Hoe fraudeurs de draad kwijtraken

Hoe fraudeurs de draad kwijtraken

Een juridisch perspectief op
(nieuwe) fraudevormen bij mobiel betalen

Eindrapportage

In opdracht van het
Wetenschappelijk Onderzoek- en Documentatiecentrum
Ministerie van Justitie

Dialogic *innovatie & interactie*
Utrecht, 3 januari 2005

Auteurs
Rudi Bekkers
Frank Bongers
Jeroen Segers
Maurice Schellekens (TILT, Universiteit van Tilburg)

M.m.v.
Andriew Lim (Technische Universiteit Eindhoven)

Inhoudsopgave

Samenvatting

Dit onderzoek gaat over vraag welke nieuwe vormen van fraude kunnen ontstaan als gevolg van technologische en marktontwikkelingen bij mobiele telecommunicatie (in het bijzonder mobiel betalen) en de vraag of het bestaande wettelijke instrumentarium toereikend is om deze (nieuwe) vormen van fraude[1] adequaat te bestrijden. Ter beantwoording van deze vragen (en de afgeleide deelvragen) is een aanpak gevolgd die bestaat uit vier onderdelen: desk research, interviews, het opstellen van varianten van mobiel betalen en een expertbijeenkomst. Het rapport bestaat uit drie onderdelen:

I. De ontwikkeling van mobiel betalen;

II. Fraude bij mobiel betalen;

III. Juridisch kader en instrumenten.

I. De ontwikkeling van mobiel betalen

De markt voor mobiel betalen omvat veel verschillende verschijningsvormen. Er wordt in Nederland al op behoorlijke grote schaal mobiel betaald, onder meer met het gebruik van premium rate SMS-diensten. Er is een aantal nieuwe, meer geavanceerde vormen van mobiel betalen op komst. De verwachtingen voor mobiel betalen in Nederland zijn echter gematigd. De financiële sector stelt dat mobiel betalen geen overtuigende voordelen heeft boven bestaande alternatieven. De kosten en complexiteit zijn aanzienlijk. In Nederland zal mobiel betalen last hebben om de markt te veroveren, omdat de (toonbank)betaalmarkt ver ontwikkeld is (denk aan het pinnen). Betalingen met chipkaarten beginnen - na een valse start - ook serieuze omvang te bereiken. De betalingsmarkt heeft verder een sterk nationaal karakter. Geavanceerde vormen van mobiel betalen vragen echter om een grote, internationale schaal voor kosteneffectieve invoering. De meeste marktpartijen verwachten dat mobiel betalen in eerste instantie nationaal vorm krijgt. De ontwikkeling van verschillende deelmarkten bij mobiel betalen spreidt zich over de tijd uit. De markt voor mobiel betalen zal zich naar verwachting het eerst ontwikkelen als diensten voor het verrichten van microbetalingen voor online content of online diensten. Alleen op deze markt zijn er weinig alternatieven voor mobiel betalen. Ook is er voor telecommunicatieoperators een direct belang bij deze vorm van betalingen: alleen bij voldoende ontwikkelde vormen van online betalingen kunnen de grote uitgaven voor UMTS vergunningen en netwerken worden terugverdiend. Pas later in de tijd volgen respectievelijk de deelmarkten voor lokale microbetalingen, remote macrobetalingen (ook internationaal) en lokale macrobetalingen. De ontwikkelingen bij mobiel betalen zijn nog omgeven door veel onzekerheden. Deze zijn primair niet van technische aard, maar eerder het gevolg van het ontbreken van een sluitende business case voor mobiel betalen.

Er ontwikkelen zich talloze initiatieven van bestaande partijen maar ook van nieuwe markttoetreders. Deze initiatieven, in Nederland en ook daarbuiten, vinden we zowel bij internetbetalingen als bij mobiel betalen. Veel initiatieven hebben echter moeite enige schaal te bereiken en soms verdwijnen ze niet lang na de introductie. Nieuwe toetreders staat dan het failliet in het vooruitzicht. De (vele) internationale normalisatie-initiatieven worden door

[1] Fraude bij mobiele betalen betreft handelingen die (1) een (persoonlijk) geldelijk gewin beogen; (2) intentioneel worden uitgevoerd; (3) een element van misleiding in zich hebben; en (4) gebruikmakend van een mobiel betaalsysteem.

marktpartijen als weinig belangrijk beschouwd. Ze staan ver van de realiteit en spelen nauwelijks in op de nationale context.

In dit rapport zijn vier varianten op mobiel betalen verder uitgewerkt. Deze verschillen onder meer op beoogd gebruik, technische invulling, rollen en verantwoordelijkheden van partijen en de aansluiting op bestaande betaalsystemen. De varianten betreffen achtereenvolgens (1) een mobiele doorontwikkeling van debettransacties via het internet; (2) een volgende generatie prepaid betalingen; (3) mobiele creditcard betalingen en (4) mobiel digitaal muntgeld via wallets. De hoofdrolspelers bij deze varianten zijn achtereenvolgens de banken, de mobiele telecommunicatieaanbieders, creditcard maatschappijen en in het laatste geval nieuwe toetreders en/of banken. Gegeven de grote onzekerheden is het nu nog te vroeg om aan te geven welke van deze varianten de grootste kansen hebben.

