillissementen. In 2006 werden 9.665 faillissementen uitgesproken en in 2010 waren dat er 8.400.

⁴⁷ Het CBS onderscheidt zekere en waarschijnlijke benadeling van schuldeisers. In beide gevallen gaat het om bestuurdersaansprakelijkheid, onrechtmatig of paulianeus handelen (ongeoorloofde vorderingen); bij zekere benadeling is er een schikking of succesvolle procedure geweest, bij waarschijnlijke benadeling bleef het bij aanwijzingen.

Figuur 11

Onbetaald gebleven schuld bij fraude (in miljoenen euro's)



In het figuur is zichtbaar dat vanaf 2006 de totale onbetaald gebleven schuld bij fraude toeneemt. De toename in 2008 kwam voornamelijk uit een stijging in het aantal waarschijnlijk strafbare benadelingen van schuldeisers. In 2006 is bij 12,1 procent van de zaken sprake van een waarschijnlijke strafbare benadeling van schuldeisers, wat neerkomt op een onbetaalde schuld van 352 miljoen euro. In 2010 is dit gestegen naar 593 miljoen euro. In 2006 is bij 9,7 procent van de beëindigde faillissementen sprake van zekere strafbare benadeling van schuldeisers. De onbetaald gebleven schuld van deze zaken is 284 miljoen euro, maar steeg in 2010 naar 688 miljoen euro.

Van de onbetaald gebleven schuld van de in 2010 beëindigde faillissementen is 33 procent toe te schrijven aan zaken met zekere en waarschijnlijke strafbare benadeling van schuldeisers (respectievelijk 17,8 en 15,3 procent). Voor het grootste deel, bijna 84 procent in 2010, zijn bij deze faillissementen besloten vennootschappen betrokken (De Boer & Lalta, 2011).

Bij de zaken waarbij zeker sprake was van strafbare benadeling bleef in 2010 gemiddeld 993.000 euro aan schulden onbetaald als gevolg van fraude. In 2008 was dat nog 586.000 euro per zaak. Bij de zaken waarbij sprake was van

waarschijnlijke strafbare benadeling is in 2010 gemiddeld 854.000 euro aan schulden onbetaald gebleven. In 2008 was dit nog gemiddeld 1.244.000 euro per zaak (De Boer & Lalta, 2011).

Deze cijfers laten zien dat bij een gemiddelde faillissementsfraude grote onbetaalde bedragen gemoeid zijn. Daarbij dient opgemerkt te worden dat bij een beperkt aantal faillissementen hele hoge bedragen voorkomen, waardoor het gemiddelde omhoog getrokken wordt. Bij deze zaken is zeer waarschijnlijk sprake van georganiseerde faillissementsfraude.

Knegt et al. vonden in een kwart van de 868 bestudeerde dossiers in meer of minder mate fraude. Zij kwamen op basis hiervan uit op een schadebedrag van in totaal 220 miljoen euro, en noemden dat een voorzichtige raming. Zij extrapoleerden de schadebedragen per faillissement naar alle faillissementen van vennootschappen, en kwamen zodoende op een totale geschatte schade over 2004 van circa 1,7 miljard euro.

In dit deelrapport baseren we ons op de cijfers van het CBS, omdat deze recentelijk zijn vastgesteld en bovendien gebaseerd zijn op dossiers van curatoren. Op basis van deze cijfers bedraagt de financiële schade uitgedrukt in onbetaalde schuld in 2010 ruim één miljard euro. Ondanks dit enorme bedrag noemt het CBS dit een onderschatting aangezien bij het berekenen van de schuldbedragen gebruik is gemaakt van de vorderingen die de crediteuren hebben ingediend bij de curator. In veel gevallen nemen crediteuren echter niet de moeite om een vordering in te dienen, als zij het vermoeden hebben dat het hen in financieel opzicht weinig zal opleveren.

Naast deze cijfers zouden aangiften en informatie over uitgevoerde onderzoeken enige indicatie over de omvang moeten geven.

Uit de analyse van de aangiften, zoals die is gedaan in hoofdstuk 3, blijkt dat faillissementsfraude slecht wordt geregistreerd. Faillissementsfraude wordt in de aangiften geregistreerd onder de juridische term bankbreuk⁴⁸. In de periode september 2010- 2011 is hiervan veertien keer aangifte gedaan bij de regio-korpsen. Uit een korte inventarisatie blijkt dat drie hiervan inhoudelijk over

⁴⁸ In de politiesystemen wordt een onderscheid gemaakt tussen eenvoudige en bedrieglijke bankbreuk, waarbij globaal genomen bij de eerste vorm in mindere mate sprake is van opzet en bedrieglijk handelen dan bij de tweede vorm.

faillissementsfraude gaan. De overige elf gingen over andere vormen van fraude, namelijk fraude met internetbankieren, pinpasfraude en skimmen.

Met betrekking tot het aantal aangiften ziet een expert van de FIOD-ECD een toename, maar verklaart dit uit het verlagen van de drempel voor curatoren om aangifte te doen⁴⁹.

De Fraudemeldpunten waren niet in staat om een overzicht te genereren van het aantal meldingen over faillissementsfraude. De oorzaak hiervan, onder meer wisselende registratie, geen uitwisseling en recentelijk de doorontwikkeling van de FMP's, is al geschetst in paragraaf 2.7. Ook het OM was niet in staat een overzicht te genereren van het aantal faillissementsfraudezaken dat binnenkomt en uiteindelijk onder de rechter komt.

De registratie van aangiften en meldingen bij de verschillende instanties is gebrekkig. Ook geeft het aantal uitgevoerde onderzoeken slechts een beperkt inzicht in de omvang van faillissementsfraude. Zo kreeg de FIOD-ECD 55 complexe zaken binnen in 2011. Bij 35 zaken was sprake van in totaal 150 faillissementen; negentien zaken werden afgerond. Deze aantallen zeggen weinig over de omvang van faillissementsfraude, maar meer over de beschikbare capaciteit.

Met betrekking tot uitgevoerde onderzoeken meldt een expert van het Fraudemeldpunt Noord- en Oost-Nederland dat het aantal grote fraudezaken stabiel bleef, terwijl het aantal kleine fraudezaken toenam, evenals het aantal vonnissen. Ook steeg het totaal aantal faillissementen, niet alleen als gevolg van de economische crisis, maar ook doordat het aantal starters was toegenomen. Daarnaast laten de cijfers van het CBS zien dat de totaal onbetaald gebleven schuld met een strafbare benadeling fors is gestegen, als ook het gemiddelde onbetaalde bedrag met strafbare bepaling per faillissement. Het lijkt erop dat vooral het aantal niet vooropgezette (incidentele) fraudes is gestegen. Dit aandeel wordt groter, omdat door de economische crisis meer bedrijven in de problemen kunnen komen, waardoor meer kans op frauderen ontstaat. Mogelijk is hierbij vooraf geen sprake van opzet, maar het is lastig om daar concrete uitspraken over te doen.

⁴⁹ Sinds 2008 kunnen curatoren een vergoeding declareren voor uren die zijn besteed aan het doen van aangifte. Dit had een dermate groot effect dat de regels omtrent de vergoeding inmiddels zijn aangescherpt. Uitbetaling vindt alleen nog plaats wanneer de aangifte leidt tot opsporing.

De geregistreerde aangiften en het aantal gedraaide onderzoeken zijn op dit moment niet geschikt als indicatie voor de omvang van faillissementsfraude. Knecht et al. gaven in hun rapport in 2005 al aan dat geen overzicht bestaat van het aantal faillissementsfraudes in Nederland. Helaas is hierin de afgelopen jaren weinig verandering gekomen.

4.8.3 Criminele samenwerkingsverbanden

Bij faillissementsfraude kunnen beroepsfraudeurs worden onderscheiden, die gebruik maken van katvangers en rechtspersonen, en gelegenheidsfraudeurs. De FIOD-ECD hanteert een top 6 van fraudeurs, en daarin staan (meestal) katvangers die de meeste rechtspersonen op naam hebben. De FIOD-ECD richt zich voornamelijk op deze katvangers, veelplegers en recidivisten. Het zijn vooral de beroepsfraudeurs die katvangers gebruiken om zelf buiten beeld te blijven en voor wie het faillissement een instrument is om op onrechtmatige wijze vermogen aan de boedel te onttrekken. Zij doen dit om een aantal redenen: door katvangers in te zetten verhullen zij hun identiteit en strooien de opsporing zand in de ogen. Daarnaast ontlopen fraudeurs persoonlijke aansprakelijkheden door schuil te gaan achter (buitenlandse) rechtspersonen. Bijvoorbeeld de faillissementsfraudeur of de flessentrekker die crediteuren op een dood spoor zet door vermogen onder te brengen in zeer gesloten rechtsvormen en jurisdicties (Kabki et al., 2011). Uit de statistieken van het CBS blijkt dat grotendeels sprake is van misbruik van bv's. Over de samenstelling van de criminele samenwerkingsverbanden die op deze wijze te werk gaan, is weinig bekend. Waarschijnlijk zijn tien à vijftien beroepsfraudeurs actief in Nederland en trekt een beperkt aantal op de achtergrond aan de touwtjes. Het is niet bekend hoeveel katvangers worden ingezet bij deze vorm van fraude. De FIOD-ECD geeft aan over onvoldoende middelen te beschikken om een goed overzicht te maken.

Uit een inventarisatie van criminele samenwerkingsverbanden over het jaar 2011 bleek dat zes zich bezighielden met faillissementsfraude. De groeperingen bestonden voornamelijk tot volledig uit leden van Nederlandse herkomst. Vier maakten gebruik van rechtspersonen. Bij één samenwerkingsverband werd het wederrechtelijk verkregen voordeel geschat op 2,2 miljoen euro. Vijf criminele samenwerkingsverbanden hielden zich bezig met flessentrekkerij. In beide gevallen, faillissementsfraude en flessentrekkerij, werden goederen op naam van de bv's besteld, waarvoor vervolgens niet werd betaald. Of de bv's bij flessentrekkerij bleven bestaan of uiteindelijk ook failliet gingen, kon niet uit de beschrijvingen worden opgemaakt. Beide vormen vinden plaats op Nederlands grondgebied. Vaak voeren de criminele samenwerkingsverbanden ook andere

vormen van criminaliteit uit, zoals de teelt van hennep of de productie van synthetische drugs en smokkelen zij de producten naar het buitenland. Er is daarom meestal sprake van een internationale component bij faillissementsfraude, maar deze hangt samen met andere criminele activiteiten.

Naast beroepsfraudeurs zijn er gelegenheidsfraudeurs die trachten wederrechtelijk voordeel te halen uit een niet vooropgezet faillissement. Juridisch heeft de eigenaar dan een scheve schaats gereden – er is wellicht geen sprake van evidente fraude, maar wel van onrechtmatige onttrekking van activa (Knegt et al., 2005). Hoewel het bij gelegenheidsfraudeurs ook om aanzienlijke bedragen kan gaan, vindt de fraude hierbij niet georganiseerd plaats. Hierdoor valt het buiten het domein van dit rapport.

4.8.4 Maatschappelijke gevolgen

De financiële schade van faillissementsfraude is groot. Het wordt geschat op één miljard euro, wat met een zekerheid grenzende waarschijnlijkheid een onderschatting is.

De belangrijkste benadeelde partijen zijn werknemers, bedrijven en de overheid. Als fraudeurs erin slagen middelen aan de boedel van failliete rechtspersonen te onttrekken, zijn het deze partijen die hun geld mislopen. Werknemers worden benadeeld omdat achterstallig salaris niet wordt uitbetaald, dat zijn er naar schatting jaarlijks 7500 (Gesthuizen, 2011). Daarnaast worden bedrijven benadeeld, omdat de vorderingen van schuldeisers open blijven staan, zij krijgen geen geld meer, en al geleverde goederen worden niet vergoed aan de leveranciers. De belastingdienst en de UWV zijn bij faillissementen preferente schuldeiser en krijgen als eerste uitbetaald. Zij hebben alleen financiële schade wanneer de boedel niet toereikend is.

Naast financiële schade voor allerlei partijen ondermijnt faillissementsfraude het handelsverkeer en de integriteit van het bedrijfsleven. Voor bonafide bedrijven kan het moeilijk worden om in te schatten of ze al dan niet met een malafide bedrijf in zee gaan. Dit is op de lange termijn potentieel bedreigend voor het handelsverkeer, omdat partijen erop moet kunnen vertrouwen dat schulden worden afgelost.

Voor werknemers die als gevolg van faillissementsfraude ontslagen worden, kunnen de emotionele gevolgen desastreus zijn, vooral wanneer zij langer werkeloos blijven.

4.8.5 Criminaliteitsrelevante factoren

Een criminaliteitsrelevante factor die de komende jaren invloed zal hebben op faillissementsfraude is de economische crisis.

Bij de beëindigde faillissementen van vennootschappen waren economische oorzaken⁵⁰ bij bijna een op de drie zaken reden voor het faillissement. Bij eenmanszaken was dat bij bijna een op de vier beëindigde faillissementen het geval (De Boer & Lalta, 2011). Hoewel deze cijfers in relatieve zin vergelijkbaar zijn met die van 2008, toen ook een derde van de faillissementen voortkwam uit economische oorzaken, was het totaal aantal faillissementen in 2010 een stuk hoger (bijna 30%). De komende jaren zal het aantal faillissementen mede door de economische omstandigheden hoog blijven. Hoewel dit natuurlijk niet altijd tot faillissementsfraude zal leiden, is wel te verwachten dat daardoor een stijging van vooral het aantal incidentele fraudeurs zal plaatsvinden. Dit beeld wordt gedeeltelijk bevestigd door de toename van het aantal kleine fraudezaken. Of dit ook gaat leiden tot een toename in het aantal georganiseerde faillissementsfraudes is moeilijk te zeggen.

Daarnaast is de pakkans laag. In 2004 rekende Kamerlid Jan de Wit (SP) uit dat bij een kwart van de faillissementen sprake was van fraude, over 10 procent werd aangifte gedaan en in slechts 2,5 procent van de zaken kwam het tot vervolging. De toenmalige minister van Justitie stuurde toen een Actieplan Bestrijding Faillissementsfraude naar de Tweede Kamer. In 2005 werd het WODC-rapport van Knecht et al. gepubliceerd over aard en omvang van faillissementsfraude, dat als basis diende voor een Aanwijzing Opsporing en Vervolging Faillissementsfraude door het College van procureurs-generaal in 2009, en een vervolg hierop. In de aanwijzing is onderscheid gemaakt naar de zwaarte van de faillissementsdelicten en is expliciet aangegeven wie de aanpak ter hand neemt. Ten tijde van het invoeren van deze wijzigingen, werd geconstateerd dat binnen de Nederlandse politie slechts incidenteel een aantal onderzoeken werd uitgevoerd (soms grote, die de aandacht van de media trokken, omdat het om miljoenen euro's ging). Ondanks de genoemde rapporten en de aanwijzingen is echter nog steeds geen sprake van een structurele aanpak van dit fenomeen.

⁵⁰ Economische oorzaken zijn niet de enige reden waarom bedrijven failliet gaan. Van de in 2010 beëindigde faillissementen was bij 28 procent sprake van mismanagement (De Boer & Lalta, 2011).

4.8.6 Verwachtingen

De economische crisis en de lage pakkans hebben een drempelverlagend effect op deze criminele activiteit. Daarom is te verwachten dat faillissementsfraude de komende jaren niet zal afnemen. Ook zal er niet veel veranderen in de gevolgen voor bedrijven die vorderingen hebben of werknemers die hierdoor ontslagen worden. Op dit moment is echter te weinig zicht op de omvang van faillissementsfraude om een uitspraak hierover te onderbouwen.

Door het meest recente voorstel (juni 2011) van de minister zal hopelijk meer inzicht komen in de werkelijke omvang en schade van faillissementsfraude. In het begin zal het aantal geregistreerde gevallen van faillissementsfraude waarschijnlijk stijgen doordat er meer aandacht voor komt. Bij een adequate aanpak zal de fraude uiteindelijk afnemen, maar blijft dit achterwege dan is er geen reden om aan te nemen dat faillissementsfraude zal verminderen.

4.8.7 Aanpak

Faillissementsfraude kan strafrechtelijk worden aangepakt. De volgende artikelen in het wetboek van strafrecht handelen over faillissementsfraude:

- Artikel 194 Sr stelt strafbaar het niet verschaffen van inlichtingen (aan de curator).
- De artikelen 340-345 Sr stellen strafbaar het benadelen van schuldeisers of rechthebbenden gedurende het faillissement. Hierbij wordt onderscheid gemaakt tussen onvoorzichtigheid (eenvoudige bankbreuk) en opzet (bedrieglijke bankbreuk).
- Artikel 442 Sr stelt strafbaar het handelen zonder medewerking van de bewindvoerder, terwijl surseance van betaling is verkregen.

De strafmaat varieert van één tot zes jaar afhankelijk van de mate van opzet.

Zaken die voortkomen uit eenvoudige bankbreuk konden door curatoren⁵¹ worden gemeld bij het betreffende Fraudemeldpunt, de regiopolitie of het arrondissementsparket. In de laatste twee gevallen diende doormelding aan en registratie van de melding bij het FMP plaats te vinden. Het FMP selecteerde de

⁵¹ De curator doet altijd aangifte. Het WODC berekende dat circa 2500 werknemers per jaar hun baan kwijtraken door een frauduleus faillissement, maar het komt zelden voor dat zij aangifte doen.

lichte zaken en droeg deze ter afhandeling over aan de regiopolitie. Voor de opsporing en vervolging van dit soort zaken is geen bijzondere (aanvullende) financiële kennis vereist. Om de kleine zaken aan te pakken werd in maart 2009 door de BRNON gestart met het project *Faillissementsfraude*, dat tot doel had om 25 kleine onderzoeken naar faillissementsfraude uit te voeren met steun van het Programmabureau Finec. De 25 zaken zijn door de politie aan het OM overgedragen, de afloop is nog niet bekend. Het betrof een eenmalige activiteit ten behoeve van het programmabureau.

Zaken die voortkomen uit bedrieglijke bankbreuk, en die zich kenmerken door complexiteit in de vorm van misbruik van rechtspersonen, andere vermogensdelicten, georganiseerd verband, een groot fraudebedrag en dergelijke, konden door curatoren worden gemeld bij de FIOD-ECD, maar ook bij het FMP of rechtstreeks bij een officier van justitie. Voor de opsporing en vervolging van dit soort zaken is bijzondere financiële kennis noodzakelijk.

De aanpak van faillissementsfraude zal naar verwachting veranderen. Aanleiding hiervoor is het meest recente voorstel van de minister van Veiligheid en Justitie voor een geïntegreerde aanpak (bijlage III), dat inmiddels in gang is gezet. Het doel hiervan is om de opbouw van expertise en samenwerking tussen de verschillende partijen te verbeteren. Op 1 juli 2011 is de wet Herziening Rechtspersonen in werking getreden, waarmee het mogelijk wordt om rechtspersonen effectiever te screenen. Ten tijde van het schrijven van dit rapport wordt een Landelijk Meldpunt Faillissementsfraude ingericht in Zwolle. Afspraken tussen politie, de FIOD-ECD en het OM moeten ertoe leiden dat meldingen niet alleen eenvoudiger kunnen worden gedaan, maar ook beter samengevoegd en geanalyseerd. In de brief van de minister staat ook dat de Garantstelling Faillissementscuratoren zal worden herzien: wanneer na het faillissement niet genoeg geld overblijft om onderzoek te doen naar onbehoorlijk bestuur, kan de curator gebruik maken van de garantstellingsregeling faillissementscuratoren. De overheid staat dan garant voor de kosten. Er worden extra financiële middelen voor deze regeling beschikbaar gesteld en de drempel om een aanvraag te doen wordt verlaagd. Tegelijkertijd worden bedrijven gestimuleerd het Insolventieregister te raadplegen, waarin gegevens staan over faillissementen, surseances van betaling en schuldsanering van natuurlijke personen. De minister werkt aan een civielrechtelijk bestuursverbod, waarmee in geval van ernstig misbruik of wanbeheer, maar geen strafrechtelijke vervolging, bestuurders voor een bepaalde tijd het recht wordt ontzegd om invloed uit te oefenen op het beleid van een rechtspersoon.

Naast deze civielrechtelijke en preventieve maatregelen is de capaciteit voor de strafrechtelijke vervolging van financieel-economische criminaliteit uitgebreid en is vorm gegeven aan een geïntegreerde aanpak door de politie, het Openbaar Ministerie en de FIOD-ECD. Het onderscheid tussen eenvoudige zaken door de regiopolitie en complexe zaken door de FIOD-ECD blijft gehandhaafd. Faillissementsfraude wordt nadrukkelijk genoemd als onderdeel van de aanpak van ondermijnende criminaliteit dat als één van de nationale prioriteiten van de politie geldt.

Een nieuwe maatregel is de invoering van het systeem TRACK op 1 juli 2011, waarmee de Dienst Justis van het ministerie rechtspersonen en hun bestuurders doorlopend kan screenen op misbruik; dit systeem is grotendeels geautomatiseerd en aan de hand van risicoprofielen kan misbruik worden voorspeld. Hierbij worden gegevens gebruikt afkomstig van onder andere de Kamer van Koophandel, de Justitiële Informatiedienst, het Centraal Insolventieregister en de Gemeentelijke Basisadministratie. De analyses kunnen risicomeldingen opleveren die worden verstrekt aan de afnemers. Dit zijn het OM, de AFM, DNB, de Belastingdienst, de politie en bijzondere opsporingsdiensten als de FIOD-ECD. Deze kunnen dan maatregelen nemen om dit misbruik aan te pakken of te voorkomen. Door TRACK kan een bijdrage worden geleverd aan het tijdig opsporen en integraal aanpakken van beroepsfraudeurs. Op dit moment kan nog niets worden gezegd over de effectiviteit van het systeem, omdat het nog in de kinderschoenen staat.

Tot slot is een leerstoel *Faillissementsfraude* ingesteld aan de Radboud Universiteit Nijmegen. Professor mr. Tineke Hilverda, heeft in haar oratie⁵² een aantal voorstellen gedaan tot verbetering van de aanpak. De overheid zou, ten eerste, middelen beschikbaar moeten stellen aan de curator om onderzoek te doen wanneer de boedel is leeggehaald (de curator doet nu alleen onderzoek wanneer zijn inspanningen uit de boedel betaald kunnen worden). Ten tweede zou een afwezige, onjuiste of onvolledige bedrijfsadministratie strafbaar moeten worden gesteld. Een ondeugdelijke administratie is niet alleen een indicatie van ondeugdelijk ondernemerschap, maar vaak ook van fraude. Tot slot is zij van mening dat curatoren en opsporingsinstanties beter opgeleid moeten worden om bedrijfsadministraties op fraude te kunnen analyseren. Voor dit doel wordt momenteel een computerprogramma ontwikkeld.

⁵² De bestrijding van faillissementsfraude: waar een wil is...Oratie professor mr. Tineke Hilverda, hoogleraar Faillissementsfraude aan de Radboud Universiteit, Nijmegen uitgesproken op 25 mei 2012.

4.9 Beleggingsfraude

In 2009 heeft Frans Roest het boek *Beleggen in gebakken lucht* geschreven. Dit boek geeft een goed overzicht van beleggingsfraude in Nederland, zowel strafrechtelijk als met betrekking tot de wijze waarop beleggingsfraude wordt gepleegd. Voor de beschrijving van onder andere de aard en omvang wordt voor een groot deel teruggevallen op dit boek.

4.9.1 Aard

Beleggingsfraude is de algemene benaming voor diverse vormen van fraude waarbij beleggingen in het spel zijn. Voorbeelden hiervan zijn fraude via ‘boilerrooms’, Ponzi-zwandel en piramidespelen:

- Boilerroomfraude ontleent zijn naam aan de ‘boilerrooms’, meestal een (relatief) klein kantoor, van waaruit mensen telefonisch benaderd worden om geld te investeren. Doordat de potentiële klanten de telefoongesprekken van de andere medewerkers op de achtergrond kunnen horen, wordt de indruk gewekt dat er een succesvol en betrouwbaar bedrijf actief is. Om potentiële klanten over te halen geld in te leggen, wordt hen zeer hoge rendementen in het vooruitzicht gesteld. In werkelijkheid blijkt het vaak om waardeloze aandelen te gaan en/of om aandelen van virtuele, niet-bestaande bedrijven. Om toezicht te ontlopen en strafrechtelijk grensoverschrijdend onderzoek te bemoeilijken, worden Nederlandse beleggers vaak vanuit het buitenland gebeld.
- Ponzi-zwandel, vernoemd naar de oplichter Charles Ponzi, is een vorm van beleggingsfraude waarbij investeerders wordt voorgehouden dat hun geld lucratief wordt belegd. In werkelijkheid wordt niets of slechts een (klein) deel van de ingelegde gelden belegd om de schijn op te houden. De vaak vooraf afgesproken (hoge) rendementen worden betaald met de inleggelden van latere investeerders⁵³. De aanvankelijke betaling van hoge rendementen aan inleggers, werkt aanlokkelijk voor andere investeerders (veelal familieleden, vrienden en kennissen van inleggers die daadwerkelijk al hoge winsten hebben opgestreken). De ogenschijnlijk fortuinlijke inleggers vertellen dit door en wekken daardoor de indruk dat hun investering succesvol is geweest. Wanneer de bron van potentiële

⁵³ Indien geld van nieuwe inleggers wordt gebruikt om eerdere inleggers uit te betalen, wordt gesproken over het ‘rob-Peter-to-pay-Paul’ principe (Roest, 2009).

investeerders is opgedroogd, stoppen de betalingen van de rendementen en blijven de beleggers gedupeerd achter.

- Een piramidespel lijkt op Ponzi-zwandel. De deelnemers krijgen hoge rendementen op hun inleg voorgespiegeld en deze rendementen worden betaald uit de inleg van andere investeerders. Bij een piramidespel moeten de deelnemers echter zelf nieuwkomers rekruteren. Na verloop van tijd komen er te weinig nieuwkomers bij en stort de constructie in, waarbij de meeste deelnemers hun inleg kwijt zijn.

Omdat deze drie vormen veel overeenkomsten vertonen, kan de navolgende beschrijving van de aard als algemene beschrijving van het fenomeen beleggingsfraude worden beschouwd. Wanneer een aspect betrekking heeft op een specifieke vorm van beleggingsfraude, dan wordt dit expliciet vermeld.

Bij alle vormen van beleggingsfraude geldt dat voor het opzetten ervan potentiële investeerders gelokaliseerd of aangetrokken moeten worden om deel te nemen aan de zwandel. Fraudeurs maken onder andere gebruik van telefoon of internet om met hen in contact te komen. Daarbij maken ze ook vaak gebruik van adreslijsten waarop mensen staan van wie bekend is dat zij interesse hebben in beleggen of eerder slachtoffer zijn geweest van beleggingsfraude.⁵⁴ Meestal is het voor degene die gebeld wordt, niet duidelijk hoe de beller aan zijn gegevens komt.

Fraudeurs en hun criminele organisaties trachten zo professioneel mogelijk over te komen (Roest, 2007). De meeste potentiële investeerders willen voordat ze investeren of gelden ter beschikking stellen, ervan overtuigd zijn dat hun geld veilig wordt beheerd en belegd. De fraudeur dient er dan ook voor te zorgen dat hij vertrouwen wekt en een uitstekende reputatie heeft. Door middel van dure brochures, (televisie)reclames, sociale media, fraaie websites en (eventueel) een mooie kantoorruimte probeert hij die indruk te wekken (Roest, 2009). De schijn van betrouwbaarheid wordt verder ondersteund door te doen alsof er zakelijke relaties bestaan met bekende banken, door bij televisie-uitzendingen reclametijd in te kopen en door de indruk te wekken dat toezichthouders op de hoogte zijn. En bij boilerroomfraude komt nog het feit dat het werken vanuit een kantoor essentieel is. Potentiële beleggers, die worden gebeld met het aanbod een

⁵⁴ Deze lijsten met adresgegevens circuleren binnen het oplichterscircuit. Verder circuleren er zogenaamde 'suckerlists' waar namen op voorkomen van mensen die al eens zijn opgelicht, waardoor ze geacht worden bevattelijk te zijn voor dit soort fraude (Roest, 2009; FEC, 2004).

financieel product te kopen, moeten door achtergrondgeluiden de indruk krijgen dat de aanbieder een druk bedrijf is dat veel zaken doet (Roest, 2009; FEC, 2004). Tot slot maken fraudeurs gebruik van rechtspersonen, inschrijvingen bij de Kamer van Koophandel, bankrekeningen en kantoorpersoneel, waaronder katvangers. Inkomsten uit inleggelden en de bedrijfsonkosten worden keurig per bank betaald, waardoor het voor de bank en de overige buitenwereld lijkt alsof het om een bonafide bedrijf gaat.

Oplichters proberen ook op een meer persoonlijk niveau vertrouwen te wekken. Ze zijn goed in staat om een potentieel slachtoffer te benaderen op een wijze die dat specifieke slachtoffer aanspreekt. Beleggingsfraudeurs leggen de focus meestal op 'selecte groepen vermogende beleggers'. Ook is het mogelijk dat fraudeurs zich richten op een bepaalde groep mensen zoals een etnische groep, ouderen, een kerkelijke gemeenschap, of een groep van professionals in sport of cultuur. Veelal is de voorgestelde belegging dan gekoppeld aan een goed doel. De zwendelaar maakt gebruik van de vertrouwenspositie die hij binnen die groep heeft verworven. Gedupeerden gaan ervan uit dat de initiator met zijn activiteiten geen verkeerde bedoelingen kan hebben, omdat hij of zij tot de eigen groep of geloofsgemeenschap behoort, of zich maatschappelijk verantwoord inzet (Politie Haaglanden, 2011).

Nadat genoeg vertrouwen is gewekt en inleggers tot betaling zijn overgegaan, is de fraudeur er alles aan gelegen om zo veel mogelijk geld binnen te halen. Bij Ponzi-zwendel en piramidespelen gebeurt dit in eerste instantie door op geregelde tijden de voorgespiegelde beleggingswinst uit te keren. In werkelijkheid is dit geen winst, maar zijn de uitbetaalde bedragen afkomstig uit de ingelegde gelden. Enerzijds worden de investeerders hierdoor verleid om hun geld opnieuw, maar ditmaal voor een langere periode, aan de zwendelaar uit te lenen. Anderzijds oefenen deze vroege succesverhalen aantrekkingskracht uit op andere investeerders, veelal familieleden, vrienden en kennissen van eerdere inleggers. In een latere fase, als er een gebrek aan liquiditeiten dreigt, zal de oplichter de overeengekomen uitbetalingen proberen te omzeilen, door met tal van uitvluchten op de propfen te komen (Roest, 2009). Dit kunnen bijvoorbeeld tijdelijke computerproblemen zijn of de oplichter beroept zich op beperkingen die hem worden opgelegd door een financiële autoriteit, bank of overheidsinstantie. De schuld ligt vanzelfsprekend altijd bij derden of bij onverwachte gebeurtenissen. Een andere methode is een truc om de inlegger zo ver te krijgen dat hij ermee akkoord gaat dat het rendement niet periodiek wordt uitbetaald, maar zogenaamd op het interne rekeningoverzicht van de cliënt wordt bijgeschreven. Aan de beleggers worden vervolgens geen rendementen in cash

meer uitgekeerd, maar worden wel periodiek fictieve rendementsoverzichten getoond, dan wel toegezonden.

Fraudeurs hebben allerlei redenen om afgesproken rendementen niet meer uit te betalen. Dit kan maken dat slachtoffers opnieuw betalingen doen. De fraudeur geeft bijvoorbeeld aan dat de investering op het betreffende moment niet vrijgemaakt kan worden. Vervolgens biedt de fraudeur aan om de rendementen uit te betalen in de vorm van aandelen. Wanneer de verraste belegger toehapt, accepteert hij dat hij niet alleen het aanvankelijk beloofde rendement, maar ook de hoofdsom, in aandelen uitbetaald zal krijgen van een veelal 'gehypte' *start-up company*. Dit wordt door de fraudeurs vervolgens ook weer gepresenteerd als een 'gouden kans'. Vaak komt de veelbelovende *start-up company* plotseling in de belangstelling te staan, omdat er een 'spectaculaire ontdekking' zou zijn gedaan. Hierbij kan gedacht worden aan een levensreddend medicijn of aan de ontdekking van een goudader (Roest, 2012). Als het slachtoffer instemt, wordt de kunstmatig opgevoerde koers van het bedrijf losgelaten, waardoor de aandelen waardeloos blijken.

Een andere mogelijkheid is dat de fraudeurs het 'Nederlandse' filiaal van het bedrijf opheffen. Naar de buitenwereld wordt deze ontwikkeling verklaard als een nieuwe stap van een groeiend bedrijf. Het fiscaal gunstige klimaat en het bankgeheim worden op voorhand als redenen opgegeven om zich in het buitenland te vestigen en de Nederlandse vestiging af te bouwen. De fraudeurs geven de klanten het nieuwe (buitenlandse) adres en telefoonnummer en zijn dan in eerste instantie nog bereikbaar. Vanaf het moment dat het slachtoffer lastige vragen gaat stellen of geld wil zien, wordt het al snel niet of nauwelijks mogelijk om de fraudeurs te bereiken. Omdat in het nieuwe juridische vestigingsgebied de vestigings- en verantwoordings-eisen minder strikt zijn, verwachten fraudeurs op deze wijze uit handen te blijven van de Nederlandse justitie (Roest, 2009).

Wanneer de bron van potentiële investeerders is opgedroogd, de rendementsuitbetalingen zijn gestopt en de terugbetalingen van de inlegsom niet langer meer plaatsvinden, zullen gedupeerde beleggers aan de bel trekken. Slachtoffers van beleggingsfraude lopen in de periode hierop gevaar een tweede keer opgelicht te worden als gevolg van een zogenaamde *recovery scam*. Een boilerroom maakt als het ware een doorstart waarbij de verontruste belegger al dan niet aan de hand van een *sucker list* opnieuw telefonisch wordt benaderd. De fraudeur biedt aan het kapitaal dat het slachtoffer verloren heeft, terug te verdienen. Teneinde dit te kunnen doen, dient er wel eerst een *restriction fee* betaald te worden afhankelijk van de grootte van de originele investering. Deze premie zou nodig zijn om de aandelen vrij te geven voor de verkoop. Wanneer

het slachtoffer de premie betaalt, leidt dit natuurlijk niet tot de gewenste terug-gave van eerdere investeringen, maar verliest het slachtoffer alleen nog maar meer geld. Deze vorm van vervolgzwendel ('boilerroom tweede fase') wordt in de literatuur ook wel *recovery fraud* genoemd (Roest, 2009).

Binnen de drie vormen van beleggingsfraude heeft vooral boilerroomfraude een sterk internationaal karakter. Terwijl vanuit Nederland potentiële slachtoffers in het buitenland worden benaderd, geldt andersom dat Nederlandse slachtoffers vrijwel altijd vanuit het buitenland worden benaderd. Bij de andere vormen worden de slachtoffers in Nederland geworven, waarna de inleg naar een rekening in het buitenland wordt overgemaakt. Daar zou zich dan het bedrijf bevinden waarin wordt 'geïnvesteerd'.

4.9.2 Omvang

Er ontbreekt een goed overzicht van de omvang van beleggingsfraude. Cijfers die betrekking hebben op de omvang, komen veelal tot stand op basis van schattingen. Bij het gebruik van deze cijfers is dus enige terughoudendheid geboden. In 2006 kwamen de schattingen door de Autoriteit Financiële Markten (AFM) in de buurt van de 500 tot 750 miljoen euro. In 2011 is de AFM terughoudender in haar uitlatingen; in het jaarverslag van 2010 staat een opmerking, waaruit afgeleid kan worden dat de schades uit beleggingen boven de 50.000 euro de afgelopen jaren honderden miljoenen euro's hebben bedragen (Roest, 2012). Het OM dat, naast de FIOD-ECD, belast is met de opsporingspraktijk, was niet in staat om een overzicht te genereren van het aantal zaken dat binnenkomt en uiteindelijk onder de rechter komt.

Zoals vermeld, hebben slachtoffers van beleggingsfraude de afgelopen jaren honderden miljoenen euro's schade geleden. In die periode vielen beleggingen boven de 50.000 euro buiten het toezichtskader van de AFM, omdat investeerders van dergelijke bedragen geacht worden professioneel te werk te gaan en minder vatbaar te zijn voor beleggingsfraude. Dubieuze aanbieders van financiële producten kunnen zich aan toezicht onttrekken door investeringen aan te bieden boven de vrijstellingsgrens. Deze aanbieders vallen buiten de statistieken van de AFM, aangezien deze zijn gebaseerd op de vastgestelde overtredingen van de toezichtwetgeving. En daarom veronderstellen fraude-experts dat het schadebedrag veel hoger ligt dan de hiervoor genoemde bedragen. Op 1 januari 2012 is de vrijstellingsgrens verhoogd naar 100.000 euro voor nieuwe aanbiedingen (AFM, 2011). Het effect hiervan zal in de toekomst moeten blijken.

Aangezien fraudeurs vaak beleggingen aanboden waarin minimaal 50.000 euro moest worden geïnvesteerd, raakten de beleggers flinke bedragen kwijt. Dit blijkt ook een analyse van de aangiften door de politie Haaglanden. Beleggingsfraude stak, met een gemiddeld schadebedrag van 80.000 euro, met kop en schouders boven alle andere hoofdvormen van fraude uit (Politie Haaglanden, 2011). Dit beeld wordt bevestigd door onze eigen analyse van de aangiften (hoofdstuk 4). Beleggingsfraude kwam in het afgelopen jaar slechts veertien keer voor in de aangiften die geregistreerd stonden onder oplichting, en daarmee is het een van de minder frequent voorkomende vormen van fraude. In acht gevallen was sprake van beleggingsfraude en de slachtoffers werden opgelicht voor bedragen variërend van enkele duizenden euro's tot en met 50.000 euro. Drie aangiften gingen over boilerroomfraude en deze slachtoffers raakten respectievelijk 6.500, 80.000 en 200.000 euro kwijt. Twee slachtoffers van piramidespelen waren voor respectievelijk 1.500 en 60.000 euro opgelicht⁵⁵.

De aangiftebereidheid met betrekking tot fraude is zeer laag. Mensen willen vaak niet geloven dat zij slachtoffer van fraude zijn geworden. Vooral bij beleggingsfraude speelt schaamte een grote rol in de terughoudendheid om fraude te rapporteren. En wanneer wel aangifte wordt gedaan, hebben slachtoffers vaak het gevoel niet serieus te worden genomen door de politie (Kunst & Van Dijk, 2009). Het aantal slachtoffers van beleggingsfraude is waarschijnlijk groter dan in de politiestructuren wordt teruggevonden. Overigens komen bij de Fraudehelpdesk per jaar ongeveer zestig meldingen van beleggingsfraude binnen (Politie Haaglanden, 2011). Welk deel daarvan uiteindelijk tot een aangifte leidt is onduidelijk.⁵⁶

Op basis van het aantal aangiften en het gemiddelde schadebedrag zou de financiële schade slechts enkele miljoenen euro's bedragen. Uit de beleggingsfraudezaken die de afgelopen jaren in het nieuws zijn gekomen, kan worden opgemaakt dat het aantal slachtoffers hoger ligt dan uit de aangiften blijkt. Zo was er in 2009 de fraude rond het Bredase beleggingsfonds Partrust dat ruim 30 miljoen euro beheerde voor ongeveer 250 beleggers. Kort daarop volgde vastgoedfonds TRE, dat 70 miljoen euro van ongeveer 900 beleggers zou hebben misbruikt. Deze (en andere) fraudeconstructies die in de afgelopen jaren zijn blootgelegd, lopen regelmatig in de tientallen miljoenen euro's per zaak.

⁵⁵ De aantallen tellen niet op tot veertien omdat overlap binnen de aangiften bestaat.

⁵⁶ Het is goed mogelijk dat de zestig meldingen voor een groot deel overeenkomen met de veertien aangiften die uiteindelijk zijn gedaan. Alleen door zaken naast elkaar te leggen, kan dit worden bevestigd.

Een kenmerk van beleggingsfraude is dat de fraudeurs proberen hun slachtoffers te bewegen tot nieuwe betalingen, waardoor deze opnieuw slachtoffer worden. Hierbij circuleren lijsten van mensen die eerder tot betaling zijn overgegaan. Een Brits onderzoek uit 2006⁵⁷ liet zien dat 13 procent van de gedupeerden voor een tweede keer een aandelenaankoop had verricht en dat ruim 26 procent van de gedupeerden meer dan vier keer was benaderd door (andere) boilerroomorganisaties. In maart 2010 werd bekend dat de Britse *Financial Services Authority* (FSA) en de politie uit London de hand hadden weten te leggen op twee *share fraud master lists*. De ene lijst bevatte de namen en adresgegevens van duizend Britten en de andere lijst telde niet minder dan 6.500 namen en adresgegevens van potentiële slachtoffers (Roest, 2012). Hoewel een soortgelijk Nederlands onderzoek nooit heeft plaatsgevonden, lijkt het niet onwaarschijnlijk dat Nederlandse slachtoffers op vergelijkbare wijze door beleggingsfraudeurs worden benaderd.

4.9.3 Criminele samenwerkingsverbanden

Criminele organisaties richten vaak meerdere rechtspersonen, veelal bv's, op om de fraude ondoorzichtig te maken (Roest, 2009; KLPD, Dienst IPOL, 2008a). Hierbij kan een fraudeur gebruik maken van dienstverleners, die de noodzakelijke kennis van de wet- en regelgeving over beleggingen, handhaving en toezicht, en rechtspersonen hebben. Deze kennis op specifieke onderdelen wordt gekocht, bijvoorbeeld bij het kopen van (lege) bv's, het opzetten van ingewikkelde beleggingsconstructies en het wegsluizen van geld. Door het gebruik van financiële dienstverleners wordt de indruk van professionaliteit en betrouwbaarheid versterkt. Incidenteel beschikken fraudeurs zelf over de specifieke kennis en vaardigheden en kunnen ze zonder adviseurs te werk gaan.