II. Fraude bij mobiel betalen

Er kan een onderscheid gemaakt worden tussen zogenaamde relatiefraude (waaronder het gebruik van een valse identiteit) en technische fraude (waarbij gebruik wordt gemaakt van technische onvolkomenheden van het systeem). Op dit moment is bij zowel telecommunicatiediensten als bij betaaldiensten relatiefraude de grootste categorie. Bij de introductie van nieuwe mobiele betaaldiensten verwachten wij echter dat technische fraude (voor enige tijd) de overhand krijgt. Hoewel marktpartijen zich inspannen om ex-ante frauderisico's in kaart te brengen en hun systemen tegen misbruik te beschermen, zijn lang niet alle technische en niet-technische risico's goed te voorspellen. Aanbieders zijn dan ook in belangrijke mate aangewezen op een reactief fraudebeleid. Het is een gegeven dat men deels achter de feiten zal blijven aanlopen. Bestaande fraude-detectiesystemen zijn tot op zekere hoogte bruikbaar in de nieuwe wereld. De huidige systemen van zowel telecommunicatieaanbieders als van financiële partijen kunnen onder meer door geavanceerde patroonherkenning bepaalde type fraudes aan het licht brengen, maar slagen er vaak niet in om geavanceerde, nog niet voorziene vormen van technische fraude op het spoor te komen.

Er bestaan uiteenlopende beelden bij de omvang van fraude en het belang van fraudebestrijding. Nieuwe toetreders lopen een verhoogd risico op schade door fraude. De aandacht voor fraude en effectieve bestrijding is noodgedwongen lager dan bij gevestigde spelers. Fraudeurs zullen inspelen op deze zwakte en zich juist op deze partijen richten. Fraude door criminele organisaties is een serieuze bedreiging. Vooral bij telecommunicatienetwerken zien we goed georganiseerde fraude, gepleegd door grote bendes met internationale vertakkingen, die ook toegang weten te krijgen tot geavanceerde cryptologische kennis, bijvoorbeeld door werkloze Oost-Europese experts in te huren. Met een complexer wordende waardeketen neemt de kans op fraude door bedrijven in de waardeketen ook toe. Reeds nu zijn er bij premium rate nummers talloze min of meer malafide partijen actief. Deze ontwikkeling zet zich mogelijk voort en versterkt als de waarketen complexer wordt en als de diversiteit van diensten (en mogelijkheden daartoe) toeneemt. De technieken waarvan fraudeurs zich bedienen, zijn steeds geavanceerder en steeds meer wordt de mens de zwakke schakel. Een goed voorbeeld is het sterk opkomende phishing: waar experts een jaar geleden nog lacherig deden over eindgebruikers die in dergelijke prakrijken trapten, moeten ze nu toegeven dat zelfs een heel zorgvuldig handelende eindgebruiker bijna niet meer in staat is vast te stellen of een bepaalde dienst of applicatie wel bonafide is.

III. Juridisch kader en instrumenten

Een hoofdconclusie van het onderzoek is dat er op dit moment onvoldoende redenen zijn om grootschalige wijziging/aanvulling van het juridisch kader te legitimeren. Er is te weinig zicht eventuele nieuwe vormen van fraude en marktpartijen verwachten in zijn algemeenheid dat het huidige wettelijk kader voldoet voor toekomstige ontwikkelingen. Dit neemt niet weg dat het verstandig is een vinger aan de pols te houden. We gaan hieronder in op een aantal specifieke juridische gebieden. Overigens wijzen wel alle partijen op de wenselijkheid van een grotere (vervolgings)capaciteit bij het Openbaar Ministerie in relatie tot dit onderwerp.

Strafbaarstellingen

Zoals hiervoor is aangegeven is er in het algemeen nog onvoldoende noodzaak nu al in strafbaarstellingen te voorzien. In een tweetal gevallen behoeft dit uitgangspunt nadere onderbouwing. In het ene geval is strafbaarstelling ons inziens te overwegen, in het andere niet.

Een aparte strafbaarstelling van phishing is te overwegen. Phishing zou strafbaar gesteld moeten worden als een bijzondere vorm van bedrog. Het door enige vorm van misleiding verkrijgen van authenticatiegegevens is een belangrijke voorbereidingshandeling op eigenlijke fraude. Het is echter onzeker of zij – als voorbereidingshandeling - gedekt wordt door de huidige bedrogbepalingen die sterk georiënteerd zijn op vermogenscriminaliteit (en niet zozeer op het verkrijgen van authenticatiegegevens). De strafbaarstelling van phishing zou overigens niet uniek zijn voor mobiele betaalsystemen, maar heeft het karakter van een algemene vorm van computercriminaliteit.

Aanmelding onder valse naam behoeft geen aparte strafbaarstelling. Een andere voorbereidingshandeling betreft het zich onder een valse naam aanmelden voor telecommunicatie- of financiële diensten. Niettemin is het twijfelachtig of hier de noodzaak bestaat om tot een nieuwe strafbaarstelling te komen. Dit is al strafbaar als valsheid in geschrift in die gevallen waarin de naam een bewijsbestemming heeft en dat zal vaak het geval zijn. Bovendien beperkt het de mogelijkheden van degene die om te honoreren redenen hun eigen naam niet willen prijsgegeven.

De status van de aanbieder van een mobiel betaalsysteem

De huidige status quo – op telecommunicatieaanbieders wordt geen enkel prudentieel toezicht gehouden - is instabiel. Op dit moment worden prepaid beltegoeden niet aangemerkt als elektronisch geld in de zin van Richtlijn 2000/46/EG en de WTK 1992 (waarin genoemde richtlijn is geïmplementeerd). De betreffende telecommunicatieaanbieders vallen dan ook niet onder het zogenaamde EGI-regime. De financiële sector ziet hier een ongerechtvaardigde bevoordeling van de telecommunicatieaanbieders. De telecommunicatieaanbieders vrezen dat zij niet kunnen voldoen aan sommige eisen die aan EGI's gesteld worden, zoals solvabiliteit en liquiditeit. Een sui generis regime voor prudentieel toezicht op telecommunicatieaanbieders komt steeds nadrukkelijker in beeld. De sleutel tot de discussie rond het prudentieel toezicht op telecommunicatieaanbieders ligt in Europa. De EC heeft onlangs een publieke consultatie over dit onderwerp afgesloten. De verwachting is dat het onontkoombaar is dat het uitgeven van prepaid beltegoeden onderworpen wordt aan op de financiële activiteiten toegespitste regels over bedrijfsvoering en aan regels over prudentieel toezicht.

Consumentenbescherming

De EGI-discussie heeft ook consequenties voor de consumentenbescherming. Het idee bestaat dat met betrekking tot financiële dienstverlening al een voldoende uitgewerkt regelstelsel tot bescherming van de consument bestaat. Indien telecommunicatieaanbieders als EGI aangemerkt worden, ligt voor de hand dat behalve regelgeving over prudentieel toezicht, de WID en de Wet MOT, ook de betreffende regelgeving met betrekking tot consumentenbescherming bij financiële dienstverlening (Aanbeveling 97/489/EG en de toekomstige implementatie van Richtlijn 2002/65/EG) op hen van toepassing wordt. De consumentenbescherming bij beltegoeden is onduidelijk. Onduidelijk is of Aanbeveling 97/489/EG en de toekomstige implementatie van Richtlijn 2002/65/EG op telecommunicatieaanbieders toegepast kan worden voor zover het hun omgang met prepaid beltegoeden betreft. Gezien de consumentenbelangen die op het spel staan zou dit wel gewenst zijn.

Preventie en zelfregulering

Privacywetgeving is geen blokkade voor het gebruik van zwarte lijsten. Marktpartijen beschouwen het aanleggen van zwarte lijsten als een belangrijk middel tegen fraude. Ze voelen zich echter belemmerd door privacyregelgeving bij het opzetten van desbetreffende databases, vooral indien die een internationaal karakter hebben. Privacywetgeving verbiedt zwarte lijsten niet maar stelt wel bepaalde voorwaarden aan het beheer en de samenstelling van dergelijke lijsten.

Het Convenant tot het tegengaan van Oneigenlijk Gebruik van Informatienummers is een voorbeeld van een redelijk geslaagde vorm van zelfregulering die voorziet in afstemming en samenwerking tussen de betrokken partijen in de telecommunicatiewaardeketen. Bij (ontbreken van) zelfregulering bij mobiel betalen is het aan de overheid de belangen van zwakke partijen te bewaken.

Summary

This study looks into the question which new forms of fraud can emerge in consequence of technological developments and market trends in mobile telecommunications (especially in effecting mobile payments), and whether today's legislative instruments are adequate to satisfactorily combat these (new) forms of fraud[2]. In order to answer these questions (and the derivative sub-questions) we have taken four lines of approach: desk research, interviews, framing variants of mobile payment, and a meeting of experts. The report itself comprises three sections:

(I) Developments in mobile payment;

(II) Fraud with mobile payments

(III) The legal framework and instruments.

I. Developments in mobile payment

The mobile payments market is very diverse. In the Netherlands, mobile payments are made on a considerably large scale and include the use of premium rate SMS services. While several new, more advanced forms of effecting mobile payments are on the horizon, expectations in the Netherlands regarding this form of payment are modest. The financial sector argues that mobile payment has no credible advantage above the current alternatives. The costs and complexity are considerable. Mobile payment will have a hard time winning the market in the Netherlands because the (over-the-counter) payments market here is highly advanced. After having made a false start, payment by chip card is now starting to achieve significant scale. Furthermore, the payments market has a strongly national character. Advanced forms of mobile payment do however require large, international scale if they are to be introduced cost-effectively. Most market parties anticipate that mobile payment will initially expand in the national dimension. Growth of the various sub-markets for mobile payment will be spread out over the course of years. The expectation is that the market for mobile payments will initially develop in the form of services for making micro payments for online content or online services. And yet it is in this market that there are very few alternatives for effecting mobile payments. There is, however, also a direct benefit for telecommunications operators from such forms of payment; only in the case of adequately developed forms of online payments will the substantial costs incurred for UMTS licences and networks be able to be recovered. Only later will the sub-markets for local micro payments, remote macro payments (also international) and local macro payments follow. Developments in mobile payment are still enshrouded in uncertainties. These uncertainties are not primarily of a technical nature, but are rather the consequence of the lack of a sound business case for mobile payment.