Bij beleggingsfraude wordt vaak met meerdere rechtspersonen, meestal bv's, gewerkt. Hierachter kunnen meerdere 'spelers in het veld' zich verschuilen, door zich erop te beroepen dat ze niet wisten wat er elders in de 'organisatie' aan de hand was. Ze kunnen schuiven met gelden, certificaten en beleggingsproducten/aandelen binnen de gebruikte rechtspersonen. Rechtspersonen worden dan ook gebruikt ter afscherming van de fraudeurs en hun activiteiten en in het algemeen om de opsporing te frustreren (Kabki et al., 2011).

⁵⁷ Zie: <http://www.fsa.gov.uk/library/communication/pr/2006/053.shtml>. Dit persbericht verwijst naar het OFT-rapport *The psychology of scams*.

Criminele samenwerkingsverbanden die zich met beleggingsfraude bezighouden, opereren meestal op internationale schaal. Een van de redenen daarvoor is afscherming. Fraudeurs zoeken bewust naar landen waar het uitwisselen van informatie met Nederlandse opsporingsinstanties te wensen overlaat. Vooral bij boilerroomfraude wordt de organisatie doelbewust over een aantal landen verspreid teneinde toezicht en opsporingsonderzoek te bemoeilijken. In het ene land vestigt de fraudeur de vennootschap die als uithangbord voor de organisatie dienst doet. Veelal een offshore maatschappij met maatschappelijke zetel op bijvoorbeeld de Bahamas. In een tweede land vestigt de fraudeur een representatiebureau. Dit is meestal niet meer dan een postbus van waaruit alles wordt doorgestuurd naar het zenuwcentrum van de organisatie, de boilerroom, welke doorgaans weer in een derde land is gevestigd. Tot slot vindt bankieren vaak nog in een vierde land plaats (Roest, 2009). Een kenmerkend detail is dat in de landen waar de infrastructuur van de groep gevestigd is, niet aan fondsenwerving wordt gedaan. Zo bedienen in Nederland gevestigde boilerrooms het buitenland en bedienen Nederlanders onder valse naam vanuit het buitenland de Nederlandse markt.

Criminele samenwerkingsverbanden die zich met boilerroomfraude bezighouden, hebben veelal een piramidestructuur. Elke laag heeft zijn eigen taak en informatiepositie (Kabki et al., 2011). De criminelen die aan de touwtjes trekken, hebben meestal meerdere boilerrooms tegelijk onder hun hoede (Roest, 2012). Daarbij werken ze vaak volgens het 'cellenprincipe' waarbij iedere cel meerdere entiteiten telt.

Medewerkers uit de belkantoren weten meestal weinig over de samenstelling van de organisatie. Zij worden slechts ingezet om hun specifieke taken te vervullen. Uit verhoren van medewerkers die binnen een boilerroom belast waren met de telemarketing, blijkt dat ze bijvoorbeeld worden ingehuurd om introducerende werkzaamheden te verrichten. Zij brachten doorgaans het eerste contact met de potentiële klanten tot stand. Ze zijn slecht tot matig opgeleid, werken in één van de cellen en worden minimaal geïnformeerd over het exacte mechanisme dat gebruikt zal worden om zeer hoge, gegarandeerde rendementen te kunnen behalen (Roest, 2009). De verkopers van financiële producten kunnen echter ook professionals zijn, zoals financiële adviseurs, accountants en juristen, die voor het aanbrengen van nieuwe deelnemers worden beloofd. Ook zij hoeven niet altijd op de hoogte te zijn van het malafide karakter van de organisatie. Hun professe verleent hen de uitstraling van betrouwbaarheid, waardoor zij makkelijker producten aan de man kunnen brengen.

Het oprollen van één boilerroom en het arresteren van de callcentermedewerkers brengt doorgaans slechts beperkte schade toe aan de complexe criminele internationale organisatie die achter de opgerolde boilerroom schuilgaat. Vaak vindt een doorstart plaats waarbij de frauduleuze boilerroomactiviteiten gewoon doorgaan, weliswaar onder een andere naam en met een (gedeeltelijk) gewijzigd personeelsbestand, maar vaak met dezelfde *settlement agent*⁵⁸. Soms zelfs op hetzelfde adres. Immers, de ruimten van waaruit gewerkt wordt, zijn gehuurd en de callcenterinventaris is in een aantal gevallen geleased (Roest, 2012). Een boilerroom heeft over het algemeen een beperkte levensduur. Vaak roeren de eerste ontevreden klanten zich al binnen een jaar en verplaatst de organisatie zich naar een andere locatie (Kabki et al., 2011).

4.9.4 Maatschappelijke gevolgen

De omvang van beleggingsfraude wordt geschat op (minimaal) enkele honderden miljoenen euro's per jaar. Jaarlijks verliest een groot aantal particuliere beleggers grote sommen geld aan frauduleuze beleggingspraktijken. Door de lage aangiftebereidheid blijft het totaal aantal slachtoffers onbekend. Uit analyse van aangiften door politie Haagland blijkt dat slachtoffers een gemiddelde schade van 80.000 euro hebben (Politie Haaglanden, 2011).

De ernst van de gevolgen van beleggingsfraude kan niet alleen worden bepaald door naar de verloren geldbedragen te kijken. Allereerst omdat de impact van een verlies van 50.000 euro per persoon verschilt. Voor de één is dit een enorm bedrag, terwijl een ander hier nauwelijks iets van zal merken. Vaak gaat het echter om verliezen die de draagkracht van de slachtoffers overstijgen. Ten tweede zit de ernst van de gevolgen ook in de psychische schade. Met de slachtoffers wordt een sterke vertrouwensband opgebouwd, waardoor de fraude vaak lange tijd kan voortduren. Slachtoffers blijven vertrouwen op een goede afloop. Opmerkelijk genoeg houden de slachtoffers dit vertrouwen, zelfs ver nadat ze hadden kunnen constateren dat toegezegde betalingen uitbleven, beloofde rendementen niet werden betaald, extra geld betaald diende te worden of andere onwaarschijnlijke tegenslagen zich voordeden die uiteraard

⁵⁸ Een *settlement agent* zorgt ervoor dat de effecten geleverd worden en dat de verkopers hun geld krijgen. Bij boilerrooms beperkt de rol van *settlement agent* zich tot het ter beschikking stellen van een bankrekening aan een persoon of bedrijf die zich naar de bank toe heeft kenbaar gemaakt als effectenhandelaar. Meestal wordt kort na het openen van de bankrekening de gemachtigde op de rekening gewijzigd, zodat deze nieuwe gemachtigde of een ander vervolgens de bankrekening kan leegtrekken.

voor de slachtoffers tot extra kosten leiden. Ondanks dit soort signalen willen mensen vaak niet geloven dat zij slachtoffer van fraude zijn geworden. Wanneer slachtoffers uiteindelijk beseffen wat hun is overkomen, zijn zij niet alleen financieel, maar ook emotioneel leeggezogen met alle gevolgen van dien. In enkele gevallen heeft dit zelfs geresulteerd in zelfmoord.

De aard van beleggingsfraude brengt met zich mee dat steeds weer nieuwe varianten kunnen worden bedacht. Het publiek kan onvoldoende onderscheid maken tussen bonafide en malafide aanbieders en aanbiedingen. Hierdoor dreigen slachtoffers het vertrouwen in het financiële systeem of in de medemens te verliezen. De ernst zit dus zowel in de persoonlijke problematiek, als in de beperkte mogelijkheden die er zijn om deze vorm van fraude te voorkomen.

4.9.5 Criminaliteitsrelevante factoren

Van alle fraudevormen zal beleggingsfraude misschien wel het meest direct de impact voelen van de economische crisis. De redenen die hiervoor kunnen worden aangereikt, zijn vrij eenvoudig: er is minder kapitaal om te beleggen, minder blind vertrouwen en een groot aantal beleggers wil zijn belegde gelden terugzien (Van Duyne, 2009). Daardoor komen fraudeconstructies sneller aan het licht. Hoewel dit een zeer aannemelijke verklaring is, zijn er nog altijd mensen te vinden die geld beschikbaar hebben om te investeren. Deze mensen ontvangen een zeer laag rendement op hun spaargeld en gaan op zoek naar manieren om hun rendement te verhogen. Beleggingen blijven hierdoor aantrekkelijk. Aangezien de gemiddelde belegger bonafide en malafide aanbieders moeilijk van elkaar kan onderscheiden, is niet te zeggen of beleggingsfraude zal afnemen of niet.

Door misbruik van internet en toename in mobiliteit (internationalisering), kan de opsporing nauwelijks bepalen wie het delict gepleegd heeft en waar. Daardoor kan ook geen effectieve aanpak bepaald worden. De oplichters bevinden zich doorgaans in een ander land dan de slachtoffers en de geldstromen gaan altijd over de grens. Dit maakt de opsporing en het toezicht door controleorganen moeilijk. Door hun grote mobiliteit kunnen beleggingsfraudeurs zich grotendeels onttrekken aan de opsporing. Bovendien kunnen zij boilerrooms gemakkelijk verplaatsen wanneer de grond hen te heet onder de voeten wordt. Binnen de kortste keren duiken ze ergens anders op, waar ze hun praktijken onder een andere naam en met een ander (financieel) product voortzetten (Roest, 2012). In de komende jaren zal dit een belemmerende werking blijven hebben op de aanpak. Het grensoverschrijdende karakter van fraude noodzaakt tot internationale samenwerking in de opsporing, maar leidt

regelmatig tot moeizame en langdurige trajecten of frustreert een onderzoek. Hier komt waarschijnlijk op korte termijn geen grote verbetering in. Daardoor zal de omvang in de komende jaren groot blijven. Dit geldt zowel voor die vormen waarbij Nederlandse slachtoffers vanuit het buitenland benaderd worden, als die waarbij buitenlandse slachtoffers vanuit Nederland benaderd worden.

De FIOD-ECD heeft vier verdachten aangehouden in een strafrechtelijk onderzoek onder leiding van het Functioneel Parket naar een vermeende internationale beleggingsfraude in Amerikaanse levensverzekeringen door het bedrijf QI. Er is de afgelopen 24 uur door de FIOD-ECD en buitenlandse autoriteiten gezocht op 27 locaties in Nederland, Spanje, Turkije, Dubai, Engeland, Zwitserland en de Verenigde Staten. Er is wereldwijd voor miljoenen euro's beslag gelegd op onroerend goed, auto's, dure horloges, boten en een vliegtuig. QI heeft tussen 1 juli 2007 en heden producten verkocht aan vermogende beleggers, vooral in Nederland en België, maar ook in andere Europese landen. Er is volgens het Openbaar Ministerie sprake van een Ponzi-fraude (Uitkeringen worden betaald van het geld van nieuwe inleggers). De FIOD-ECD doorzocht in totaal vijf woningen in Grootebroek, Alkmaar, Hoorn, Amsterdam en Bussum. Daarnaast zijn drie bedrijven in Sassenheim, Amsterdam en Heemskerk doorzocht. In Amsterdam en Arnhem zijn twee advocatenkantoren doorzocht. In het buitenland zijn nog negen woningen, twee bedrijfspanden en een advocatenkantoor doorzocht. De actie kon tot stand komen door goede samenwerking met de Virginia Financial & Securities Fraud Task Force en opsporingsdiensten in onder meer België, Duitsland, Engeland, Denemarken, Malta, Cyprus, Zwitserland, Spanje, Turkije, Bermuda en de Verenigde Arabische Emiraten. De buitenlandse acties zijn gecoördineerd door Eurojust.

Website Openbaar Ministerie, 28 september 2011

4.9.6 Verwachtingen

De komende jaren zal de economische crisis waarschijnlijk een versterkend effect hebben op de omvang van beleggingsfraude. Daarnaast zijn fraudeurs flexibel en kunnen, wanneer details van de uitvoering bekend worden, met simpele modificaties weer (nieuwe) slachtoffers maken en opbrengsten genereren. Deze aanpassingen zijn bijvoorbeeld een ander 'verhaal' of een nieuw product. Ze volgen hierbij vaak trends die in de legale markt spelen. Het is daarom waarschijnlijk dat ook in de komende jaren nieuwe populaire, frauduleuze beleggingsproducten worden ontwikkeld.

Door de economische crisis zal de doelgroep waarschijnlijk kleiner worden. Er zullen echter altijd mensen zijn die zich graag door een aanlokkelijk aanbod willen laten overtuigen. Doordat potentiële slachtoffers het onderscheid tussen malafide en reguliere producten moeilijk kunnen maken, zullen ook de komende jaren veel beleggers het slachtoffer worden van malafide beleggingsproducten.

Het grensoverschrijdende karakter van beleggingsfraude noodzaakt tot internationale samenwerking, maar leidt regelmatig tot moeizame en langdurige trajecten of frustreert een onderzoek. Hier komt waarschijnlijk op korte termijn geen grote verbetering in.

Tot slot blijft beleggingsfraude aantrekkelijk omdat de opbrengst hoog is in verhouding tot het (relatief) kleine risico.

Niets wijst er dan ook op dat de omvang van beleggingsfraude in de komende vier jaar zal afnemen. Zelfs als dit wel het geval is, dan blijft het probleem hoogstwaarschijnlijk onverminderd omvangrijk.

4.9.7 Aanpak

De aanpak van beleggingsfraude gebeurt in grote lijnen nog op dezelfde manier als beschreven in het NDB van 2008. Vanwege de ernst werden in het vorige NDB de fraudeconstructies beleggingsfraude en voorschotfraude als dreiging gekwalificeerd. Deze kwalificatie heeft echter niet geresulteerd in structureel beleid ten aanzien van de problematiek.

In de dagelijkse opsporingspraktijk zijn de FIOD-ECD en het OM belast met onderzoek naar beleggingsfraude. De AFM is als toezichthouder aangesteld om over de belangen van partijen te waken. De AFM heeft onder meer de taak om zo veel mogelijk te voorkomen dat partijen slachtoffer worden van fraude met beleggingsproducten. Daarnaast heeft zij als taak om fraude te signaleren en te bestrijden. Dat doet zij onder meer door het geven van voorlichting. Hiertoe werkt de AFM aan vergroting van de bekendheid van het Meldpunt Financiële Markten waar consumenten dubieuze aanbieders van financiële producten kunnen melden. Daarnaast proberen diverse organisaties, waaronder de AFM, de financiële kennis van consumenten toe te laten nemen via de website www.wijzeringeldzaken.nl⁵⁹.

⁵⁹ *Wijzer in geldzaken* is een initiatief van ruim veertig partijen onder andere uit de financiële sector, de overheid en consumentenorganisaties.

Met ingang van 1 januari 2007 is de Wet op het financieel toezicht (Wft) van kracht geworden. Hierin zijn nagenoeg alle regels en voorschriften voor de financiële markten en het toezicht daarop samengebracht. De wet gaat uit van ruimte voor de eigen verantwoordelijkheid van consumenten. Zij dienen zich voldoende op de hoogte te stellen van alle voorwaarden en risico's en zich op die manier te wapenen tegen misleiding. Consumenten van wie kan worden aangenomen dat zij zelf voldoende inzicht hebben, hoeven in die redenering niet extra in bescherming te worden genomen. Bij het opstellen van de wet was het uitgangspunt dat investeerders die meer dan 50.000 euro kunnen vrijmaken om beleggingsproducten te kopen, met voldoende inzicht en kennis van zaken handelen. In de praktijk blijkt die aanname niet op te gaan en is een aanzienlijk aantal investeerders geld kwijtgeraakt in fraudes die door hun omvang de landelijke pers hebben gehaald.⁶⁰ Het gaat daarbij niet alleen om grote investeerders, maar ook om particulieren die met geleend geld zijn gaan speculeren (KLPD, Dienst IPOL, 2008b).

Per 1 januari 2012 is de grens waarboven partijen vrijgesteld beleggingen mogen aanbieden, verhoogd van 50.000 naar 100.000 euro. Dat betekent dat elk beleggingsobject of deelnemingsrecht in een beleggingsinstelling dat na die datum⁶¹ onder de 100.000 euro wordt aangeboden, onmiddellijk onder toezicht valt. Indien hierdoor malafide beleggingsproducten worden ontwikkeld met inleggeden boven deze grens dan zal het aantal potentiële slachtoffers waarschijnlijk worden ingeperkt. Blijft de vraag of hiermee een grens wordt bereikt, waarboven alleen investeerders met kennis van zaken deelnemen aan beleggingsproducten. Het is immers een gegeven dat ook een goed geïnformeerde belegger de dupe kan worden van een oplichter met een geloofwaardig verhaal.

In de toekomst zal moeten blijken of op basis van deze aanpassing van de wetgeving het aantal slachtoffers zal afnemen. Malafide aanbieders in binnen- en buitenland zullen zich door de bepalingen van de wet – zo is de verwachting – niet laten weerhouden om met nieuwe varianten van bestaande producten op de markt te verschijnen.

⁶⁰ Onder meer Easy Life, Quality Investments en de vastgoedfondsen 'Royal Duba' en Golden Sun Resort.

⁶¹ Voor beleggingsproducten die vóór 1 januari 2012 zijn gedaan en die waren vrijgesteld op grond van de 50.000 euro vrijstelling en die ná 1 januari 2012 niet meer worden aangeboden of worden aangeboden met gebruikmaking van de nieuwe vrijstelling van 100.000 euro geldt een overgangsregeling. Deze regeling voorziet in de verlenging van de termijn waarop partijen aan alle toezichtseisen moeten voldoen tot en met augustus 2012.

4.10 Merkfraude

Rechten⁶² op intellectuele creaties, zoals een product, uitvinding, software-programma, merknaam, muziekstuk of literair werk, worden intellectueel eigendom genoemd. Alleen degene die over het intellectueeleigendomsrecht beschikt, mag het product produceren, de merknaam hanteren, het muziekstuk vastleggen, het boek publiceren et cetera.

In de meeste gevallen van intellectueeleigendomsfraude, is er sprake van het namaken van merkgoederen waarmee inbreuk wordt gemaakt op het merkrecht (merkfraude/namaakproducten) of het verspreiden van materiaal waar auteursrecht op rust (piraterij).

In dit hoofdstuk komt uitsluitend merkfraude aan de orde; piraterij is een van de aandachtsgebieden van de Dienst Nationale Recherche. Voor dit hoofdstuk is gebruik gemaakt van diverse nationale en internationale rapporten en een interview met een expert van Europol.

4.10.1 Aard

Merken zijn beschermd in Nederland. Een merk is, kort gezegd, een teken⁶³ dat wordt gebruikt om goederen of diensten in het economisch verkeer aan te duiden (Engelfriet, 2012). Bijna alles kan een merk zijn, zolang men in staat is om op basis van dat kenmerk de producten of diensten van de ene onderneming van die van een andere te onderscheiden. De bekendste zijn woord- en beeldmerken (logo's), maar ook kleuren, geuren en geluiden kunnen in sommige gevallen onder het merkrecht vallen.

Naast deze kenmerken, die doorgaans onder de juridische definitie vallen, hebben merken ook immateriële kenmerken. Voorbeelden hiervan zijn het merkimago, gebruiksnut en de status die het product de koper verschaft. In deze immateriële kenmerken zit voor de rechthebbende op het merk de grootste waarde. Beide kenmerken, de materiële en de immateriële, kunnen dan ook niet los van elkaar worden gezien.

⁶² Onder de noemer van intellectueeleigendomsrechten worden sterk uiteenlopende regimes als het auteursrecht, naburige rechten, portretrecht, octrooirecht, merkenrecht, modellenrecht, handelsnaamrecht, kwekersrecht en chipsrecht verstaan.

⁶³ Meestal is het nodig om een teken als merk te registreren bij een Merkenbureau alvorens het beschermd is door de merkenwet.

Met merkfraude wordt bedoeld op de productie van en de handel in valse, nagemaakte merkartikelen (Mul, 2000). Meestal betreft het artikelen met een luxe en/of stijlvol imago die een zekere exclusiviteit uitstralen. Voorbeelden hiervan zijn: parfums, horloges, kleding en schoenen. Naast luxe merkartikelen worden ook dure producten nagemaakt, zoals computer-, auto- en vliegtuigonderdelen, bestrijdingsmiddelen en geneesmiddelen⁶⁴. Tot slot worden ook meer alledaagse artikelen nagemaakt, zoals brillen, ballpoints, tuinkabouters, tuinstoelen, speelkaarten, koekjes, schakelaars en kookpannen.

De productie van en handel in valse en nagemaakte merkartikelen speelt zich af op internationaal niveau. Het grootste deel van de namaakgoederen die bij de grenzen van de Europese Unie onderschept worden, komt uit China (54% in 2008). Daarnaast zijn ook relatief veel namaakgoederen uit de Verenigde Arabische Emiraten (12%) en Taiwan (10%) afkomstig. In 2008 kwam 80 procent van de onderschepte goederen de EU binnen via zeevervoer, 12 procent over de weg, 6 procent met luchtvervoer en de rest via andere vervoersstromen, zoals de post (Algemene Rekenkamer, 2010).