Numerous initiatives are taken both by existing parties and new entrants to the market. These initiatives (in the Netherlands and in other countries) are to be seen in Internet payments and mobile payments. Nevertheless, many initiatives fail to achieve adequate scale, and some are even withdrawn from the market not long after their introduction. New entrants are then faced with bankruptcy. The (numerous) international standardisation initiatives are not regarded by the market parties as significant. They are far distanced from reality and take very little advantage of the national context.

[2] Fraud with mobile payments relates to acts that (1) are intended for the purpose of procuring (personal) financial gain; (2) are carried out with intent; (3) contain an element of deception; and (4) make use of a mobile payment system.

Four variants of mobile payment are worked out in detail in this report. They differ in terms of intended use, technical structure, the roles and responsibilities of the parties concerned, and the link with existing payment systems. These variants concern (1) the further development of mobile debit transactions via the Internet; (2) the next generation of prepaid payments; (3) mobile credit card payments and (4) mobile digital cash via wallets. The main players in these variants are banks, the providers of mobile telecommunications, credit card companies, and (for mobile digital cash via wallets) new entrants and/or banks. Given the major uncertainties involved it is too early to say which of these variants has or have the highest chance of success.

II. Fraud with mobile payments

A distinction can be drawn between so-called relational fraud (including using a false identity) and technical fraud (where use is made of technical imperfections in the system). Relational fraud is currently the main category of fraud in both telecommunications services and payment services. Nevertheless we anticipate that technical fraud will (for some time) gain the upper hand with the introduction of new mobile payment services. Although market parties are putting efforts into mapping out the ex-ante fraud risks and in protecting their systems from misuse, not all the technical and non-technical risks can be predicted. Providers will therefore to a large extent have to rely on a reactive fraud policy. It is a fact that the situation will to some extent continue to be overtaken by events. The current fraud detection systems, both of telecommunications providers and financial parties, can bring certain types of fraud to light by using advanced methods of pattern recognition and other systems, yet they are often unsuccessful in detecting advanced, unexpected forms of technical fraud.

There are many views regarding the extent of fraud and the importance of combating it. New entrants run a higher risk of loss from fraud. Out of sheer necessity these players devote less attention to fraud and effectively combating it than established players. Individuals frauds will take advantage of this weakness and focus on this group in particular. Fraud by criminal organisations poses a serious threat. Especially in telecommunications networks do we see highly organised fraud being committed by gangs with international branches who are able to gain access to advanced cryptographic knowledge, for instance by calling in unemployed East-European experts. A value chain which is gradually becoming more complex entails a higher risk of fraud by companies in the value chain too. Even now do we see numerous, more or less fraudulent parties active on premium rate numbers. This trend will probably continue and intensify as the value chain becomes more complex and if there is an increase in the diversity of services (and the relevant possibilities). The techniques used by frauds are constantly becoming more advanced and man is increasingly becoming the weak link in the chain. An appropriate example of this is the rise in phishing; a year ago the experts laughed about end-users that fell far this ruse, but they now admit that it is virtually impossible today for even a very cautious end-user to determine whether a certain service or application is *bona fide* or not.

III. Legal framework and instruments

One of the study's main conclusions is that at the present time there is insufficient reason to validate large-scale changes/supplements to the legal framework. There is too little insight into new forms of fraud, and the market parties generally expect that the current legal framework will be adequate to cope with future developments. Nevertheless, this does not alter the fact that it is still wise to keep a finger on the pulse. We shall deal with several specific legal aspects in the following. Apart from that, all parties point out the desirability of

more scope for the Public Prosecutor (to take legal action) in connection with this subject matter.

Penalization

As was indicated in the above, there is still more or less too little necessity to make provisions for penalization. This point of departure calls for an explanation in two cases. We feel that penalization could be considered in the one, but not in the other.

Special penalization could be considered for phishing. Phishing should be made a punishable offence as a special form of fraud. Obtaining authentication data by any form of deception is a major preparatory act of unadulterated fraud. However, it is still uncertain whether phishing – as a preparatory act – is covered by the current fraud provisions, which are strongly geared towards property crime (and not so much towards obtaining authentication data). While making phishing a punishable offence would not be unique for mobile payment systems, it is characteristic of a general form of computer crime.

Registration under a false name need not be made a separate punishable offence. A preparatory act of quite a different nature is registering for telecommunication or financial services under a false name. Nevertheless, it is still doubtful whether there is the need to create a new punishable offence. It is already punishable as forgery in cases where the name is intended as proof, and this will indeed often be the case. Furthermore it restricts the possibilities open to persons who do not wish to disclose their name for good reasons.

The status of mobile payment system providers

The current *status quo* is unstable; there is absolutely no prudential supervision over telecommunications providers. Today, prepaid phone credit (*beltegoed*) is not regarded as electronic money within the meaning of Directive 2000/46/EG and the WTK 1992 (Credit System (Supervision) Act) (in which the directive is implemented). Therefore the telecommunications providers in question do not fall within the terms of the so-called Electronic Money Institutions (EMI) regime. The financial sector sees this as unjustified preferential treatment of telecommunications providers. Telecommunications providers fear that they are unable to meet some of the requirements imposed on EMIs, such as solvability and liquidity. A *sui generis* regime for prudential supervision over telecommunications providers is coming more distinctly into view. The key to the discussion on prudential supervision over telecommunications providers lies in Europe. The European Commission recently concluded a public debate on this subject. The expectation now is that the issue of prepaid phone credit will inevitably be governed by management regulations geared towards financial activities and regulations on prudential supervision.

Consumer protection

The EMI discussion also has consequences for consumer protection. Regarding the provision of financial services it is felt that there is already an adequately worked out regulatory system to protect consumers. If telecommunications providers are seen as EMI then it is only obvious that besides regulations on prudential supervision, the Compulsory Identification Act (*WID*) and the Disclosure of Unusual Transactions (Financial Services) Act (*WMOT*), other relevant regulations concerning consumer protection in terms of financial services (Recommendation 97/489/EG and the future implementation of Directive 2002/65/EG) could be applicable to telecommunications providers in as far as how they deal with prepaid phone credit. Considering the interests of consumers that are at stake, this would indeed be desirable.

Prevention and self-regulation

Privacy legislation does not stand in the way of using black-lists. Market parties see the drawing up of black-lists as a major tool to combat fraud. Nevertheless, they still feel restricted by privacy regulations when setting up relevant databases, particularly those with

an international character. Privacy legislation does not prohibit blacklisting, but it does impose certain conditions on the management and composition of such lists.

The Agreement to Counteract the Improper Use of Information Numbers is one example of a reasonably successful form of self-regulation that makes provision for coordination and collaboration between the relevant parties in the telecommunications value chain. In (the lack of) self-regulation for mobile payments it is up to the government to safeguard the interests of the weaker parties.

1 Inleiding

Markt- en technische ontwikkelingen bij mobiele netwerken staan wederom in de belangstelling. Naar verwachting komt er de komende tijd een keur aan nieuwe toepassingen op de markt, mede als gevolg van de (wat vertraagde) komst van nieuwe technieken zoals UMTS.

Vooral betaaldiensten staan daarbij in de belangstelling. Het gaat daarbij zeker niet alleen meer om diensten die *via* een mobiel toestel worden afgerekend *en* afgenomen, zoals videojournaals, beursberichten, ringtonen, opnames van voetbaldoelpunten en online games. Het gaat ook om betaaldiensten voor andere goederen en diensten, zoals hotelkamers, concerttickets, parkeermeters, of de formele bevestiging voor de aankoop van waardevolle zaken.

Het Ministerie van Economische Zaken is bijvoorbeeld gestart met het initiatief "betalen via nieuwe media". Dit traject beoogt ondermeer het Nederlandse bedrijfsleven en de consument een prikkel te geven om betalen via nieuwe media - zoals mobiel betalen - meer te gebruiken. Binnenkort verwacht het ministerie in samenwerking met partners uit de waardeketen een kosten-batenanalyse te publiceren voor betalen via nieuwe media en een strategische agenda over dit onderwerp.

Het belang van de ontwikkeling van mobiel betalen wordt ook door de EU onderkend, zoals dat weerklinkt in haar slogan *towards a single payment area*. In de zomer van 2003 verscheen de 'EU Blueprint on mobile payments', gericht op het verkrijgen van reacties vanuit de markt. In het voorjaar van 2004 heeft de Europese Commissie een formele consultatieronde geopend waarin (met name) aanbieders van mobiele communicatie kunnen reageren op de gevolgen van de 'e-money directive.[3]

Vanuit het perspectief van de rechtshandhaving leveren dergelijke ontwikkelingen een aantal interessante vragen op. In de afgelopen jaren is er onder meer vanuit het Ministerie van Justitie al aandacht besteed aan nieuwe ontwikkelingen bij mobiele telecommunicatie. Een workshop (najaar van 2002) heeft inzicht verschaft in allerlei vraagstukken rondom verkeersstromen en de status daarvan vanuit een juridisch perspectief.[4] Niet alleen het voorkomen en bestraffen van fraude, maar ook de inzet van mobiele netwerken ter opsporing van criminele activiteiten (die op zich geheel los kunnen staan van het gebruik van het mobiele netwerk zelf) zijn tijdens die workshop besproken. Mobiel betalen (anders dan de facturering van de telecommunicatiediensten zelf) kwam tijdens deze workshop niet aan bod.

Met het hierboven geschetste, toenemende belang van mobiel betalen en de nieuwe vraagstukken daarbij betreffende fraude, heeft Dialogic in samenwerking met de Universiteit van Tilburg (UvT) voor het Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC) van het Ministerie van Justitie een onderzoek uitgevoerd naar frauderisico's bij mobiele telecommunicatie. Ook de Technische Universiteit Eindhoven heeft bijgedragen aan het onderzoek.

---

[3] Het betreft hier Richtlijn 2000/46/EG van het Europese Parlement en de Raad van 18 september 2000 betreffende de toegang tot, de uitoefening van en het bedrijfseconomische toezicht op de werkzaamheden van instellingen voor elektronisch geld.

[4] Het betreft hier de workshop 'Verkeersgegevens' van 6 september 2002, gehouden door het Instituut voor Informatierecht.