De EU is voor de afzet van namaakgoederen een aantrekkelijke markt, omdat deze landen samen de grootste handelsnatie ter wereld vormen. In 2007 bedroeg de waarde van de EU-export in totaal 1.241 miljard euro, wat aanzienlijk meer was dan de export van China (872 miljard euro) en de VS (829 miljard euro). Wat import betreft ontlieden de EU en de VS elkaar in 2007 nauwelijks: 1.434 miljard euro (EU) en 1.443 miljard euro (VS). China importeerde in 2007 voor 624 miljard euro (Eurostat, 2009). Binnen deze grote handelstromen kunnen namaakproducten eenvoudig hun weg vinden naar verschillende landen binnen de EU.

Nederland vormt een relatief kleine afzetmarkt voor namaakgoederen, maar is wel een belangrijk doorvoerland vanwege twee belangrijke *mainports*: de haven van Rotterdam en de luchthaven Schiphol. De haven van Rotterdam is de grootste haven van Europa en tevens de derde haven van de wereld, met een totale goederenoverslag van 420 miljoen ton in 2008 (Eurostat, 2009). De Rotterdamse haven is vooral belangrijk door de overslag van containers en massagoederen, ook wel *bulkoverslag* genoemd. Schiphol staat in 2008 zowel

⁶⁴ Voor een uiteenzetting van fraude met geneesmiddelen wordt de lezer verwezen naar het deelrapport *Nieuwe vormen van georganiseerde criminaliteit, in het bijzonder afpersing en medicijnvervalsing* (KLPD, Dienst IPOL, 2012a).

voor het aantal passagiers als voor cargo (goederenvrachten via de lucht) op een veertiende plaats in de wereldranglijst (Algemene Rekenkamer, 2010).

De handel in namaakgoederen is zeer winstgevend. Volgens een aantal bronnen zijn de verdiensten zelfs hoger dan met de smokkel van drugs. Dit komt onder andere vanwege de hoge marges op de afgezette goederen en de lage risico's. Volgens de Europese Commissie heeft een vervalsers al winst op zijn investering wanneer hij erin slaagt slechts één van zijn tien containers met namaak-sigaretten de grens over te krijgen (Europese Commissie, 2005). De lage risico's die bij de handel in namaakgoederen spelen, hangen samen met de geringe pakkans en de in vergelijking met andere smokkel geringe strafmaat na vervolging. De combinatie van een hoge opbrengst en een lage pakkans maken van handel in namaakproducten een laagdrempelig delict.

4.10.2 Omvang

De omvang van merkfraude is moeilijk aan te geven. Om de grootte van het probleem enigszins in kaart te brengen, worden schattingen vaak gebaseerd op de totale internationale handel en het deel dat daarvan nagemaakt zou zijn. De *Organisation for Economic Co-operation and Development* (OECD) schatte de wereldhandel in namaakartikelen in 2007 op ongeveer 250 miljard US Dollar. Dit was een stijging van 25 procent ten opzichte van 2005 toen dit nog 200 miljard bedroeg. Het aandeel van de nagemaakte goederen in de wereldhandel is toegenomen van 1,85 procent in 2000 tot 1,95 procent in 2007. Hoewel dit een kleine stijging lijkt, kan toch gesproken worden over een aanzienlijke stijging aangezien de omvang van de totale wereldhandel in diezelfde periode is verdubbeld (OECD, 2008; OECD, 2009)⁶⁵.

Het is niet bekend hoe deze handelscijfers zich verhouden tot de waarde van de namaakgoederen die voor de Europese markt bestemd zijn. Het is echter aannemelijk dat het bij namaakgoederen om honderden miljoenen, zo niet miljarden euro's per jaar gaat (Algemene Rekenkamer, 2010).

Naast schattingen van de handel in namaakproducten, beschikken we over de cijfers van het aantal namaakgoederen die de douane jaarlijks in beslag neemt.

⁶⁵ Deze schattingen hebben alleen betrekking op de internationale handel in namaakproducten. De nagemaakte producten die in een en hetzelfde land worden geproduceerd en geconsumeerd, samen met de grote aantallen illegale producten die worden verspreid via het internet, zijn niet inbegrepen. Wanneer deze wel zouden worden meegenomen dan komt de geschatte omvang mogelijk met enkele tientallen tot honderden miljarden hoger uit.

In tabel 6 is een overzicht te zien van de inbeslagnames (Een update van de cijfers is opgevraagd, maar niet geleverd).

Tabel 6

Aantal in beslag genomen namaakartikelen			
	2006	2007	2008
Speelgoed en spellen	1.191.526	61.590	18.771
Cosmetica	56.562	34.645	30.725
Kleding en accessoires	843.539	794.924	572.136
Cd's en dvd's	255.476	81.159	53.146.829
Electra	304.897	253.322	223.176
Computers en accessoires	4.883	6.175	23.663
Horloges en juwelen	18.219	33.091	32.886
Diversen	1.573.395	285.562	1.480.121
Totaal	4.248.497	1.550.468	55.528.307

Uit de cijfers in tabel 6 komt geen eenduidig beeld naar voren. Hoewel in het laatste jaar een enorme stijging van het totaal aantal in beslag genomen namaakartikelen is geregistreerd, is deze toename geheel toe te schrijven aan cd's en dvd's. Deze categorie artikelen is verantwoordelijk voor meer dan 95 procent van de inbeslagnames in 2008. In 2006 was dit slechts zes procent. Dit kan een eenmalige uitschieter zijn geweest, zoals het grote aandeel van speelgoed en spellen in 2006. In dat jaar was deze categorie goederen verantwoordelijk voor 28 procent van de inbeslagnames. In 2008 is het aandeel teruggebracht tot minder dan een procent. De gerapporteerde inbeslagnames van namaakartikelen lijken sterk afhankelijk van toevallige (omvangrijke) vangsten. Als gevolg hiervan kunnen geen uitspraken worden gedaan over trends in deze cijfers.

Tabel 7 laat de herkomst zien van de in beslag genomen goederen. Verreweg de meeste namaakgoederen komen uit China, gevolgd door Taiwan, Japan, de Verenigde Arabische Emiraten en India. In 2008 is China verantwoordelijk voor 73 procent van de herkomst van in beslag genomen namaakartikelen.

Tabel 7

Herkomst in beslag genomen namaakartikelen in 2008		
Land	Aantal artikelen	Percentage
China	40.666.630	73,2%
Taiwan	9.633.257	17,4%
Japan	3.338.618	6,0%
Verenigde Arabische Emiraten	768.636	1,4%
India	546.598	1,0%
Hong Kong	449.050	0,8%
Ethiopië	21.450	0,0%
Turkije	18.671	0,0%
Kenia	7.940	0,0%
Thailand	7.238	0,0%
Overig	70.219	0,1%
Totaal	55.528.307	100,0%

Sigaretten en tabak

De inbeslagnames van nagmaakte sigaretten worden apart geregistreerd. In tabel 8 is voor de afgelopen jaren te zien hoeveel sigaretten en losse tabak in beslag zijn genomen.

Tabel 8

Inbeslagnames sigaretten en tabak		
Jaar	Aantal sigaretten	Hoeveelheid losse tabak
2010	132 miljoen	3.221 kilo
2009	210 miljoen	483 kilo
2008	204 miljoen	500 kilo
2007	85 miljoen	1.000 kilo
2006	116 miljoen	11.000 kilo
2005	107 miljoen	50.000 kilo
2004	185 miljoen	25.000 kilo

In 2010 daalde in Nederland het aantal in beslag genomen sigaretten van 210 miljoen in 2009 naar 132 miljoen (Rijksoverheid, 2011). In 2009 kon van twee

procent worden vastgesteld dat het echte sigaretten betrof⁶⁶. In dat jaar bestonden de overige sigaretten voor 51 procent uit namaaksigaretten en 47 procent uit zogenoemde *cheap whites*, dat wil zeggen sigarettenmerken die in geen enkele lidstaat van de Europese Unie zijn geregistreerd.

De meeste illegale zendingen zijn afkomstig uit China en het Midden-Oosten (in 2010 respectievelijk 53% en 17%), in het bijzonder de Verenigde Arabische Emiraten. Ook in Europa worden nageemaakte sigaretten geproduceerd. De meeste illegale fabrieken worden opgerold in Polen en Tsjechië. Van 51 procent van de inbeslagnames kon de herkomst van de zendingen niet worden vastgesteld door het ontbreken van vervoersdocumenten.

Van de in beslag genomen zendingen was negen procent in 2010 bestemd voor Nederland en 60 procent voor het Verenigd Koninkrijk. In 2009 was 23 procent voor Nederland bestemd en ging 49 procent richting het Verenigd Koninkrijk. Vooral *cheap whites* worden voor het overgrote deel naar het Verenigd Koninkrijk en Ierland gesmokkeld. Hierbij fungeren België en Nederland dikwijls als opslagplaats voor de sigaretten die vervolgens worden doorvervoerd naar het Verenigd Koninkrijk (KLPD, Dienst IPOL, 2010a).

De schade door sigarettensmokkel in 2009, door het verlies van accijns en BTW, wordt geraamd op ruim 36 miljoen euro (Ministerie van Financiën, 2010).

4.10.3 Criminele samenwerkingsverbanden

De informatie over criminele samenwerkingsverbanden die zich bezighouden met merkfraude is beperkt. In de meeste gevallen wordt slechts melding gemaakt van handel in vervalste merkkleding als nevenactiviteit naast andere kernactiviteiten. Omdat tijdens het rechercheonderzoek de nadruk op de andere (kern)activiteiten ligt, blijft merkfraude onderbelicht. Bij de inventarisatie van de criminele samenwerkingsverbanden over het kalenderjaar 2007 zijn slechts drie criminele groepen aangeleverd die handelden in namaakgoederen. In twee gevallen betrof het handel in vervalste merkkleding en in het derde geval ging het om het in bezit hebben van vervalste merkhorloges. In 2008 waren dat ook drie criminele samenwerkingsverbanden; zij hielden zich bezig met vervalste merkkleding (jassen) en sigaretten. In 2009 deden twee criminele groepen aan

⁶⁶ Deze zijn gedeeltelijk afkomstig uit parallelimport. Bij parallelimport koopt een onderneming goederen in een bepaald land - veelal tegen een aanzienlijk lagere prijs, bijvoorbeeld als gevolg van uiteenlopende accijnstarieven - om deze vervolgens te verkopen in een ander land.

illegaal branden en verkopen van informatiedragers met muziek en films, naast de handel in namaakkledij.

De handel in merkartikelen was in slechts één geval kernactiviteit. In vier gevallen was het een nevenactiviteit en drie maal was het onbekend. Vijf criminele samenwerkingsverbanden deden ook aan handel in softdrugs en vier hielden zich ook bezig met harddrugs. De drugsactiviteiten waren in bijna alle gevallen een kernactiviteit.

Het samengaan van merkfraude met andere criminele activiteiten is volgens een expert een typerend kenmerk. Vooral drugs (cocainehandel) en illegale immigratie komen regelmatig voor. Ook komt het voor dat criminelen geld dat met behulp van BTW-fraude was verkregen, investeerden in het maken van namaakartikelen (bijvoorbeeld schoenen). Aangezien voor beide vormen van fraude weinig aandacht is, blijven fraudeurs met deze activiteiten lang onzichtbaar.

Groepen die zich met merkfraude bezighouden, zijn goed georganiseerd. Dit komt deels voort uit de aard van het delict. Het vereist veel organisatie(-talent) om een internationale handel op poten te zetten en goederen, vaak in China geproduceerd, naar verschillende landen in Europa te transporteren en deze vervolgens te verspreiden onder handelaren die de producten aan de man brengen. De groep moet beschikken over de benodigde expertise en over allerlei contacten, zoals met producenten en verkopers van namaakproducten, met bedrijven om geloofwaardig producten aan te kunnen schaffen en met verkoopkanalen om producten af te zetten.

4.10.4 Maatschappelijke gevolgen

Met betrekking tot de omvang van merkfraude in Nederland zijn geen cijfers of schattingen bekend. De gevolgen van de handel in namaakproducten kunnen worden onderverdeeld in gevolgen voor consumenten, bedrijven en overheid.

Namaakproducten worden niet onderworpen aan de strenge eisen en tests waaraan merkproducten wel moeten voldoen. De consument is slachtoffer omdat het aangekochte namaakproduct van inferieure kwaliteit kan zijn. Dit kan uiteenlopen van speelgoed dat giftige stoffen bevat tot parfums die irritaties veroorzaken. Hoewel er ook namaakproducten van goede kwaliteit kunnen zijn, lopen consumenten altijd een risico bij de aankoop van deze producten. Sommige consumenten kiezen hiervoor, maar soms wordt een groep

consumenten daadwerkelijk opgelicht, zoals met parfums en horloges, omdat zij valse merkartikelen niet van echte kunnen onderscheiden.

Ook het bedrijfsleven is slachtoffer van de namaakindustrie. Hierbij is sprake van verschillende belangen. Aan de ene kant wordt door de verkoop van namaakartikelen een deel van de afname van merkartikelen ingenomen. Daarnaast brengt het namaakproduct schade toe aan het (imago van het) echte merk, waardoor exclusieve merken gedeeltelijk hun status verliezen doordat namaakproducten van hun werk een alledaagse verschijning maken. Aan de andere kant kunnen namaakartikelen voordelen opleveren. Het kan gratis reclame betekenen, wat weer tot omzetvergroting leidt. Ook is het mogelijk dat consumenten die eerst goedkope namaakartikelen kopen, het na verloop van tijd niet meer chic vinden en vervolgens het echte merkartikel aanschaffen. Een (tijdelijke) toename van namaakartikelen als gevolg van slechte economische tijden zou op de lange duur, wanneer de economie weer aantrekt, wellicht voordelig voor de merkproducenten kunnen uitpakken (Van Duyne, 2009).

Tot slot is de overheid slachtoffer doordat ze belastinginkomsten (BTW-, omzet- en winstbelasting) misloopt en kosten maakt om het naleven van het intellectueel eigendomsrecht af te dwingen.

Bovenstaande gevolgen zijn algemeen van aard. De mate waarin deze gevolgen specifiek Nederland treffen is moeilijk te kwantificeren. Zolang er weinig zicht is op de omvang van gederfde inkomsten voor bedrijven of de impact van merkfraude op de Nederlandse economie kan de ernst van bovenstaande gevolgen niet worden aangegeven.

4.10.5 Criminaliteitsrelevante factoren

Er zijn verschillende criminaliteitsrelevante factoren die de komende jaren invloed hebben op merkfraude, zoals het gebruik van het internet, de economische crisis en de internationale wereldhandel.

Het internet is de afgelopen jaren meer en meer een plek geworden om producten te kopen. In 2010 winkelden 9,3 miljoen Nederlanders van 12 tot 74 jaar via het internet, een half miljoen meer dan een jaar daarvoor. Nederland behoort daarmee tot de top in Europa. Het is te verwachten dat deze trend zich in de komende jaren zal voortzetten. Deze ontwikkeling schept ook mogelijkheden voor merkfraudeurs om hun goederen aan de man te brengen, zeker wanneer nagemaakte goederen zich steeds meer gaan mengen in het koop-aanbod van (internet)winkels.

De economische crisis zal de komende jaren invloed uitoefenen op de maatschappij in zijn geheel. Hoe dit fenomeen zal uitwerken op merkfraude is moeilijk te zeggen. Aan de ene kant zal een grote groep mensen minder geld te besteden hebben, waardoor zij ook minder uitgeven aan merkproducten, ongeacht of ze authentiek dan wel nagemaakt zijn. Aan de andere kant willen mensen er, ook in slechte tijden, 'goed' uitzien. Merkproducten kunnen bij deze wens een belangrijke rol spelen. Bij een tekort aan financiële middelen om merkproducten aan te schaffen, kunnen consumenten namaakproducten als een aantrekkelijk alternatief zien die ze voor minder geld eenzelfde status verlenen. Dit effect wordt versterkt door verbeteringen in de kwaliteit van namaakgoederen. De productie van namaakgoederen vindt steeds vaker plaats op industriële schaal en de kwaliteit is dusdanig dat ze zonder technische hulpmiddelen niet of nauwelijks van echt te onderscheiden zijn (Algemene Rekenkamer, 2010). Hierdoor kunnen merkproducten in de komende jaren mogelijk meer schade ondervinden van de namaakindustrie.

Ondanks de economische crisis, is de verwachting dat de wereldhandel zal blijven toenemen. Door de toenemende welvaart in opkomende economieën zal daar meer behoefte aan merkartikelen ontstaan. Als gevolg hiervan zal in die landen ook de markt voor valse merkartikelen toenemen. Dit zou kunnen leiden tot een verschuiving van een deel van het aanbod van valse merkartikelen naar andere landen, waardoor de aanvoer naar Nederland vermindert.

Tot slot voelt China, al jaren de grootste producent van namaakproducten, zelf ook steeds meer de negatieve kanten van de namaakindustrie. Ook hun eigen merkproducten worden het slachtoffer van namaakpraktijken. Dit heeft ertoe geleid dat China de afgelopen jaren meer bereid is bij te dragen aan de bestrijding van de namaakindustrie. Indien deze ontwikkeling doorzet, zal het aanbod van namaakartikelen kleiner worden.

4.10.6 Verwachtingen

De handel in namaakproducten is een internationaal en omvangrijk probleem. Het aandeel van de nagemaakte goederen zou in 2007 naar schatting 1,95 procent van de wereldhandel bedragen. Binnen Europa gaat het waarschijnlijk om honderden miljoenen zo niet om miljarden euro's. De omvang van het probleem is voor Nederland echter moeilijk te kwantificeren.

Voor de kortere termijn geven de maatschappelijke ontwikkelingen geen duidelijke richting aan hoe de handel in namaakproducten zich gaat ontwikkelen. Het steeds grotere aanbod van valse merkartikelen via (internet)

winkels, de economische crisis en de verbeterde kwaliteit van namaakproducten zijn redenen om een stijging te vermoeden. Een mogelijke verschuiving van het aanbod naar andere delen van de wereld of een daling van de productie vanuit China zou een daling aannemelijk maken, zoals in de vorige paragraaf beschreven.

Het beperkte zicht op de omvang van gedeerde inkomsten voor bedrijven of de impact van merkfraude op de Nederlandse economie maakt het lastig om uitspraken te doen over verwachtingen. Daarbij is op basis van deze maatschappelijke ontwikkelingen geen eenduidig beeld te schetsen over de ontwikkeling van deze fraudevorm. De meeste van deze ontwikkelingen spelen zich af op internationaal niveau. Mede daardoor is niet vast te stellen in hoeverre de situatie in Nederland zal worden beïnvloed. Hoe merkfraude zich binnen Nederland gaat ontwikkelen is als gevolg hiervan niet te voorspellen.

4.10.7 Aanpak

Nederland heeft ervoor gekozen om de intellectuele eigendomsrechten hoofdzakelijk via civielrechtelijke handhaving te beschermen. Daarbinnen nemen vooral private belangenorganisaties zoals BREIN⁶⁷ en SNB-REACT⁶⁸ een prominente plaats in, maar zijn ook individuele merkrechtshouders actief. De douane heeft hierbij vooral een faciliterende rol. Als de douane goederen heeft onderschept, is het vervolgens aan de rechthouder om civielrechtelijke actie te ondernemen.

Strafrechtelijke handhaving valt onder de verantwoordelijkheid van de FIOD-ECD en het OM. De douane kan alleen in bepaalde gevallen zelfstandig strafrechtelijk optreden. Dat gebeurt dan op basis van de richtlijn intellectuele eigendomsfraude van het ministerie van Justitie (Justitie, 2006).

In het EU-trendrapport uit 2010 worden twee ontwikkelingen zichtbaar in de handhaving van het intellectueel eigendomsrecht aan de Nederlandse buitengrens (Algemene Rekenkamer, 2010). Ten eerste is de douane steeds meer gaan optreden op verzoek van een rechthouder, en minder vaak op eigen initiatief (ambtshalve optreden). Ten tweede is er een absolute daling in het aantal gevallen van strafrechtelijk optreden door de FIOD-ECD en het OM, waardoor civielrechtelijk optreden door rechthouders belangrijker is geworden. Tabel 9 laat

⁶⁷ Stichting BREIN is opgericht in april 1998 en formaliseert de sinds de jaren 70 bestaande samenwerking tussen auteurs en naburig rechthebbenden op het gebied van bescherming tegen ernstige en georganiseerde inbreuk en misbruik van hun werk.

⁶⁸ SNB-REACT is opgericht in 1991 en richt zich wereldwijd op de bestrijding van merkfraude.

de verhouding tussen het ambtshalve optreden van de douane en het optreden op verzoek van een rechthouder zien tussen 2005 en 2008.

Tabel 9

Optreden douane		
Jaar	Ambtshalve optreden	Optreden op verzoek rechthouder
2005	50%	50%
2006	39%	61%
2007	28%	72%
2008	26%	74%

Bron: Algemene Rekenkamer (2010)

In 2005 was de verhouding 50%-50%, in 2008 verschoof deze naar 26% ambtshalve optreden en 74% op verzoek van een rechthouder. De douane is dus steeds meer gaan optreden op verzoek van rechthouders. Wanneer deze ontwikkeling doorzet, kan dit enerzijds een positief effect hebben, omdat rechthouders veelal eigen rechercheonderzoek doen waardoor zij de douane informatie kunnen leveren over het vervoer van namaakgoederen naar Nederland. De douane treedt vervolgens op, waarbij de kans groot is dat de namaakgoederen daadwerkelijk worden onderschept. Anderzijds is het de vraag of de douane in de handhaving van intellectueleigendomsrecht niet te afhankelijk wordt van rechthouders die de middelen hebben om eigen rechercheonderzoek te betalen. Dit kan ten koste gaan van rechthouders die geen eigen onderzoek doen. In dat geval wordt de kans steeds kleiner dat goederen die inbreuk maken op het intellectueleigendomsrecht van laatstgenoemde rechthouders door de douane worden onderschept (Algemene Rekenkamer, 2010).