1.1 Vraagstelling en onderzoeksvragen

De volgende vraagstelling staat centraal in het onderzoek:

> *Welke nieuwe vormen van fraude kunnen als gevolg van technologische en marktontwikkelingen bij mobiele telecommunicatie – in het bijzonder mobiel betalen - ontstaan en is het bestaande wettelijke instrumentarium toereikend om deze (nieuwe) vormen van fraude adequaat te bestrijden?*

Bij deze vraagstelling passen de volgende onderzoeksvragen:

1. Hoe zien de technologische ontwikkelingen er op hoofdlijnen uit?
2. Wat zijn de gevolgen van deze ontwikkelingen voor de "factureringsrelaties" en voor het opereren van telecommunicatieaanbieders in de markt? Zullen de telecommunicatieaanbieders zich gaan transformeren tot een ander type dienstverlener?
3. Welke (nieuwe) marktpartijen zullen betrokken zijn? Zal er een nieuw type (financiële) dienstverlener ontstaan?
4. Tot welke (nieuwe) vormen van fraude zouden in de diverse varianten van mobiel betalen de technologische ontwikkelingen kunnen leiden?
5. Hoe anticiperen de aanbieders van telecommunicatiediensten en van toegevoegdewaardediensten daarop?
6. Is het bestaande wettelijke instrumentarium toereikend om deze (nieuwe) vormen van fraude adequaat te bestrijden?
7. Zo niet, op welke terreinen bestaan lacunes? Hoe kunnen deze lacunes gedicht worden? Kan buitenlandse wetgeving hierbij als voorbeeld dienen?
8. In hoeverre bieden (parallelle) nieuwe technische ontwikkelingen ook *oplossingen* voor de bestrijding of preventie van de onderzochte vormen van fraude?

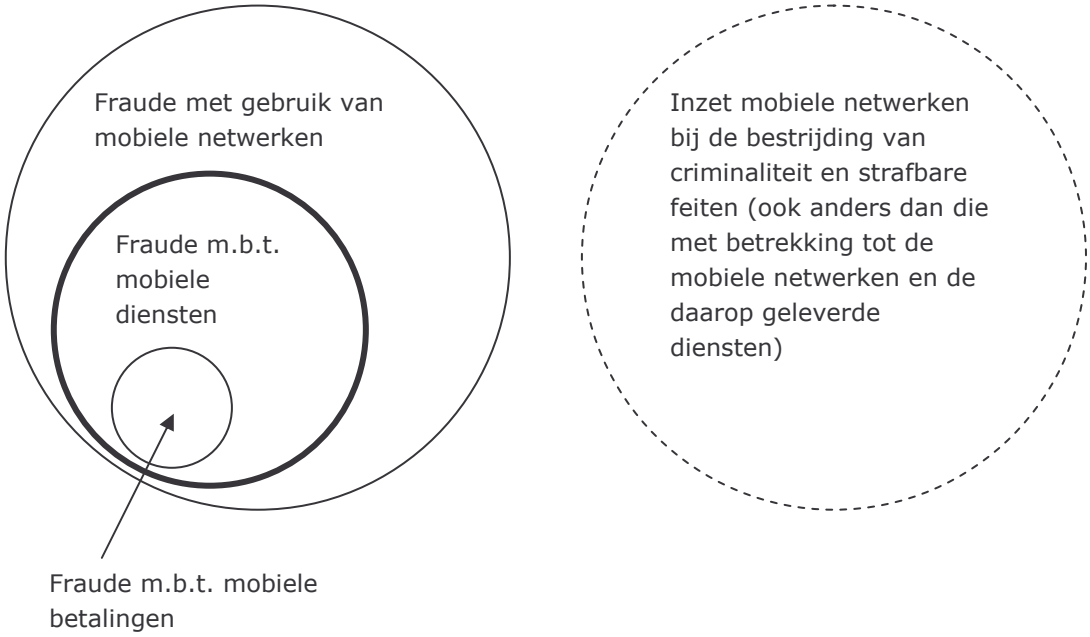
1.2 Afbakening

Risico's met betrekking tot frauduleuze en criminele activiteiten liggen breder dan alleen daar waar betalingsprocessen in beeld komen. Toch is enige afbakening gewenst. Er zijn immers veel manieren waarop mobiele telecommunicatie ingezet kan worden bij fraude. Het onderzoek richt zich dan ook op vormen van fraude met betrekking tot het afnemen van diensten via mobiele netwerken, met de nadruk op betalingsdiensten. Het gaat hier zowel om betaling van diensten die via mobiele communicatie geleverd worden als om betalingen van andere diensten en producten. De bedoelde mobiele netwerken omvatten de huidige netwerken maar ook nieuwe ontwikkelingen zoals WiFi.

Deze afbakening is grafisch in figuur 1 weergegeven. We benadrukken daarbij nog eens dat het onderzoek *niet* gaat om het gebruik van (gegevens uit) mobiele netwerken bij de *bestrijding* van criminaliteit en strafbare feiten[5] – voorzover ze niet direct samenhangen met de hierboven genoemde afbakening.

Binnen de gekozen afbakening speelt fraude met betrekking tot mobiele betalingen een grote rol.