Een tweede ontwikkeling in de handhaving betreft de daling in strafrechtelijk optreden door de FIOD-ECD en het OM. Het aantal strafrechtelijke zaken is gedaald van 180 in 2004 naar 33 in 2008 (tabel 10). Dit is het gevolg van een keuze door de FIOD-ECD en het OM, om zich te concentreren op zaken met een significante financiële omvang (in de praktijk is dit 50.000 euro) en waarbij aanwijzingen bestaan dat criminele organisaties in hoge mate betrokken zijn. De genoemde instanties waren genoodzaakt tot prioritering vanwege hun beperkte capaciteit in vergelijking tot hun takenpakket.

Tabel 10

Strafrechtelijke en civielrechtelijke zaken		
Jaar	Aantal strafrechtelijke zaken	Aantal civielrechtelijke zaken
2004	180	Onbekend
2005	184	Onbekend
2006	66	670
2007	37	632
2008	33	627

Bron: Algemene Rekenkamer (2010)

De FIOD-ECD behandelt daarnaast ook zaken waarbij het algemeen belang in het geding is, zoals de volksgezondheid, of indien de inbreukpleger een bedrijfsmatige aanpak hanteert en een groot deel van de markt bedient. Zaken die niet in aanmerking komen voor strafrechtelijke vervolging worden verwezen naar de douane die de rechthouders wijst op de mogelijkheden voor civielrechtelijke afhandeling. Het aantal civielrechtelijke zaken laat tussen 2007 en 2009 een lichte daling zien (Algemene Rekenkamer, 2010).

5

Horizontale fraude als fenomeen

In de voorgaande hoofdstukken zijn voor de tien verschillende hoofdvormen van horizontale fraude de afzonderlijke onderzoeksvragen beantwoord. Dit is gedaan door middel van interviews met experts, op basis van cijfers uit diverse bronnen, door literatuurstudie en uit een analyse van de fraudeaangiften. Met deze werkwijze is getracht zoveel mogelijk recht te doen aan de individuele aspecten van de diverse vormen van fraude. Daarbij zijn ontwikkelingen die zich specifiek binnen deze fraudevormen hebben voorgedaan verwerkt.

Een deel van de hoofdvormen van fraude heeft echter een aantal gemeenschappelijke kenmerken en modi operandi, die onder andere het resultaat zijn van belangrijke ontwikkelingen in de afgelopen jaren. Vooral de toenemende invloed van het internet heeft op vrijwel alle vormen van horizontale fraude een enorme impact gehad. Betalingen, aankopen, maar ook toegang tot veel persoonlijke informatie zijn steeds meer verschoven naar het internet. Internet heeft er ook voor gezorgd dat fraudeurs nu ongekennde mogelijkheden hebben om hun slag te slaan en dit zal in de toekomst alleen maar toenemen.

In dit hoofdstuk zullen eerst de gemeenschappelijke kenmerken van de diverse vormen van fraude beschreven worden, waarbij vooral op de aard wordt ingegaan. In paragraaf 5.2 volgt een beschrijving van de financiële omvang op basis van die gemeenschappelijke kenmerken. Een beschrijving van criminele samenwerkingsverbanden blijft buiten beschouwing, omdat we hierover onvoldoende informatie hebben. Als laatste bespreken we de ondermijnende gevolgen van horizontale fraude, de factoren die het in stand houden en nieuwe ontwikkelingen. Wij pleiten ervoor om de diverse vormen van fraude niet afzonderlijk te wegen, maar in samenhang te beschouwen. Dit wordt ook in deze afsluitende paragraaf bepleit.

5.1 Aard

In deze paragraaf worden drie gemeenschappelijke kenmerken beschreven die bij de tien vormen van fraude naar voren zijn gekomen. Achtereenvolgens zijn dit: massmarketingfraude, identiteitsfraude en witwassen.

Massmarketingfraude

In zes horizontale fraudevormen speelt massmarketingfraude een belangrijke rol als modus operandi⁶⁹. Dat zijn achtereenvolgens: acquisitiefraude, beleggingsfraude (vooral *boilerroomfraude*), fraude met betaalmiddelen (phishing⁷⁰), fraude met online handel, telecomfraude (vooral sms-diensten) en voorschotfraude.

Massmarketingfraude heeft betrekking op de vormen van fraude waarbij fraudeurs gebruik maken van massacommunicatiemiddelen om grote groepen mensen te benaderen. Er wordt in toenemende mate gebruik gemaakt van e-mail, van het adverteren op online handelsplaatsen en *social media*, maar ook post, fax en telefoon spelen nog steeds een rol van betekenis.

Het massaal benaderen van potentiële slachtoffers via telefoon of mailings gebeurt vooral bij acquisitiefraude, *boilerroom*- en telecomfraude. Daarnaast zoeken fraudeurs contact via advertenties op websites en online handelsplaatsen (Marktplaats, eBay, Speurders en dergelijke). Doordat potentiële slachtoffers hierop reageren, zoeken ze in alle onschuld zelf contact met de fraudeur.

De gemene deler bij massmarketingfraude is en blijft de massale benadering van potentiële slachtoffers. Als gevolg van deze massale benadering is het voor fraudeurs al profijtelijk wanneer maar een heel klein deel van de geadresseerden op hun mails ingaat. Slechts een paar personen op een miljoen verstuurd berichten is voldoende om winstgevend te zijn. In de praktijk gaat twee tot vijf procent van de geadresseerden in op de frauduleuze praktijken, ondanks het feit dat steeds meer mensen kennis hebben van phishing of voorschotfraude (UNODC, 2010).

Om slachtoffers tot betalen te bewegen, hanteren fraudeurs globaal twee tactieken. Bij de ene tactiek is sprake van het zogenaamde *many-little*-principe. Hierbij wordt een groot aantal slachtoffers steeds (relatief) kleine bedragen afhandig gemaakt. Door de grote aantallen slachtoffers die de fraudeurs maken, lopen de bedragen die worden gegenereerd echter enorm op. Bij de tweede tactiek is meer sprake van een trechter. Hierbij benaderen fraudeurs aanvankelijk veel verschillende potentiële slachtoffers. Vervolgens richten de fraudeurs zich

⁶⁹ Massmarketingfraude (MMF) is een internationaal geaccepteerde term, een goede Nederlandse term is nog niet voor handen.

⁷⁰ Phishing is aangestipt in paragraaf 4.2 (fraude met betaalmiddelen) en komt op deze plaats ook terug, hoewel het een onderwerp is dat onder het aandachtsgedebied van de Dienst Nationale Recherche valt. De reden is dat het een herkenbaar deel is van massmarketingfraude.

op specifieke (bijvoorbeeld kwetsbare) slachtoffers met wie ze een relatie opbouwen. Bij deze tactiek worden vaak grote bedragen afhandig gemaakt en veel emotionele schade toegebracht.

Bij beide tactieken blijven fraudeurs lange tijd buiten het zicht van de opsporing en zijn de risico's laag. De bedragen zijn ofwel klein waardoor slachtoffers niet snel aan de bel zullen trekken, ofwel de slachtoffers zijn te beschaamd of verbouwereerd om hiermee naar buiten te treden. Daarbij opereren de fraudeurs vrijwel altijd internationaal wat het voor politie en justitie moeilijk maakt om ze op te sporen.

Identiteitsfraude

Naast massmarketingfraude komt in veel hoofdvormen van fraude identiteitsfraude terug. Identiteitsfraude is altijd faciliterend: het is noodzakelijk om een andere vorm van fraude te plegen, het wordt gebruikt om een vertrouwde hoedanigheid te creëren en om de eigen identiteit af te schermen. Het stelt fraudeurs in staat om lange tijd onzichtbaar te blijven en zorgt voor een lage pakkans, omdat bij de opsporing vaak anderen, namelijk katvangers, in beeld komen. Wij hanteren de volgende definitie van identiteitsfraude:

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 (De Vries, Tigchelaar, Van der Linden & Hol, 2007).

Deze definitie, ontleend aan een rapport van het WODC, gaat expliciet over natuurlijke personen. In dit rapport komt regelmatig naar voren dat fraudeurs ook de identiteit van rechtspersonen misbruiken. Fraudeurs doen zich voor als een bedrijf, zij proberen het slachtoffer te bewegen om te investeren in een belegging ofwel om een rekening te betalen waar geen tegenprestatie tegenover staat (Kabki, et al., 2011). Ten behoeve van dit deelrapport vatten wij misbruik van rechtspersonen ook als identiteitsfraude op.

Identiteitsfraude wordt bij vrijwel alle hoofdvormen van fraude door fraudeurs toegepast om de eigen identiteit af te schermen en/of andermans identiteit te misbruiken. Het kan gaan om valse namen of het gebruik van andermans rekeningnummer, zoals bij online handelsplaatsen en fraude met betaalmiddelen, maar ook om katvangers, zoals bij hypotheekfraude en telecomfraude, of om het misbruik van rechtspersonen, zoals bij faillissementsfraude. Bij een aantal hoofdvormen van horizontale fraude is sprake van overlap waarbij verschillende vormen van identiteitsfraude worden gebruikt.

Door de ontwikkelingen op het internet hebben fraudeurs tal van nieuwe mogelijkheden gekregen om fraude te plegen met behulp van identiteitsfraude. Potentiële slachtoffers worden op fora en *social media* op het internet benaderd en verleid om persoonlijke gegevens prijs te geven⁷¹. Een groot aantal mensen gebruikt overal hetzelfde wachtwoord voor zowel privé als zakelijke accounts, waardoor ze kwetsbaar voor fraude worden. Door een website te hacken, kunnen fraudeurs toegang krijgen tot zeer vertrouwelijke gegevens. Wanneer fraudeurs eenmaal toegang hebben, kunnen zij tal van informatie verzamelen waarmee het uiteindelijk mogelijk wordt om iemands identiteit over te nemen of te misbruiken⁷². Dit gebeurt bijvoorbeeld bij het afsluiten van een lening, het openen van een account voor een creditcard, of bij het op een andere manier verwerven van (financiële) goederen op kosten van het slachtoffer.

Het overnemen van een bestaande identiteit gebeurt soms met medeweten van een persoon. Zo worden jonge scholieren gerekruteerd door ronselorganisaties om als katvanger te fungeren. Ze worden misbruikt om bijvoorbeeld tegen een (kleine) vergoeding een rekening te openen. Na het openen van de rekening worden rekeningnummer, inlogcodes en pincodes aan de fraudeur overhandigd om de rekening te gebruiken voor het bijeenbrengen en wegsluizen van door fraude verkregen gelden. Dit zien we onder andere terug bij telecomfraude, waarbij katvangers worden benaderd voor het aanvragen van telefoonabonnementen.

Tot slot wordt identiteitsfraude ook gebruikt om ontdekking en vervolging te voorkomen en om te voorkomen dat de opbrengsten van criminele activiteiten worden opgespoord en in beslag worden genomen. Deze toepassing van identiteitsfraude is een afschermingsmethode bedoeld om de criminele activiteiten te verbergen. Dit vindt echter niet alleen bij fraude plaats, maar ook bij andere vormen van criminaliteit.

Witwassen

Het laatste gemeenschappelijke kenmerk is witwassen. Hoewel witwassen een rol speelt bij een groot aantal, zo niet alle, criminele activiteiten, is vooral een sterk verband met fraude te zien. Unger et al. (2006) rekenden door dat

⁷¹ Deze benadering, waarbij fraudeurs zich direct richten op het zwakste punt in iedere beveiliging, de mens zelf, wordt *social engineering* genoemd. Het is een techniek waarbij een fraudeur mensen probeert te misleiden door in te spelen op typisch menselijke eigenschappen zoals vertrouwen, nieuwsgierigheid, naïviteit, angst of hebzucht.

⁷² Een uitvoerig overzicht van dit soort methodes is te vinden in *High Tech Crime*. Deelrapport criminaliteitsbeeld (KLPD, NR, 2011).

criminaliteit in Nederland tenminste 8,6 miljard euro aan witwasgeld oplevert, waarvan 70 procent afkomstig is van een of andere vorm van fraude⁷³. Nederland is een aantrekkelijk land om geld wit te wassen (net als een aantal andere Europese landen, zoals Duitsland en Frankrijk). Voor het witwassen van geld worden moneytransfers op grote schaal misbruikt. Om de relatie tussen fraude en witwassen beter in kaart te brengen, is het noodzakelijk om de (witwas)geldstromen uitvoerig te analyseren. In dit hoofdstuk zal verder niet op witwassen worden ingegaan, omdat hierover door de Nationale Recherche een apart deelrapport is geschreven (KLPD, NR, 2012).

5.2 Omvang

In hoofdstuk 4 zijn de tien hoofdvormen van horizontale fraude afzonderlijk besproken. De financiële omvang hiervan bedraagt ruim drie miljard euro. Dit is een optelsom van de bedragen die in hoofdstuk 4 per fraudevorm genoemd zijn en deze staan in tabel 11.

Tabel 11

Overzicht omvang hoofdvormen van fraude in miljoenen euro's				
Fraudehoofdform	Omvang Geschat	Gemeld	Massmarketing- fraude	Identiteits- fraude
Fraude met online handel	90	10,5	Ja	Ja
Fraude met betaalmiddelen	57		Ja	Ja
Voorschotfraude	Nederlandse slachtoffers	60		Ja
	Buitenlandse slachtoffers	50	1,5	
	Loterijfraude	150		
Acquisitiefraude	400	5	Ja	Ja
Hypotheekfraude	Onbekend		Nee	Ja
Telecomfraude	40		Ja*	Ja
Verzekeringsfraude	900	25	Nee	Onbekend
Faillissementsfraude	1.000		Nee	Ja
Beleggingsfraude	500		Ja	Ja
Merkfraude	Onbekend		Nee	Onbekend

* Hier gaat het alleen om fraude met sms-diensten

⁷³ In dit onderzoek wordt fraude zeer breed opgevat, variërend van professionele financieel-economische fraude tot uitkeringsfraude en zwart werk.

Deze bedragen zijn grotendeels gebaseerd op schattingen door experts of wetenschappelijke rapporten. Omdat de werkelijke schade zelden goed is onderzocht, hanteren we deze schattingen als uitgangspunt.

Massmarketingfraude

Een expert op het gebied van massmarketingfraude schat de totale financiële omvang van dit fenomeen in Nederland op ruim 1 miljard euro per jaar. Op basis van de schattingen van de afzonderlijke vormen van horizontale fraude waarin massmarketing een rol speelt, komen we tot een vergelijkbare omvang (zie tabel 11). Vooral beleggingsfraude, acquisitiefraude en voorschotfraude hebben een belangrijk aandeel in dit hoge bedrag. Ondanks dat het om grove schattingen gaat, is het onmiskenbaar dat massmarketingfraude een omvangrijk probleem is. Het is daarom van groot belang om de komende jaren meer zicht op dit fenomeen te krijgen.

Identiteitsfraude

Identiteitsfraude speelt in vrijwel alle hoofdvormen van horizontale fraude een rol. Over de omvang van identiteitsfraude in Nederland zijn nauwelijks uitspraken te doen. Studies naar dit fenomeen zijn schaars, en door de diversiteit in vormen en bijbehorende criminele groepen is het moeilijk te onderzoeken (Tromp et al., 2010). De Vries et al. (2007) schrijven dat op basis van bijvoorbeeld het aantal geregistreerde gestolen of vermiste reisdocumenten en ervaringsgegevens van justitiële instanties (zoals de opgeheven Centrale Recherche Informatiedienst (CRI) en het Openbaar Ministerie) de potentiële schade op jaarbasis globaal geschat in de honderden miljoenen euro's loopt. Anno 2009 stond deze schatting nog overeind, met de kanttekening dat betrouwbare gegevens over omvang ontbreken (Tromp et al., 2010).

De schatting van enkele honderden miljoenen euro's lijkt op basis van tabel 11 aan de lage kant. Dit komt deels omdat de door De Vries et al. (2007) gehanteerde definitie van identiteitsfraude nauwer is. In dit deelrapport wordt ook het misbruik maken van de identiteit van rechtspersonen meegenomen. De financiële omvang van faillissementsfraude, een vorm van identiteitsfraude waarbij rechtspersonen worden misbruikt, is volgens het CBS (De Boer & Lalta, 2011) 1 miljard euro per jaar. Deze schatting is aan de lage kant aangezien deze is gebaseerd op dossiers van curatoren waarop actie is ondernomen. Het meenemen van rechtspersonen in de schatting van identiteitsfraude zorgt ervoor dat de financiële omvang een stuk hoger zal uitvallen dan de 1 miljard die door het CBS is gegeven. Identiteitsfraude is een omvangrijk probleem en ook bij dit fenomeen is het van groot belang om hier de komende jaren meer zicht op te krijgen.

Witwassen

Fraude gaat altijd hand in hand met witwassen. Omdat miljarden euro's door fraude verkregen geld moeten worden witgewassen, is het noodzakelijk om zicht op de geldstromen te krijgen.

5.3 Maatschappelijke gevolgen

In de vorige paragrafen is aandacht besteed aan een aantal gemeenschappelijke fraudefenomenen. Na een korte introductie van de aard van deze fenomenen is aangetoond dat het om financieel omvangrijke verschijnselen gaat.

Fraude van deze omvang en het gegeven dat het al jaren doorwoekert, ondermijnt het vertrouwen in een rechtvaardige samenleving. Het leidt niet alleen tot wantrouwen in het functioneren van het financieel-economische stelsel, doordat illegale gelden in omloop komen die worden witgewassen of gebruikt voor andere criminaliteitsvormen (hennepsteelt, mensenhandel), maar het schendt ook het vertrouwen in elkaar, in medemensen. Daarnaast ondermijnt het de positie van organisaties, waaronder de opsporing, die in het leven zijn geroepen om de samenleving tegen criminaliteit in het algemeen, en fraude in het bijzonder, te beschermen. Tot slot leidt het achterblijven van een adequate (strafrechtelijke) aanpak tot normvervaging bij burgers, tot vermindering van het zelfreinigend vermogen van (financiële) ondernemingen, tot ontduiking van regels en (betalings)verplichtingen en tot een lage publieke moraal in het algemeen.

De gevolgen van horizontale fraude voor het slachtoffer zijn afhankelijk van het schadebedrag en de vertrouwensband die is opgebouwd: hoe groter het bedrag, hoe ernstiger de economische, emotionele en psychische gevolgen, zeker wanneer sprake was van een vertrouwensband tussen slachtoffer en dader. Wij noemen in dit verband de katvangers die bij veel fraudevormen in toenemende mate gebruikt worden en nog vele jaren kunnen lijden onder de (financiële) gevolgen van hun daden. Daarnaast komen de gevolgen voor rekening van bedrijven, organisaties en instellingen, werknemers van bedrijven, of voor de overheid zelf. Vooral private partijen zijn in een voortdurende wedloop met de fraudeurs om hun systemen, gegevens en eigendommen te beveiligen en hun klanten tegen aanvallen van fraudeurs te beschermen. Niet alleen lijden deze partijen soms grote verliezen en reputatieschade als gevolg van de fraude, maar ze moeten ook grote (financiële) inspanningen leveren om de fraudeurs voor te blijven.

5.4 Criminaliteitsrelevante factoren

De belangrijkste factoren die horizontale fraude van deze omvang in stand houden, zijn de hoge verdiensten en het kleine risico voor fraudeurs, tezamen met de lage pakkans door de geringe prioriteit bij de opsporing. Behoudens de vormen die door internet gefaciliteerd worden, is dit niet van vandaag of gisteren, maar duurt het bij een aantal vormen al jaren. De aangiftebereidheid is in het algemeen laag. En wanneer aangifte wordt gedaan, blijkt dat dit niet altijd serieus wordt genomen door de politie (Kunst & Van Dijk, 2009). Doordat de informatieorganisatie bij de politie niet op orde is, ontbreken gegevens voor analyse en clustering, en kan de bestrijding in alle facetten niet gestuurd worden.

5.5 Aanpak

Zoals bij de afzonderlijke fraudevormen is meer zicht op de brede fenomenen noodzakelijk. De nieuwe organisatie van de politie biedt daarbij kansen: fraude krijgt op diverse plekken een plaats binnen de Nationale Politie, zoals bij de Landelijke Recherche en de nieuwe regionale informatie- en opsporingsknooppunten. Daarnaast is fraude tot speerpunt benoemd binnen de *Nationale Intelligence Agenda* (NIA), samen met witwassen, vastgoed en ontnemen.