[5] Denk aan de moord op de Franse prefect Claude Erignac in Corsica 1998. De dader bleek net voor de moord zijn mobiele telefoon te hebben gebruikt. Gegevens opgeslagen in het telefoonnetwerk hebben vervolgens de politie geleid naar de moordenaar en hebben een rol gespeeld in de rechtszaak.



Figuur 1: Afbakening van het onderzoek

1.3 Onderzoeksaanpak

Ter beantwoording van de onderzoeksvragen zijn verschillende instrumenten ingezet, waaronder desk research, interviews, opstellen van varianten mobiel betalen en een expertbijeenkomst.

1.3.1 Desk research

Desk research bestaat uit een literatuur- en internetverkenning. Deze verkenning levert een lijst op met relevante bronnen zoals artikelen, rapporten, wetboeken en websites over mobiel betalen, vormen van fraude en relevante wet- en regelgeving. De bronnen staan vermeld in de literatuurlijst. Deze bronnen zijn geanalyseerd met het oog op technologische ontwikkelingen, consequenties van deze ontwikkelingen, vormen van fraude, opsporingsinstrumentarium en betrokken partijen. Het resultaat van deze analyse komt op verschillende plekken terug in dit rapport. Een van de resultaten betreft bijvoorbeeld een *generieke waardeketen* voor mobiel betalen. De analyse is tevens gebruikt om een vragenlijst op te stellen voor de interviewronde.

1.3.2 Interviews

De tweede stap in het onderzoek betreft een interviewronde langs relevante partijen uit de waardeketen mobiel betalen, zoals banken, aanbieders van mobiele telecommunicatie (telco's), creditcardmaatschappijen en dienstenleveranciers. In totaal zijn twaalf personen geïnterviewd. In Bijlage 4 staat een lijst met geïnterviewde personen en de vragenlijst. De resultaten van de interviews zijn geanonimiseerd verwerkt in het eindrapport.

1.3.3 Varianten mobiel betalen

Op basis van de generieke waardeketen zijn aan de hand van de resultaten uit de desk research en de interviews vier varianten van waardeketens voor mobiel betalen opgesteld. Binnen elke variant speelt een verschillende partij, techniek of mobiele betalingsmethode een hoofdrol. Per variant zijn identieke en verschillende vormen van fraude denkbaar. Deze varianten zijn vervolgens tegen het licht gehouden van het *bestaande wettelijke*

instrumentarium. Op deze wijze kunnen eventuele tekortkomingen in wet- en regelgeving bij het bestrijden van frauderisico's worden geïdentificeerd.

1.3.4 Expertbijeenkomst

De laatste stap in de dataverzameling betreft een expertbijeenkomst op het WODC. Een lijst met deelnemers staat in Bijlage 5. Tijdens deze bijeenkomst zijn twee onderwerpen aan de orde gekomen, namelijk (1) een bespreking van bestaande en nieuwe vormen van fraude bij mobiel betalen; (2) een bespreking van de mate waarin het huidige recht uitgerust is om deze (nieuwe) vormen van fraude te bestrijden en de aanpassingen die eventueel noodzakelijk zijn. De input van deze bijeenkomst vormde de resultaten uit voorgaande onderzoeksstappen zoals een lijst met (nieuwe) vormen van fraude en de vier varianten van mobiel betalen.

1.4 Leeswijzer

Het rapport is opgebouwd uit drie delen, namelijk de ontwikkeling van mobiel betalen (deel I), fraude bij mobiel betalen (deel II) en juridisch kader en instrumenten (deel III).

I. De ontwikkeling van mobiel betalen

Het eerste deel van dit rapport (hoofdstuk 2 tot en met 4) schetst recente ontwikkelingen in mobiel betalen. In hoofdstuk 2 wordt een beeld geschetst van drie vormen van betalen, namelijk traditioneel betalen, betalen via internet en mobiel betalen. Voorts komen de verschillende partijen uit de waardeketen en de belangen van deze partijen aan de orde (hoofdstuk 3). Dit deel sluit af met een globale beschrijving van verschillende ontwikkelingsvarianten van mobiel betalen (hoofdstuk 4).

II. Fraude bij mobiel betalen

Na een uitleg van ontwikkelingen in mobiel betalen (deel I) gaat deel II (hoofdstuk 5 tot en 7) in op mogelijke vormen van fraude die bij mobiel betalen een rol kunnen spelen. Dat gaat in drie stappen. Eerst wordt aandacht besteed aan bestaande vormen fraude bij mobiele telecommunicatiediensten (hoofdstuk 5). Daarna komen bestaande en nieuwe vormen van fraude bij betaaldiensten aan de orde (hoofdstuk 6 en 7).

III. Juridisch kader en instrumenten

Wanneer bekend is welke bestaande en nieuwe vormen van fraude een rol kunnen spelen bij mobiel betalen (deel II) is het mogelijk om vast te stellen of bestaande wet- en regelgeving voldoende uitgerust is om deze fraude te bestrijden. Deze vraag staat centraal in deel III (hoofdstuk 8 en 9). Hoofdstuk 8 beschrijft het juridische kader (o.a. relevante rechtsgebieden). Hoofdstuk 9 gaat in op de doeltreffendheid van het juridische kader en de doeltreffendheid van het juridische instrumentarium.

Het rapport sluit af met een hoofdstuk met conclusies, waarin tevens een aantal punten voor discussie worden gegeven (hoofdstuk 10).