Wij pleiten ervoor om bij de aanpak van fraude de hoofdvormen van fraude niet alleen afzonderlijk te wegen, maar ook vooral op gemeenschappelijke fenomenen in te zetten. Een focus op massmarketingfraude, identiteitsfraude en witwassen, ofwel een aanpak van meerdere criminaliteitsvormen tegelijk is niet alleen efficiënt maar ook effectief. Met een adequate aanpak, gericht op samenwerking tussen private en publieke partijen, onder auspiciën van een coördinerende fraudeautoriteit valt veel te winnen (zie verder hoofdstuk 6).

6

Aanpak van fraude

Naar aanleiding van de vraag die BRO stelde naar de haalbaarheid van een fraudemonitor, zoals beschreven in hoofdstuk 2, is een voorstel tot aanpak voor fraude ontwikkeld. De aanpak is nog niet geëffectueerd, dat wil zeggen dat het ten tijde van de totstandkoming van dit deelrapport in het stadium van een voorstel verkeert. De uitgangspunten zijn geformuleerd voordat de Nationale Politie zijn intrede deed, maar zijn in essentie te generaliseren naar de nieuwe organisatie.

6.1 Fraudebeheersstrategie

Tijdens het onderzoek naar de haalbaarheid van een fraudemonitor, zoals beschreven in paragraaf 2.1, werd door verschillende partijen de wens geuit dat de Dienst IPOL een centrale rol zou gaan spelen. Ook in het huidige onderzoek is door nagenoeg alle partijen de wens uitgesproken om de informatieorganisatie te verbeteren, zodat beter inzicht in aard en omvang wordt verkregen, waardoor een betere sturing mogelijk is.

De wensen zijn vertaald naar een fraudebeheersstrategie (FBS), welke hierna in detail staat beschreven. In de FBS wordt voorgesteld om een *I-Platform* in te richten, waar gegevens uit verschillende bronnen samenkomen, worden geanalyseerd en veredeld. Het doel hiervan is verbanden tussen fraudezaken te leggen, zaken te clusteren en verdachten te identificeren. Daardoor zou op relatief eenvoudige wijze inzicht kunnen worden verkregen in aard, omvang en ernst van de verschillende vormen van fraude. Dat inzicht kan gebruikt worden voor zowel tactische als strategische keuzes. Deze werkwijze sluit aan op het Nationaal Intelligence Model (NIM), dat in essentie het sturen op basis van informatie inhoudt. Tot nu toe was een meer delictgestuurde criminaliteitsanalyse gangbaar. Voorwaarde voor een werkwijze conform het NIM is dat tussen verschillende veiligheidspartners wordt samengewerkt, en dat deze hun eigen informatiehuishouding op orde hebben, waardoor informatie-, kennis- en gegevensuitwisseling structureel kan plaatsvinden.

6.2 Achtergrond FBS

Door het ontbreken van voldoende capaciteit is gezocht naar andere en vooral slimmere bestrijdingsmethodieken. Door technische ontwikkelingen (internet, e-mail, callcenters) kunnen fraudeurs hun (potentiële) slachtoffers massaal benaderen en oplichten, waardoor het aantal, soms relatief kleine fraudezaken tegen particulieren en kleine bedrijven escaleert.

De fraudebestrijding zoals nu gehanteerd door de politie is voornamelijk gericht op afpakken en ontnemen. Daardoor nam het aantal fraudezaken niet af. Inzicht in aard, omvang, ernst en samenhang van de verschillende vormen van fraude ontbrak, en door de veelheid aan fraudevormen was het niet mogelijk om alle betrokken daders op te sporen en te vervolgen. De geringe opsporingscapaciteit zou bij voorkeur dadergericht ingezet moeten worden op basis van centraal verzamelde informatie. Hierbij lijkt de strategie die gehanteerd wordt bij de aanpak van veelplegers de meest effectieve. Dit houdt in dat onderzocht wordt welke daders of csv's over langere tijd de meeste strafbare feiten plegen (zaken stapelen), waarna ze voor al die zaken aangehouden worden, en dus ook een langere straf krijgen. Deze aanpak bleek zeer effectief bij andere vormen van criminaliteit: daders vallen na een dergelijke straf minder snel terug. Naast deze aanpak leek een werkwijze die gericht is op voorkomen de meest effectieve werkwijze.

Het is aan te bevelen dat één instantie alle activiteiten rond deze strategie coördineert, bijvoorbeeld zoals in Groot-Brittannië gebeurt door de *National Fraud Authority* die onder verantwoordelijkheid van een ministerie valt. Daar wordt de aanpak van fraude vanuit drie uitgangspunten gestuurd: bewustwording, preventie en opsporing. Toen de autoriteit in het leven werd geroepen was de informatieorganisatie vergelijkbaar met die in Nederland, dat wil zeggen dat uitspraken over aard en omvang nauwelijks gedaan konden worden. Men startte echter vanuit het uitgangspunt dat criminelen die zich met fraude bezighouden steeds vaker en beter georganiseerd zijn, steeds meer technisch competent zijn en steeds meer over landsgrenzen opereren. Door de verschillende samenwerkende partijen werd een plan van aanpak opgesteld dat dient als sturingsinstrument voor de autoriteit.

6.3 Werkwijze FBS

Een belangrijk uitgangspunt van de fraudebeheersstrategie (Figuur 12) is het beheersen van fraude door verschillende instanties, private en publieke partijen, die bij voorkeur in een keten samenwerken. Het beheersen van fraude gebeurt

op basis van informatie en omvat activiteiten op het gebied van preventie, tegenhouden, frustreren, opwerpen van barrières, en aanpassing van wet- en regelgeving; het is niet noodzakelijk gericht op repressie. In deze strategie werken instanties samen met betrekking tot de 'intake', de centrale informatie-verwerking (veredelen, analyseren en coördineren) en de bestrijdings- of beheersactiviteiten, die op basis van de informatie worden uitgevoerd. Iedere instantie krijgt in de FBS zijn eigen taakaccent.

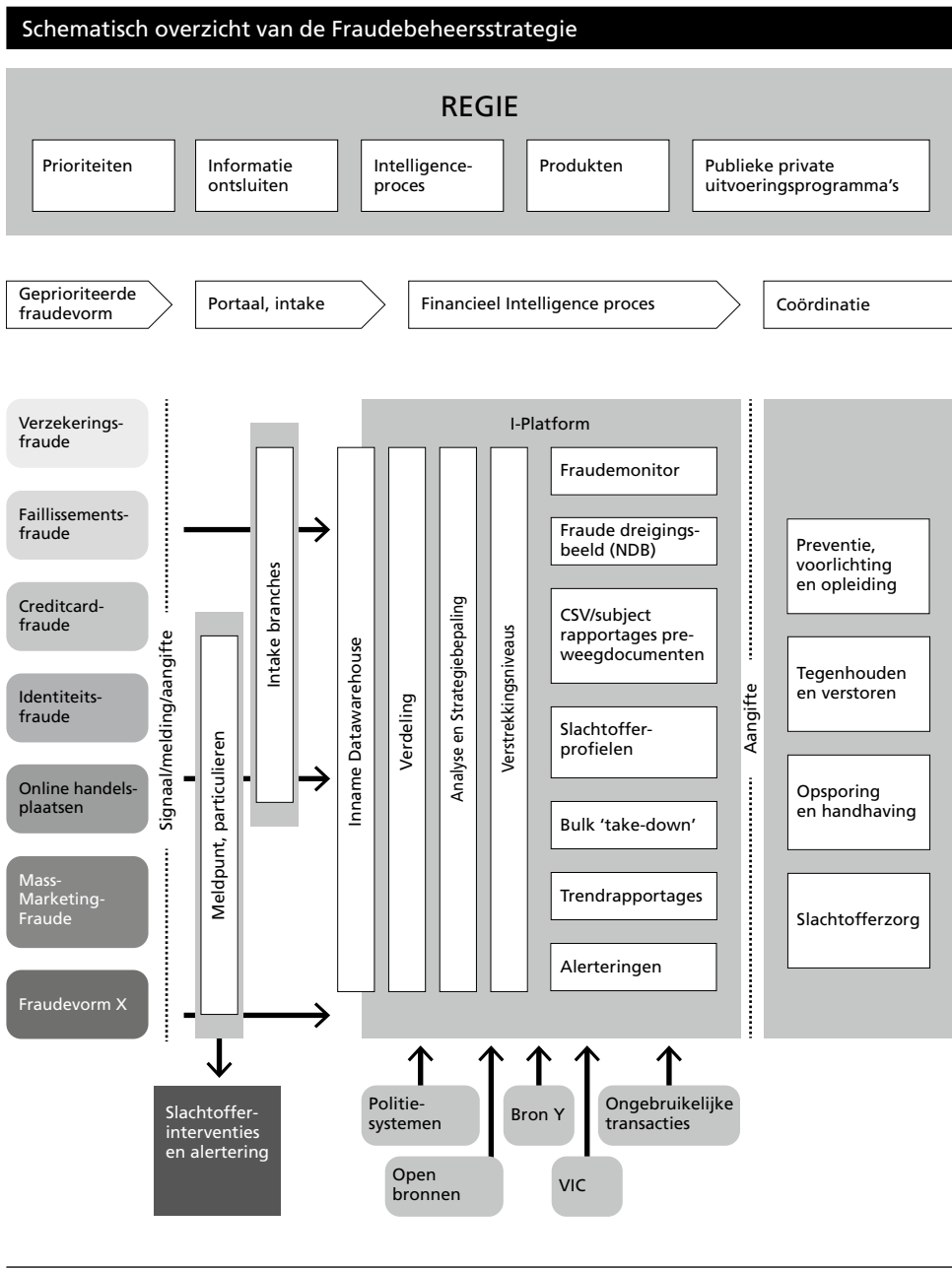
In de toekomst zullen aangiften van veelvoorkomende fraude tegen burgers (zoals cybercrime) naar verwachting steeds meer bij een online meldpunt gedaan worden. Alle relevante informatie over fraude (uit politiesystemen, (fraude)meldpunten en buitenlandse rechtshulpverzoeken) dient op eenduidige wijze te worden geregistreerd. Dit vereist eenduidige definities van fraude die alle meewerkende partijen hanteren, die niet tot misverstanden leiden, en waarmee uiteindelijk aard en omvang kunnen worden bepaald. Daarna kan deze informatie op één centraal punt (*I-Platform*) worden veredeld en geanalyseerd.

Tot slot worden de bestrijdings- of beheersactiviteiten, zoals preventie, tegenhouden, frustreren en repressie, bij voorkeur als taakaccenten ondergebracht bij één van de betrokken partijen. Een organisatie zoals MKB/VNO-NCW kan zich bijvoorbeeld richten op het voorkomen van acquisitiefraude, terwijl de opsporing om de hoek komt wanneer het gaat om zware, strafrechtelijke zaken.

6.4 Voordelen FBS

Op basis van de informatiegestuurde activiteiten zou bij het *I-Platform* inzicht in aard, omvang, ernst en samenhang kunnen worden verkregen voor zowel het strategisch niveau (bijvoorbeeld voor het NDB), het tactisch niveau (monitorberichten, preweegdocumenten) als het operationele niveau. Ook kan zicht op trends worden verkregen, waarop preventie kan worden gericht, en daarnaast levert de informatie criminaliteitsbeelden op. De werkwijze voldoet dan eveneens aan de eisen die door het NIM worden gesteld. Deze informatie is van belang voor alle genoemde beheersactiviteiten. Slimmere methodieken die effectiever werken zullen de geloofwaardigheid van de politie (bestrijding) ten goede komen; het zal leiden tot meer meldingen (beter inzicht in aard en omvang van fraude) en uiteindelijk tot een betere beheersing van de problematiek. Tot slot leidt de aanpak tot een efficiënter gebruik van de capaciteit in de regio's.

Figuur 12



Literatuur

AFM (2010). *AFM Jaarverslag 2010*. Den Haag: Autoriteit Financiële Markten.

AFM (2011, 22 december). *Aanbieders beleggingen tot €100.000 onder toezicht; aanpassing regeling van 26 oktober 2011*. Ontleend aan <http://www.afm.nl/nl/professionals/afm-actueel/nieuws/2011/dec/vrijstellingsgrens-aanpassing-regeling.aspx>

Algemene Rekenkamer (2004). *Fraudebestrijding: stand van zaken 2004* (Tweede Kamer, vergaderjaar 2004–2005, 29 810, nrs. 1–2). Den Haag: Sdu.

Algemene Rekenkamer (2010). *EU-trendrapport 2010* (Tweede Kamer 2009/10, 32306, nrs. 1-2). Den Haag: Sdu.

Algemene Rekenkamer (2011). *ICT politie 2010* (Tweede Kamer, vergaderjaar 2010–2011, 29 350, nr. 9). Den Haag: Sdu.

Anderson, R., M. Bond, & S. J. Murdoch (2005). *Chip and spin*. <http://www.chipandspin.co.uk/spin.pdf>

Benedick, B. (2002). *Handboek bestrijding telecommunicatiefraude. Een nieuwe dimensie voor het onderzoek van telecommunicatie*. Den Haag: Koninklijke Vermande.

Boer, D. de & V. Lalta (2011). *Faillissementen: oorzaken en schulden 2010*. Den Haag/Heerlen: Centraal Bureau voor de Statistiek.

BRNON (2012). *Verzekeringsfraudebeeld (concept)*. Politie intern.

BRO (2010). *Jaarverslag 2010, Politie en Openbaar Ministerie*. Den Haag: DeltaHage.

Centraal Planbureau (2010). *Macro Economische Verkenning 2011*. www.cpb.nl

CMC (2005). *Kwantificering van verzekeringsfraude bij schadeproducten. Kwetsbaarheidsanalyse en beheersingsmogelijkheden*. In opdracht van het Verbond van Verzekeraars. Amsterdam: TMC/T11 Company.

CMI (2012). *Jaarverslag 2011. Vooruitblik 2012*. Den Haag: Centraal Meld- en informatiepunt identiteitsfraude en –fouten.

Corpeleijn, C. (2008). *Rijk worden? Eerst betalen. Een profielschets van het 419-slachtoffer* (Scriptie Universiteit van Utrecht).

Currence (2010). *Jaarverslag 2010: Op de drempel van het Europese betalen*. Amsterdam: Currence.

Dienst Regionale Informatie (2011). Themanummer identiteitsfraude. Kenniscentrum februari 2011. http://www.fec-artners.nl/media_dirs/2/media_files_data/dri_themanummer_identiteitsfraude_tcm15-207545.pdf

DREO (2010). *Beschrijving methodiek PIM (Politie Intelligence Methodiek)*.

Duyne, P.C. van (2009). De zwarte doos van justitie, kredietcrisis en misdaadgeld. *Strafblad*, 6, 531-540.

Elsevier (2012, 5 januari). 'Jeugdwerkloosheid Italië naar recordniveau'. Ontleend aan <http://www.elsevier.nl/web/Artikel/326936/Jeugdwerkloosheid-Italie-naar-recordniveau.htm>

Engelfriet, A. (2012). *Merken*. Ontleend aan <http://www.iusmentis.com/merken/>.

Europese Commissie (2005). *Mededeling van de Commissie aan de Raad, het Europees Parlement en het Europees Economisch en Sociaal Comité betreffende het douaneoptreden tegen de laatste tendensen op het gebied van namaak en piraterij*. COM (2005) 479 def., 1 oktober 2005. Brussel: Europese Commissie.

Eurostat (2009). *External and intra-European Union trade. Data 2002-2007*. Luxembourg: Office for Official Publications of the European Communities.

FEC: Financieel Expertise Centrum (2004). *Rapportage Boilerrooms* [elektronische versie]. Amsterdam: Financieel Expertise Centrum.

FEC: Financieel Expertise Centrum (2008). *Rapportage project vastgoed*. Amsterdam: Financieel Expertise Centrum.

Ferwerda, H., J. Staring, E. de Vries Robbé & J. van de Bunt (2007). *Malafide activiteiten in de vastgoedsector. Een exploratief onderzoek naar aard, actoren en aanpak*. Amsterdam: Uitgeverij SWP in opdracht van het WODC.

Financial Services Authority (2006). *Typical boiler room victim loses £20,000, warns FSA*. Ontleend aan <http://www.fsa.gov.uk/library/communication/pr/2006/053.shtml>

FIU (2011). *Geldstromen tussen Nederland en de West-Afrikaanse landen Nigeria & Ghana (periode 1 januari 2008 t/m 13 mei 2011)*. Politie intern rapport. Zoetermeer: Korps landelijke politiediensten, Dienst IPOL.

Fleuren, J. (2009). *Acquisitiefraude: Oplichting of slimme handel* (Scriptie Erasmus Universiteit, Rotterdam).

Functioneel Parket (2010). *Dreigingsanalyse Financieel-economische criminaliteit Nederland*. Den Haag: Functioneel Parket.

Geldrop, A. van & T. de Vries (2012). *Fraude loont: de toekomst van fraude en ICT*. Enschede: Universiteit Twente.

Gesthuizen, S. (2011). *Bedrog bij bankroet. Acht voorstellen van de SP ter bestrijding van faillissementsfraude*. Ontleend aan: http://www.sp.nl/service/rapport/110413_Bedrog_Bankroet.pdf

Huisman, K. & H. G. van de Bunt, (2009). *Misleidende handelspraktijken. Een onderzoek naar de aard, achtergronden en aanpak van acquisitiefraude in Nederland*. Rotterdam: Erasmus Universiteit, WODC.

Justitie (2006). *Richtlijn voor strafvordering intellectuele-eigendomsfraude*. <http://www.rechtennieuws.nl/files/stcrt2006-6-1.pdf>

Kabki, A., J. van Koningsveld, J. Staat & A. Westerbeek, (2011). *Misbruik van Rechtspersonen. Verkennend onderzoek naar fraudepatronen waarbij misbruik wordt gemaakt van rechtspersonen, specifiek voor het plegen van oplichting en flessentrekkerij*. Apeldoorn: Politieacademie.

Kerkdijk, H., J. W. Knobbe, A. J. Helmus & M. van Staden (2006). *Telecommunicatiefraude in Nederland. Aard, omvang en vooruitzichten*. Groningen: WODC, TNO.

Klerks, P. & N. Kop (2007). *Maatschappelijke trends en criminaliteitsrelevante factoren. Een overzicht voor het Nationaal dreigingsbeeld criminaliteit met een georganiseerd karakter 2008-2012*. Apeldoorn: Politieacademie.

KLPD, Dienst IPOL (2008a). *De staatsruif en de Fata Morgana. Een onderzoek naar fraudeconstructies in het kader van het Nationaal dreigingsbeeld 2008*. Zoetermeer: Korps landelijke politiediensten, Dienst IPOL.

KLPD, Dienst IPOL (2008b). *Nationaal dreigingsbeeld 2008*. Zoetermeer: Korps landelijke politiediensten, Dienst IPOL.

KLPD, Dienst IPOL (2009). *Nigerianen een nieuwe dreiging? Quickscan Nigerianen*. Zoetermeer: Korps landelijke politiediensten, Dienst IPOL.

KLPD, Dienst IPOL (2010a). *Georganiseerde criminaliteit in Nederland 2009. Nederlandse bijdrage aan het Europese dreigingsbeeld 2011*. Zoetermeer: Korps landelijke politiediensten, Dienst IPOL.

KLPD, Dienst IPOL (2010b). *Project 'Brainstest KLPD'*. Zoetermeer: Korps landelijke politiediensten, Dienst IPOL.

KLPD, Dienst IPOL (2012a). *Nieuwe vormen van georganiseerde criminaliteit, in het bijzonder afpersing en medicijnvervalsing*. Zoetermeer: Korps landelijke politiediensten, Dienst IPOL.

KLPD, Dienst IPOL (2012b). *Update effecten economische recessie in het veiligheidsdomein. Update van het onderzoek naar de effecten van de economische recessie op criminaliteit en veiligheid*. Rapport nog niet gepubliceerd.

KLPD, Dienst IPOL (2012c). *Skimmen. Verslag van een onderzoek voor het Nationaal dreigingsbeeld 2012*. Zoetermeer: Korps landelijke politiediensten, Dienst IPOL.

KLPD, NR (2011). *High Tech Crime. Deelrapport criminaliteitsbeeld 2011*. Driebergen: Korps landelijke politiediensten, Dienst Nationale Recherche.

KLPD, NR (2012). *Witwassen. Criminaliteitsbeeldanalyse 2012*. Driebergen: Korps landelijke politiediensten, Dienst Nationale Recherche.

Knegt, R., A. M. Beukelman, J. R. Popman, P. van Willigenburg & I. Zaal (2005). *Fraude en misbruik bij faillissement: een onderzoek naar hun aard en omvang en naar de mogelijkheid van bestrijding*. Amsterdam: Hugo Sinzheimer Instituut in opdracht van het WODC.

Kunst, M. J. J. & J. J. M. van Dijk (2009). *Slachtofferschap van fraude: een explorerend onderzoek naar de impact van diverse vormen van financieel-economische criminaliteit*. Tilburg: Intervict.

Leipoldt, F. & Laning, G. (2006). *Een blik op de telecomsnelweg. Een criminaliteitsbeeldanalyse betreffende elektronische communicatiefraude*. Zwolle: Bovenregionale Recherche Noordoost Nederland.

Leukfeldt, R. & Stol, W. (2011). De Marktplaatsfraudeur ontmaskerd. *Secondant*, 6, 27-31.

Ministerie van Financiën (2010). *Brief aan de Voorzitter van de Tweede Kamer der Staten Generaal over de resultaten van sigarettencontroles*. Den Haag, 26 Mei 2010.

Mul, V. (2000). Merkenfraude. In H. J. B. Sackers & P. A. M. Mevis (red.), *Fraudedelicten* (pp. 105-117). Deventer: Kluwer.

Murdoch, S. J., Drimer, S., Anderson, R. & Bond, M. (2010). Chip and PIN is broken. Paper gepresenteerd op het IEEE Symposium on Security and Privacy 2010. <http://www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf>

NOS (2011, 24 september). 'criminele bellers kosten bedrijven geld'. Ontleend aan <http://nos.nl/artikel/275497-criminele-bellers-kosten-bedrijven-geld.html>

NOS (2012, 5 mei). 'Rabobank: nieuw anti-skimbeleid'. Ontleend aan <http://nos.nl/artikel/369865-rabobank-nieuw-antiskimbeleid.html>

NVB (2011). *Jaarverslag 2010*. Amsterdam: Nederlandse Vereniging van Banken.

NVB (2011, 14 november). 'Veelgestelde vragen persconferentie "Nepmail, daar trapt u niet in!"'. Ontleend aan <http://www.nvb.nl/veelgestelde-vragen.pdf>

NVB (2012). *Jaarverslag 2011*. Amsterdam: Nederlandse Vereniging van Banken.

NVB (2012, 1 juni). 'betalingsverkeer veilig ondanks toename fraude'. Ontleend aan <http://www.nvb.nl/home-nederlands/nieuws/nieuwsberichten/betalingsverkeer-veilig-ondanks-toename-fraude.html>

NVB (2012, 1 juni). 'infographic fraude'. Ontleend aan http://www.nvb.nl/infographic-fraude_v5b.pdf

OECD (2008). *The Economic Impact of Counterfeiting and Piracy*. Parijs: the Organisation for Economic Co-operation and Development. Ontleend aan www.oecd.org/sti/counterfeiting

OECD (2009). *Magnitude of counterfeiting and piracy of tangible products: an update*. Parijs: the Organisation for Economic Co-operation and Development. <http://www.oecd.org/dataoecd/57/27/44088872.pdf>

Openbaar Ministerie en politie (2011). *Verantwoording aanpak georganiseerde criminaliteit 2010*. Vertrouwelijk rapport.

Pak, K. & Shadel, D. (2007). *The psychology of consumer fraud* (Proefschrift Universiteit van Tilburg).

Politie Haaglanden (2011). *Criminaliteitsbeeldanalyse fraude*. Den Haag: Regiopolitie Haaglanden.

Politie IJsselland, BRNON (2008). *Bestuurlijke rapportage Jupiter II*. Zwolle.

Politie Zuid-Holland-Zuid (2010). *Beschrijving methodiek PIM (Politie Intelligence Methodiek)*. Divisie Recherche Expertise en Ondersteuning (DREO) versie 0.5.

Roest, F. (2007). *Beleggen in gebakken lucht. Een studie naar de typerende kenmerken van grensoverschrijdende georganiseerde (mega) zwendels in beleggingsproducten*. Een studie van de afdeling Onderzoek & Expertise van het Functioneel Parket.

Roest, F. (2009). *Beleggen in gebakken lucht. Herkennen, bestrijden en voorkomen van fraude met beleggingsproducten*. Zeist: Uitgeverij Kerckebosch.

Roest, F. (2012). *Succesvolle bestrijding Boilerroom-beleggingsfraude vraagt publiek-private samenwerking*. Update ten behoeve van deelrapport horizontale fraude van het NDB.

Rijksoverheid (2011). *Sigarettenvangsten in Nederland tot 2011*. Ontleend aan <http://www.rijksoverheid.nl/onderwerpen/invoer-en-douane/documenten-en-publicaties/verslagen/2011/06/16/sigarettenvangsten-in-nederland-tot-2011.html>

Schermer, B.W. (2009). *Onze digitale schaduw: een verkennend onderzoek naar het aantal databases waarin de gemiddelde Nederlander staat*. Den Haag: College Bescherming Persoonsgegevens.

Schoenmakers, Y.M.M., E. de Vries Robbé & A. Ph. van Wijk (2009). *Gouden bergen. Een verkennend onderzoek naar Nigeriaanse 419-fraude: achtergronden, daderkenmerken en aanpak*. Den Haag: Reed Business.

Standaard (2012, 28 januari). 'Helft Spaanse jongeren werkloos'. Ontleend aan <http://www.standaard.be/artikel/detail.aspx?artikelid=O93LFH9Q>

Telegraaf (2010, 17 januari). 'AFM verdubbelt onderzoeken beleggingsfraude'. Ontleend aan http://www.telegraaf.nl/binnenland/5809923/___Meer_onderzoek_beleggingsfraude___html

Telegraaf (2010, 22 april). 'Criminelen hacken telefooncentrales van bedrijven, miljoenen weggesluisd'. Ontleend aan http://www.telegraaf.nl/mijnbedrijf/praktische_zaken/veiligheid/6576079/___We_staan_machteloos___html

Thuiswinkel.org (2010, 1 juni). 'Creditcardfraude blijft aandacht trekken'. Ontleend aan <http://www.wijnandjongen.com/cms/showpage.aspx?id=1839>

Tromp, N., J. Snippe, B. Bieleman & E. de Bie. (2010). *Preventieve maatregelen horizontale fraude*. Groningen: IntraVal, WODC.

Ultrascan (2010). *419 Advance Fee Fraud Statistics 2009*. Amsterdam: Ultrascan AGI.

Unger, B., M. Siegel, J. Ferwerda, W. de Kruijf, M. Busuioic, K. Wokke & G. Rawlings (2006). *The amounts and the effects of money laundering. Report for the Minister of Finance 2006*. Utrecht: School of Economics / Australia: Australian National University.

UNODC (2010). *Cybercrime*. Wenen: UNODC.

Verbond van Verzekeraars (2008). *Verzekeringsfraude, een kostbaar probleem. Aanpak door het Centrum Bestrijding Verzekeringsfraude*. Den Haag: Verbond van Verzekeraars.

Verbond van Verzekeraars (2011). *Kerncijfers verzekeren in Nederland*. Den Haag: Verbond van Verzekeraars.

Vos, A. de. (2011, 17 december). Moeilijk verzekeraar. *Het Financieele Dagblad*.

Vries, U. R. M. Th., de, H. Tigchelaar, M. van der Linden, A.M. Hol. (2007). *Identiteitsfraude: Een afbakening*. Universiteit Utrecht: Disciplinegroep Rechtstheorie Departement Rechtsgeleerdheid.

Wilsem, J. van (2011). 'Bought it, but never got it'. Assessing risk Factors for online consumer fraud victimization. *European Sociological Review*. doi: 10.1093/esr/jcr053.

Bijlage I

Klankbordgroep en experts

Leden klankbordgroep:

Alan Kabki:	Onderzoeker Fraude, Politieacademie
Cees Schep:	Senior Specialist Expertise Dienst IPOL en Adviseur Fraudehelpdesk
Esther Jägers:	Senior Beleidsmedewerker Fraude en Ordening, Ministerie van Veiligheid en Justitie
Joost van Onna:	Adviseur Analyse en Expertise, Functioneel Parket
Pim van der Veer:	Clustermanager Programma FinEC, Politie Nederland

Experts geïnterviewd van de volgende organisaties:

- BRNON: Adviseur Koers en Strategie
- BRNON: Informatiemanager Telecomfraude
- BRNON: Informatiemanager Verzekeringsfraude
- BR Zuid-Nederland: Deskundige Koers en Strategie
- Considerati: Partner
- Equens: Manager Fraud Control en Investigator Fraud Control
- Europol: Operations Department, Criminal Finances & Technology
- ING: Manager Fraudepreventie / Secretaris werkgroepen Stichting Fraudebestrijding Hypotheken (SFH)
- International Card Service: Manager risk management ICS
- Marktplaats: Manager Vertrouwen en Veiligheid
- Meldpunt Internet Oplichting: Coördinator Fraudemeldpunt Proeftuin Landelijk Meldpunt Internetfraude
- Ministerie van Veiligheid en Justitie: Beleidsmedewerker
- MKB: Secretaris Auteursrecht, Betalingsverkeer & Criminaliteit
- Nederlandse Vereniging van Banken: Criminaliteitsbeheersing
- Steunpunt Acquisitiefraude / Fraudehelpdesk: Directeur
- Dienst IPOL, Unit Criminaliteit: Senior Specialist Expertise
- Ultrascan: Chief Executive Officer
- VNO-NCW: Secretaris Criminaliteitsbeheersing & Veiligheid
- Verbond van Verzekeraars: Adviseur Criminaliteitsbeheersing & Publiekprivate samenwerking

Ondersteuning bij analyse steekproef

We zijn veel dank verschuldigd aan Dirk Aangeenbrug, instructeur Brains en werkzaam bij Korps Zuid-Holland-Zuid. Hij heeft veel tijd gestoken in het bieden van ondersteuning bij het uitvoeren van de analyse van de 30.000 aangiften. Zonder zijn hulp hadden we dat niet binnen de gestelde tijd kunnen doen.

Bijlage II

Lijst met afkortingen

AFM	Autoriteit Financiële Markten
AIVD	Algemene Inlichtingen- en Veiligheidsdienst
BOD's	Bijzondere Opsporingsdiensten
BR	Bovenregionale Recherche
BRNON	Bovenregionale Recherche Noord- en Oost-Nederland
BRO	Bovenregionaal Recherche Overleg
CBS	Centraal Bureau voor de Statistiek
CPB	Centraal Planbureau
CSV	Crimineel Samenwerkingsverband
DNB	De Nederlandsche Bank
FBS	Fraudebeheersstrategie
FEC	Financieel Expertise Centrum
FinEC	Financieel-Economische Criminaliteit
FIOD-ECD	Fiscale Inlichtingen- en Opsporingsdienst- Economische Controledienst
FIU	Financial Intelligence Unit
FMP's	Fraude Meldpunten
FP	Functioneel Parket
KLPD	Korps landelijke politiediensten
LIRC	Landelijk Internationaal Rechtshulpcentrum
MIO	Meldpunt Internet Oplichting
MOT	Melding Ongebruikelijke Transacties
NIA	Nationale Intelligence Agenda
NIM	Nationaal Intelligence Model
NVB	Nederlandse Vereniging van Banken
OM	Openbaar Ministerie
PRS	Premium Rate Services
SAF	Steunpunt Acquisitiefraude
SFH	Stichting Fraudebestrijding Hypotheken
VIC	Vastgoedinformatiecentrum

Bijlage III

Overzicht hoofdvormen van horizontale fraude en hun zoekvragen in BRAINS

Fraudehoofdvorm	Zoekvraag
Acquisitiefraude	(spookrekening* OR spookfact* OR spooknota* OR (acquisitie AND fraude) OR (aquisitie AND fraude) OR nefactu* OR factuurfraud*)
Fraude met online handel	(*marktplaat* OR ebay wijkopenniet* OR oplichtingvia* OR e-bay OR bay OR speurders* OR koopplein OR tweedehands OR tweakers)
Hypotheekfraude	(hypotheek* OR hypotheclair* OR depot*) AND (*fraud* OR financier* OR vervals* OR bedrog)
Beleggingsfraude	((belegging* OR investering*) AND (*fraud* OR oplicht* OR opgelicht* OR bedrog)) OR (pyramide* OR piramide* OR (boiler AND room) OR boilerroom OR (boiller AND room) OR (nova AND lusus))
Fraude met betaalmiddelen	(spaarbank* OR betaalreken* OR creditcar* OR pinpas* OR bankpas* OR tankpas* OR internetbankier* OR (optisch* AND overschrijvingsf*) OR olo) AND ((skimmen OR skimde* OR skimt OR skimming OR geskim*) OR (tancode*) OR (tan AND code) OR (phish* or fishing) OR hengelen)
Intellectueel eigendomsfraude	(merkenrecht OR merknaam OR merkennaam OR merkenvervalsing OR "valse merkartikelen" OR "nep goederen" OR merkvervalsing OR (auteurs* AND beschermd) OR "STICHTING NAMAAKBESTRIJDING" OR "Snb-React" OR "oneerlijke mededinging") OR namaak

Fraudehoofdvorm	Zoekvraag
Telecomfraude	((telefooncontract* OR telefoonkaart* OR telecomkaart* OR telecomcontract* OR telefoonabonnement* OR telecomabonnement* OR telecombedr* OR telefooncentr* OR telefoonbedr*) AND (telecomfraude OR telefoonfraude OR hacken OR hackte OR hackt OR gehackt OR kraakte OR gekraakt OR *fraud* OR pabx)) NOT Wehkamp
Verzekeringsfraude	(verzekeringsfr* OR verzerkeringsfr* OR *verzekeraar) AND (bedrog OR fraude OR gefraudeerd OR oplichting OR opgelicht)
Voorschotfraude	(schenking* OR voorschot* OR voorgeschoten OR voorschieten OR aanbetalen OR aanbetaal* OR aanbetaling OR (419 AND fraude) OR (artikel AND 419) OR (nigeria* AND fraude)) AND (post* OR mail* OR gemaïld OR brieven OR brief) AND (erfenis OR overlijden OR *kosten OR loterij OR dating OR relatie OR gewonnen OR stervend* OR *opleiding* OR *ziekte OR *kanker OR familielid OR minister)
Faillissementsfraude	(faillissementsfra* OR faillissementsfraude OR (failliet* AND fraude) OR (bedrieglijke AND bankbreuk))

Specifieke zoekvragen online handelsplaatsen:

Producten:

(Mobiele)telefoons: (iphone OR samsung OR htc OR nokia OR "mobiele telefoon" OR i-phone) AND (*marktplaat* OR ebay wijkopenniet* OR oplichtingvia* OR e-bay OR bay OR speurders* OR koopplein OR tweedehands OR tweakers)

iPods en mp3-spelers: (ipod OR i-pod OR mp3 OR mp4 OR mediaspeler) AND (*marktplaat* OR ebay wijkopenniet* OR oplichtingvia* OR e-bay OR bay OR speurders* OR koopplein OR tweedehands OR tweakers))

Toegangskarten (Concert, evenementen, etc): (toegangskarten OR concert* OR kaarten OR kaartjes) AND ((*marktplaat* OR ebay wijkopenniet* OR oplichtingvia* OR e-bay OR bay OR speurders* OR koopplein OR tweedehands OR tweakers))

(Spel)computers: (ipad OR imac OR apple OR acer OR asus OR toshiba OR spelcomputer OR xbox OR playstation OR nintendo OR DSi) AND (*marktplaat* OR ebay wijkopenniet* OR oplichtingvia* OR e-bay OR bay OR speurders* OR koopplein OR tweedehands OR tweakers)

Schoenen: (uggs OR schoenen OR laarzen) AND (*marktplaat* OR ebay wijkopenniet* OR oplichtingvia* OR e-bay OR bay OR speurders* OR koopplein OR tweedehands OR tweakers)

modus operandi:

Betaald, maar niet ontvangen: ("niet ontvangen" OR "nooit ontvangen" OR "niet gekregen" OR "nooit gekregen") AND (*marktplaat* OR ebay wijkopenniet* OR oplichtingvia* OR e-bay OR bay OR speurders* OR koopplein OR tweedehands OR tweakers)

Verstuurd, maar niet betaald: ("niet betaald" OR "nooit betaald" OR "geen geld ontvangen" OR "nooit geld ontvangen") AND (*marktplaat* OR ebay wijkopenniet* OR oplichtingvia* OR e-bay OR bay OR speurders* OR koopplein OR tweedehands OR tweakers)

Specifieke zoekvragen fraude met betaalmiddelen:

Producten:

Phishing: (phishing OR phish* OR fishing) AND ((spaarbank* OR bankrekening OR betaalreke* OR creditca* OR pinpas OR bankpas OR tankpas OR OLO OR internetba*) AND ((skimmen OR skimming) OR ("tan-code" OR tancode*) OR (phish* or fishing) OR hengelen))

Skimmen: (skimmen OR skimming) AND ((spaarbank* OR bankrekening OR betaalreke* OR creditca* OR pinpas OR bankpas OR tankpas OR OLO OR internetba*) AND ((skimmen OR skimming) OR ("tan-code" OR tancode*) OR (phish* or fishing) OR hengelen))

Internetbankieren: (("tan-code" OR tancode*) AND ((spaarbank* OR bankrekening OR betaalreke* OR creditca* OR pinpas OR bankpas OR tankpas OR OLO OR internetba*) AND ((skimmen OR skimming) OR ("tan-code" OR tancode*) OR (phish* or fishing) OR hengelen))) NOT (phish* or fishing)

Hengelen: (hengelen) AND ((spaarbank* OR bankrekening OR betaalreke* OR creditca* OR pinpas OR bankpas OR tankpas OR OLO OR internetba*) AND ((skimmen OR skimming) OR ("tan-code" OR tancode*) OR (phish* or fishing) OR hengelen))

Bijlage IV

Brief Minister van Veiligheid en Justitie inzake faillissementsfraude

29 911 **Bestrijding georganiseerde criminaliteit**

Nr. 52 Brief van de Minister van Veiligheid en Justitie

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 30 juni 2011

Tijdens het algemeen overleg Financieel Economische Criminaliteit (FINEC) en Georganiseerde criminaliteit dat op 27 april 2011 plaats had (kamerstuk 29 911, nr. 50), heb ik aan uw Kamer toegezegd schriftelijk te zullen reageren op de notitie «Bedrog bij bankroet» van het lid Gesthuizen van de SP. Met deze brief doe ik deze toezegging gestand.

1 Inleiding

Het nemen van risico maakt inherent onderdeel uit van het vrije ondernemersklimaat zoals wij dit in Nederland kennen. Uit genomen risico's vloeien successen, maar ook mislukkingen voort. Wanneer een onderneming onherstelbare betalingsproblemen heeft, kan een faillissement worden aangevraagd. Het faillissement is een procedure waarin de resterende baten over de schuldeisers worden verdeeld en de vennootschap wordt ontbonden. Het faillissement is bedoeld om een einde te maken aan financiële onmacht en om een nieuw begin met een schone lei mogelijk te maken. In de meeste faillissementen wordt rechtmatig gehandeld. In sommige gevallen wordt de mogelijkheid van faillissement echter misbruikt om financieel gewin te behalen. In dergelijke gevallen wordt gesproken van faillissementsfraude. Schattingen over in hoeveel gevallen hier sprake van is, lopen uiteen. Er bestaan twee hoofdverschijningsvormen van faillissementsfraude. Onderscheid kan worden gemaakt tussen gelegenheidsfraudeurs, die wederrechtelijk voordeel trachten te halen uit een niet vooropgezet faillissement en beroepsfraudeurs, waarvoor het faillissement

een doelbewust instrument is om op onrechtmatige wijze vermogen aan de boedel te onttrekken.

Terwijl de mogelijkheid om faillissement aan te vragen een onmisbaar instrument is binnen het economische stelsel, is fraude bij faillissementen een vorm van criminaliteit die datzelfde stelsel ondermijnt. Het kabinet wil dat malafide ondernemers die profiteren van faillissementen worden gestopt. Van wezenlijk belang voor het bedrijfsleven, voor werknemers en voor de belastingbetaler, is dat bij faillissementen zoveel mogelijk middelen in de boedel blijven. Uit de boedel kunnen immers schuldeisers, waaronder leveranciers en de belastingdienst, betaald worden en worden voormalige werknemers van failliete ondernemingen betaald voor geleverde arbeid. Als fraudeurs er in slagen middelen aan de boedel van failliete rechtspersonen te onttrekken, zijn het deze partijen die hun geld mislopen en daardoor slachtoffer worden.

De notitie «Bedrog bij bankroet» van het lid Gesthuizen bevat voorstellen ten aanzien van de inzet van capaciteit bij de opsporing, het uitwisselen van relevante informatie tussen betrokken instanties, het stimuleren en faciliteren van faillissementscuratoren om signalen af te geven over faillissementsfraude, bestuursverboden en het afnemen van onrechtmatig verkregen voordeel.

Eerder heb ik aangegeven (TK nr. 1230, vergaderjaar 2010–2011) dat de afgelopen jaren is geïnvesteerd in de aanpak van faillissementsfraude, onder andere door de opbouw van expertise bij het Openbaar Ministerie en de politie. Verdere verbetering is mogelijk en nodig onder andere op het punt van informatie-uitwisseling en de samenwerking tussen de betrokken organisaties. De drempels voor samenwerking en het delen van informatie tussen verschillende betrokken partijen kunnen worden verlaagd. Curatoren kunnen meer worden gestieerd om signalen af te geven over onrechtmatigheden en het aangifte- en meldingenproces kan worden verbeterd.

In de aanpak van verschillende organisaties in de opsporing kan meer samenhang worden aangebracht. De politie, de Fiscale Inlichtingen- Opsporingsdienst (FIOD-ECD) en het Openbaar Ministerie behandelen zaken op het gebied van faillissementsfraude, maar de focus op faillissementsfraude kan sterker en er is ruimte voor verbetering in de inrichting en aansturing van de opsporing op dit terrein.

In het vervolg van deze brief beschrijf ik wat vanuit het specifieke beleidsterrein van Veiligheid en Justitie de bijdrage kan zijn aan het geheel van een geïntegreerde aanpak. Hierbij licht ik toe wat onder een geïntegreerde aanpak wordt

verstaan (paragraaf 2). Daarna zet ik uiteen welke versterking ik voor ogen heb in de aanpak op het gebied van preventie, toezicht en civielrechtelijke instrumenten (paragraaf 3). Tot slot ga ik in de brief in op de strafrechtelijke handhaving (paragraaf 4).

2 Geïntegreerde aanpak

In de Beleidsbrief voor de BOD-en (TK nr. 32 715, nr. 1 vergaderjaar 2010–2011) heb ik de Kamer aangegeven dat dit kabinet bij de bestrijding van criminaliteit en in het beperken van de manoeuvreerruimte van criminelen inzet op een geïntegreerde aanpak. Er dient aandacht te zijn voor zowel preventie, toezicht als voor bestuurlijke- en strafrechtelijke handhaving. Voorwaarde voor een effectieve inzet van deze combinatie van verschillende instrumenten is een goede samenwerking tussen alle betrokken organisaties. Iedere partner vormt een onmisbare schakel in de keten en partijen stemmen de aanpak met elkaar af, zodat optimaal gebruik wordt gemaakt van elkaars capaciteit, informatie, deskundigheid en bevoegdheden.

Fraudestrategie

Om de bestrijding van faillissementsfraude zo effectief mogelijk te organiseren is het essentieel dat duidelijk is hoe de verantwoordelijkheden onder de betrokkenen zijn verdeeld en welke verwachtingen op basis van deze verantwoordelijkheden kunnen worden waargemaakt.

In de aanpak van fraude wil het kabinet toewerken naar een coherente strategie die wordt uitgewerkt en toegepast, in nauwe samenwerking met bestaande publieke en private initiatieven. Hiervoor is een beleidskader ontwikkeld aan de hand waarvan taken en verantwoordelijkheden helder worden gemaakt en een gerichte keuze kan worden gemaakt voor de te volgen interventiestrategie. Het fraudekader is vormgegeven aan de hand van twee dimensies, te weten: gelegenheidsbeperking en de impact op de samenleving. Door deze uitgangspunten in een afwegingskader te plaatsen kan zichtbaar worden gemaakt welke interventie het meest effectief zal zijn. Inzet van het strafrecht zal in principe alleen aan de orde zijn wanneer de opgeworpen barrières adequaat zijn en de impact op de samenleving groot. In een dergelijke strategie voor faillissementsfraude kunnen tevens afspraken worden opgenomen met betrokken partijen, waaronder het bedrijfsleven, INSOLAD, de Nederlandse Vereniging van Insolventierechtadvocaten, en RECOFA, het landelijk overlegorgaan van rechters-commissarissen in faillissementen en surseances van betaling.

Figuur 1.1



3 Preventie, toezicht en civielrechtelijke instrumenten

Faillissementsfraude kan het meest effectief worden bestreden door preventie, hierbij staat de civielrechtelijke aanpak voorop.

In deze paragraaf licht ik toe hoe ik daar vanuit mijn rol als minister van Veiligheid en Justitie een bijdrage aan lever. In de notitie van lid Gesthuizen wordt in dit verband ingegaan op het uitwisselen van relevante informatie tussen betrokken instanties, het stieren van curatoren om signalen van misstanden te onderzoeken en het onttrekken van fraudeurs aan het handelsverkeer om fraude te voorkomen.

Herziening van het toezicht op rechtspersonen

Faillissementsfraude kan plaats vinden door misbruik van rechtspersonen. Om dit misbruik tegen te gaan, zal de Wet controle op rechtspersonen in werking treden. Daarmee start een nieuwe wijze van toezicht op rechtspersonen op 1 juli 2011. De nieuwe wijze van toezicht maakt het mogelijk dat op relevante

levensloopmomenten van een rechtspersoon een screening wordt uitgevoerd door de Dienst Justis van het Ministerie van Veiligheid en Justitie. Ook stichtingen en buitenlandse bedrijven worden meegenomen in het nieuwe toezicht. Door de Dienst Justis van het Ministerie van Veiligheid en Justitie is een nieuw werkproces en een ondersteunend systeem gerealiseerd op grond waarvan het – kort samengevat – mogelijk wordt om grote hoeveelheden informatie over rechtspersonen automatisch en in samenhang te bekijken en daarmee rechtspersonen doorlopend te screenen. De screening zal bestaan uit een automatische analyse en een nadere analyse. Als uit de aanvullende analyse blijkt dat er inderdaad een verhoogd risico is op misbruik van rechtspersonen, verstuurt de Dienst Justis een risicomelding aan relevante organisaties zoals de belastingdienst, politie, de bijzondere opsporingsdiensten, AFM, DNB, Arbeidsinspectie en het OM. Juist de gepresenteerde samenhang van gegevens biedt de instanties met een publiekrechtelijke taak die de risicomeldingen gaan ontvangen, de mogelijkheid om het misbruik van rechtspersonen aan te pakken. De afnemers gaan op zoek naar de juiste mix van bestuursrechtelijke en strafrechtelijke maatregelen om het misbruik van rechtspersonen aan te pakken en te voorkomen.

De doorlopende controle van rechtspersonen draagt op deze manier bij aan een effectievere en efficiëntere bestrijding en voorkoming van financieel-economische criminaliteit en faillissementsfraude en levert daarmee een positieve bijdrage aan het Nederlandse ondernemingsklimaat.

Garantstelling faillissementscuratoren

Om het belang van werknemers, schuldeisers en andere mogelijke gedupeerden van faillissementsfraude te dienen, wil het kabinet het zo eenvoudig en aantrekkelijk mogelijk maken voor de curator om onderzoek te verrichten naar mogelijk onbehoorlijk bestuur. Met het oog daarop wordt de Garantstellingsregeling Curatoren 2005 dit jaar herzien. Deze regeling heeft tot doel de faillissementscurator in staat te stellen een rechtsvordering in te stellen op grond van bestuurdersaansprakelijkheid of faillissementspauliana of een onderzoek daarnaar in te stellen, indien hij een lege boedel aantreft. Doordat de overheid garant staat voor de kosten van de curator, kan de curator onder meer de bestuurder die zijn taak onbehoorlijk heeft vervuld en waarbij die onbehoorlijke taakvervulling tot een faillissement heeft geleid, aansprakelijk stellen. De regeling heeft van 1987 tot heden € 4.6 miljoen gekost. Daar staat tegenover dat de regeling ertoe heeft geleid dat € 28,4 miljoen euro door de curatoren is teruggeleid naar de boedel ten gunste van schuldeisers van failliete ondernemingen. Daarnaast is een stijging waar te nemen in het aantal nieuwe

aanvragen. Terwijl het aantal nieuwe aanvragen in 2005 nog 74 bedroeg, werden er in 2010, 159 nieuwe aanvragen ingediend. De Garantstellingsregeling werpt zijn vruchten af. Tegelijkertijd zie ik mogelijkheden om de regeling te verbeteren. Ten eerste wordt de toegankelijkheid van de regeling vergroot door extra middelen ter beschikking te stellen binnen de financiële kaders die hiervoor zijn gesteld in de begroting en ten tweede worden de administratieve lasten teruggedrongen. Zo zal ik onder andere de mogelijkheid bezien om bepaalde kosten die reeds zijn gemaakt vóór de aanvraag voor een garantstelling is ingediend, onder de reikwijdte van de garantie te brengen. Daarnaast zal ik in overleg met de Nederlandse Vereniging van Insolventie-echtadvocaten aandacht besteden aan het zo gebruiksvriendelijk mogelijk maken van de regeling.

Preventie en bewustwording

Een bestuurder die in ernstige mate zijn verplichtingen als bestuurder heeft geschonden, kan in het kader van een strafrechtelijk onderzoek, naast andere sancties, een strafrechtelijk bestuursverbod opgelegd krijgen. Met een dergelijk verbod kunnen bestuurders van rechtspersonen voor bepaalde tijd het recht worden ontzegd direct of indirect invloed uit te oefenen op het beleid van een rechtspersoon. Het bestuursverbod is voornamelijk gericht op preventie van faillissementsfraude door de aanpak van systematische faillissementsfraudeurs. Deze fraudeurs worden de mogelijkheid ontnomen ondernemingen te besturen, zodat ze geen faillissementsfraude meer kunnen plegen. Momenteel wordt ook de mogelijkheid bezien om te komen tot een civielrechtelijk bestuursverbod, waardoor in gevallen waarin geen strafzaak wordt gestart maar waarin wel sprake is van ernstig misbruik of wanbeheer, snel kan worden ingegrepen door de civiele rechter.

Bij een geïntegreerde aanpak van faillissementen speelt het bedrijfsleven een belangrijke rol. Bedrijven kunnen bijvoorbeeld controleren of de partijen waar zij handel mee drijven bekend staan als onbetrouwbare partij om te voorkomen dat zij slachtoffer worden van faillissementsfraude. Branche- en koepelorganisaties kunnen een belangrijke rol spelen om bedrijven hierin te stimuleren. Het Centraal Insolventieregister, raadpleegbaar via *Rechtspraak.nl* bevat de gegevens van faillissementen, surseances van betaling en schuldsaneringen van natuurlijke personen die in de lokale registers bij de verschillende rechtbanken worden bijgehouden.

Om het fraudebewustzijn te versterken en academische kennis over faillissementsfraude te vergroten, draagt het ministerie van Veiligheid en Justitie sinds

2011 bij aan de financiering van een leerstoel Faillissementsfraude die door de Universiteit van Nijmegen is ingesteld. Door dit soort initiatieven en door met de betrokken partijen in gesprek te blijven wordt continu nagedacht over nieuwe maatregelen en instrumenten die kunnen bijdragen aan de bemoelijking van faillissementsfraude.

4 Gerichte inzet van het strafrecht

Tijdens het Algemeen Overleg Financieel Economische en Georganiseerde Criminaliteit van 27 april 2011 en in de notitie «Bedrog bij bankroet» van het lid Gesthuizen zijn suggesties gedaan voor een effectieve inzet van het strafrecht in de bestrijding van faillissementsfraude. In deze paragraaf informeer ik uw Kamer nader over de strafrechtelijke aanpak van faillissementsfraude en maatregelen die ik neem op het gebied van prioriteitstelling, sturing en inrichting van de opsporing.

Uitgangspunt voor de inzet van het strafrecht binnen de geïntegreerde aanpak is dat het een beperkte, complementaire rol heeft naast preventieve en civielrechtelijke instrumenten. In de regel wordt er pas voor het strafrecht gekozen indien preventie en toezicht niet doeltreffend blijken of indien de ernst van de fraude een strafrechtelijke aanpak vergt.

Verdere versterking van de aanpak van financieel economische criminaliteit

De aanpak van financieel economische criminaliteit is de afgelopen jaren aanzienlijk versterkt. Naast een flinke vergroting van de capaciteit is vorm gegeven aan een gezamenlijke, geïntegreerde aanpak. Voor fraudebestrijding heeft dit significante verbeteringen tot gevolg gehad in de inrichting, capaciteit en expertise bij de Politie, de FIOD-ECD en het Openbaar Ministerie. Dit is een goede ontwikkeling die door dit kabinet met kracht wordt voortgezet. In de landelijke prioriteiten (TK nr. 29 628, nr. 237 vergaderjaar 2010–2011) van de politie vormt ondermijnende criminaliteit één van de nationale prioriteiten van de politie. De aanpak van faillissementsfraude maakt daar nadrukkelijk onderdeel van uit. Bij de inrichting van de Nationale Politie wordt de opsporingscapaciteit op het gebied van financieel economische criminaliteit verder versterkt. De politie trekt professionals aan met de juiste achtergrond om fraude en andere vormen van financieel economisch criminaliteit tegen te gaan. Dit waarborgt dat de politie over de juiste kennis en deskundigheid beschikt – en

daarover blijft beschikken – om faillissementsfraude op te sporen en aan te pakken.

Verbetering van het meldingen- en aangifteproces

In veel gevallen is de curator bij faillissementen degene die misstanden signaleert. Cruciaal is in dergelijke gevallen dat de curator melding maakt van signalen van (mogelijke) fraude. Op basis van deze signalen kan eventueel opsporing en vervolging plaats vinden. Om het doen van aangiften en het maken van meldingen te vereenvoudigen maken politie, FIOD-ECD en Openbaar Ministerie afspraken de bestaande fraudemeldpunten door te ontwikkelen naar één centraal meldpunt voor faillissementsfraude. Daarnaast streven het Openbaar Ministerie, de politie en de FIOD-ECD ernaar dit najaar met de vereniging van faillissementscuratoren, INSOLAD, afspraken te maken over meldingen. Uitgangspunt hierbij is dat curatoren bij vermoeden van fraude in beginsel uitsluitend op eenvoudige en snelle wijze melding maken bij het centrale meldpunt. Op basis van deze voor curatoren eenvoudiger en minder tijdrovende meldingen zullen politie en Openbaar Ministerie afwegen in welke gevallen het doen van aangifte zinvol is. Hierin worden curatoren in dergelijke gevallen ondersteund.

Terugkoppeling bij meldingen en aangiften

Wanneer er in ernstige gevallen over wordt gegaan tot het doen van aangifte is het voor personen die aangifte doen, veelal curatoren, en voor slachtoffers van faillissementsfraude belangrijk dat zij op de hoogte worden gehouden van wat er met de aangifte wordt gedaan en eventueel van het verloop van het betreffende opsporingsonderzoek. Een situatie waarin duidelijkheid is over wat er met aangiften en meldingen gebeurt, draagt er aan bij dat personen die misstanden signaleren eerder geneigd zijn de verantwoordelijkheid te nemen om deze signalen te delen. De politie, FIOD-ECD en Openbaar Ministerie streven ernaar nog dit najaar afspraken te maken met curatoren over de terugkoppeling van wat er met meldingen en aangiften is of wordt gedaan.

Verbetering van de informatiepositie

Door de inrichting van het eerder genoemde centrale meldpunt voor faillissementsfraude kunnen meldingen worden samengevoegd en geanalyseerd. Hierdoor ontstaat een landelijk beeld en wordt intelligence rondom faillissementsfraude inzichtelijker. Het Openbaar Ministerie laat daarnaast de dienst IPOL een actuele Criminaliteitsbeeldanalyse (CBA) opstellen over de aard en omvang

van faillissementsfraude. Door de Politieacademie is een kenniskring faillissementsfraude opgezet die samenkomt met het doel kennis over faillissementsfraude te vergroten en te verspreiden onder betrokken partijen. Op basis van een verbeterde informatiepositie kan de opsporing met actuele kennis van zaken zo gericht mogelijk worden ingezet.

Inzet van de opsporing

Bij de bestrijding van faillissementsfraude geldt – zoals ook voor andere vormen van fraude – dat er keuzes gemaakt moeten worden over de inzet van capaciteit. Beperkte middelen dienen slim te worden ingezet om zo een optimaal rendement te behalen. Het strafrecht zal met de juiste focus, gericht worden ingezet. In de opsporing van faillissementsfraude spelen de politie en de Fiscale Inlichtingen en Opsporingsdienst (FIOD-ECD) een hoofdrol. De *Aanwijzing Opsporing en Vervolging Faillissementsfraude*, die op 1 maart 2009 in werking is getreden, maakt onderscheid tussen eenvoudige, lichte zaken en complexe, zware zaken. De eenvoudige categorie komt in aanmerking voor opsporing door de regiopolitie. De meer complexe categorie komt in aanmerking voor opsporing primair door de FIOD-ECD en daarnaast de politie. Om te komen tot een versterking van de aanpak van faillissementsfraude maken het Openbaar Ministerie, de politie en de FIOD-ECD voor het einde van dit jaar afspraken waarin deze rolverdeling verder wordt geconcretiseerd en waarin verantwoordelijkheden worden vastgelegd. De opsporing richt zich op die zaken die ertoe doen.

Doeltreffende aanpak van relatief eenvoudige faillissementsfraudezaken

Relatief eenvoudige zaken hebben als kenmerk onder meer het ontbreken van administratie, het niet uitleveren van de bedrijfsadministratie aan de curator en/of het onttrekken van activabestanddelen aan de boedel. Voor de aanpak van dit soort faillissementsfraudezaken maken de politie en het Openbaar Ministerie afspraken om te komen tot een gestandaardiseerde aanpak, gebaseerd op ervaringen met de «korte klap-methode». Hierbij worden gelegenheidsfraudeurs met een kortere doorlooperperiode en met inzet van minder capaciteit dan bij de tot op heden gebruikelijke aanpak vervolgd. Deze aanpak wordt landelijk uitgerold om meer faillissementsfraudezaken aan te pakken.

Bestrijding van complexe faillissementsfraude

Naast gelegenheidsfraudeurs is er ook een groep beroepsfraudeurs die gebruik maakt van onder andere katvangers en complexe constructies. Op dit soort zware zaken richt de FIOD-ECD zich. Het Functioneel Parket van het Openbaar Ministerie en de FIOD-ECD hebben een handhavingsarrangement waarin prioritaire thema's benoemd zijn en de werkwijze voor een effectieve aanpak is opgenomen. De deskundigheid van het FP en FIOD-ECD richt zich op zaken met een grote maatschappelijke impact. Deze zaken worden, conform de *Aanwijzing opsporing en vervolging faillissementsfraude* van het Openbaar Ministerie, geselecteerd op basis van de hoogte van het fraudebedrag, de mate van misbruik van rechtspersonen, de aanwezigheid van ondoorzichtige eigendomsverhoudingen of bestuurdersrelaties of het gebruik van een stroman, een georganiseerd verband, een relatie met andere vermogensdelicten, de branche waarin de fraude speelt en de persoon van de verdachte(n).

De voorbeeldfunctie en normbevestigende werking van de aanpak van dit soort zaken is van groot maatschappelijk belang. De aanpak hiervan vergt veel capaciteit en vereist bijzondere financiële kennis. In dat verband streeft de FIOD-ECD ernaar om (ten opzichte van voorgaande jaren) een veelvoud aan opsporingsuren in te zetten op het doen van onderzoeken naar faillissementsfraude.

5 Concluderend

De voorstellen die het lid Gesthuizen doet, vertonen op veel punten overeenkomsten met de ontwikkelingen en huidige plannen voor de aanpak van ondermijnende criminaliteit, waaronder faillissementsfraude, verder te versterken. De afgelopen jaren is de aanpak van financieel-economische criminaliteit versterkt. Naast een flinke vergroting van de capaciteit is vorm gegeven aan een gezamenlijke geïntegreerde aanpak. Voor fraudebestrijding heeft dit significante verbeteringen tot gevolg gehad in de inrichting, capaciteit en expertise bij de Politie, de FIOD-ECD en het Openbaar Ministerie. Dit is een goede ontwikkeling die door dit kabinet met kracht wordt voortgezet. Om de bestrijding van faillissementsfraude verder te versterken wordt een combinatie van verschillende instrumenten en maatregelen ingezet die elkaar aanvullen en versterken. Hierbij is er aandacht voor preventie, toezicht, civielrechtelijke instrumenten en strafrechtelijke handhaving. Op het terrein van preventie, toezicht en civielrechtelijke instrumenten gaat ondermeer een nieuw systeem van start voor het toezicht op rechtspersonen en wordt de Garantstellings-

regeling Faillissementscuratoren uitgebreid en toegankelijker gemaakt. Daarnaast wordt gewerkt aan bewustwording en verspreiding van kennis en worden nieuwe preventieve instrumenten – naast het inmiddels bestaande strafrechtelijk bestuursverbod – ingericht. Op het terrein van het strafrecht wordt de samenwerking met curatoren verbeterd. Een centraal meldpunt faillissementsfraude wordt ingericht. Afspraken worden gemaakt met de Vereniging van Faillissementscuratoren om in beginsel uitsluitend op een voor de curatoren eenvoudige wijze melding te maken en alleen in relevante gevallen worden aangiften opgenomen. Bovendien wordt de terugkoppeling verbeterd naar degene die melding maakt of aangifte doet. De informatiepositie voor de opsporing en preventie wordt verbeterd door de uitvoering van een Criminaliteitsbeeldanalyse faillissementsfraude. De politie en het Openbaar Ministerie werken aan een landelijke uitrol van een gestandaardiseerde aanpak van relatief eenvoudige faillissementsfraudezaken met het streven meer van dit soort zaken aan te pakken. Tot slot zet de Fiscale Inlichtingen- en Opsporingsdienst in samenwerking met het Openbaar Ministerie significant meer uren in voor de opsporing van complexe zaken. Bij het aanbrengen van verbeteringen in de aanpak van faillissementsfraude heb ik aangegeven dat faillissementsfraude een typisch ketenprobleem is, dat alleen adequaat kan worden aangepakt als alle betrokken partijen samenwerken. Voor een doeltreffende aanpak zijn de overheid en private partijen wederzijds afhankelijk van elkaar. Een geïntegreerde aanpak voorziet in een combinatie van verschillende instrumenten die elkaar aanvullen en versterken, waarbij er aandacht is voor zowel preventie, toezicht, civielrechtelijke instrumenten en strafrechtelijke handhaving.

De minister van Veiligheid en Justitie,

I. W. Opstelten