Deel I: De ontwikkeling van mobiel betalen

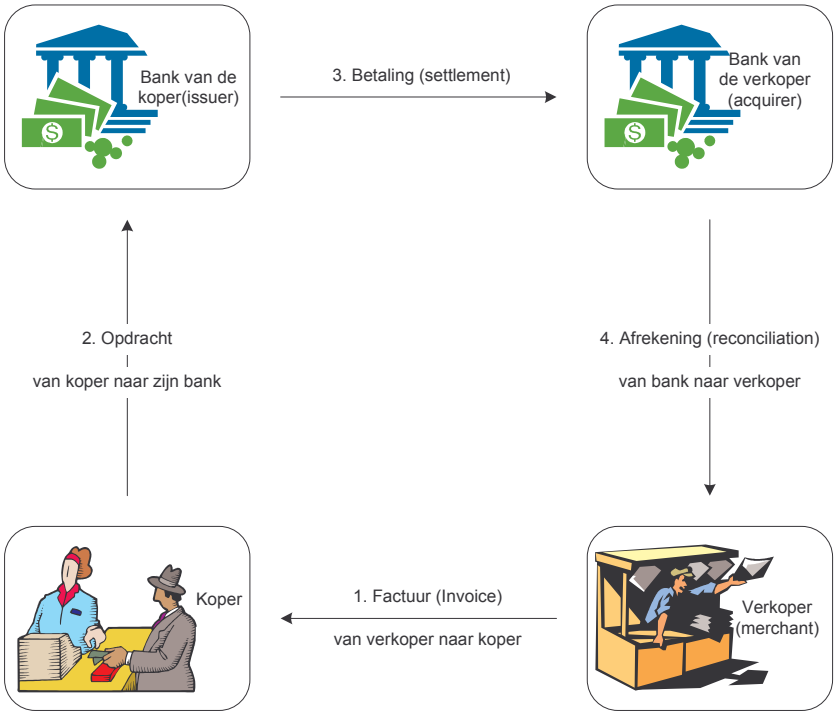
2 Betalen: traditioneel, via internet en mobiel

2.1 Inleiding

Dit hoofdstuk presenteert een structuurschets van een betalingstransactie die in het rapport wordt gebruikt om partijen en processen te identificeren (paragraaf 2.2). Omdat mobiel betalen haar oorsprong vindt in zowel de traditionele markt als in de markt voor betalen via internet, worden deze twee markten kort beschreven (paragrafen 2.3 en 2.4). In paragraaf 2.5 wordt mobiel betalen gedefinieerd. Het hoofdstuk vervolgt met drie categorieën om mobiel betalen te classificeren (betaling naar omvang, moment en samenhang dienst en locatie). De laatste paragraaf is een samenvatting en conclusie. Hoewel dit hoofdstuk geen onderzoeksvraag beantwoordt, legt het wel een (begrippen)basis voor de volgende hoofdstukken.

2.2 Basisonderdelen van een betaaltransactie

Bij een betaling van een koper aan de verkoper zijn over het algemeen vier partijen betrokken: de koper, de verkoper en twee financiële instellingen die de betalingstransactie onderling afhandelen. De onderlinge communicatie tussen de partijen is steeds verder geautomatiseerd, dit verschilt echter per schakel in de betalingscirkel (weergegeven in figuur 2).



Figuur 2: Schematische weergave van de betalingscirkel

De verschillende transacties worden hieronder beschreven:

1. De betalingstransactie wordt geïnitieerd door de koper die besluit een bepaald goed aan te schaffen. De verkoper presenteert de koper daarvoor een rekening ('invoice'). Dit gebeurt ter plekke van de verkoop ('toonbankbetaling') of de verkoper stuurt de rekening naar de klant. Dat laatste is beperkt gedigitaliseerd. Veelal wordt een acceptgiro of een papieren rekening gestuurd.
2. De koper geeft zijn bank de opdracht om een bedrag over te maken. In de laatste jaren is er grote verscheidenheid ontstaan in elektronische betaalsystemen die het opgeven van de opdrachten aan de bank ondersteunen (zie bijvoorbeeld paragraaf 2.4).
3. Het interbancaire betalingsverkeer voor de afhandeling van de onderlinge betalingsopdrachten is de schakel in de betalingscirkel met de hoogste graad van elektronische communicatie.
4. De laatste schakel bestaat uit het versturen van de bankafschriften en ontvangstbewijzen (voor boekhoudkundige doeleinden) vanuit de bank naar de verkoper. Dit is voor grote bedrijven grotendeels al mogelijk via digitale kanalen en in toenemende mate ook voor kleinere bedrijven.[6]

Deze schematische weergave is het uitgangspunt om verschillende toekomstige (mobiele) betalingsystemen te beschrijven.

2.3 Overzicht van de traditionele betalingsmarkt

Velen zullen de grote verschuivingen in de betalingsmarkt in de laatste twee decennia hebben opgemerkt. Twintig jaar geleden waren voor grotere betalingen in winkels contant geld en euro- of girocheques gemeengoed. Pinbetalingen hebben deze rol grotendeels overgenomen. De genoemde cheques bestaan zelfs nog maar amper. Ook het gebruik van creditcards is sterk gegroeid.

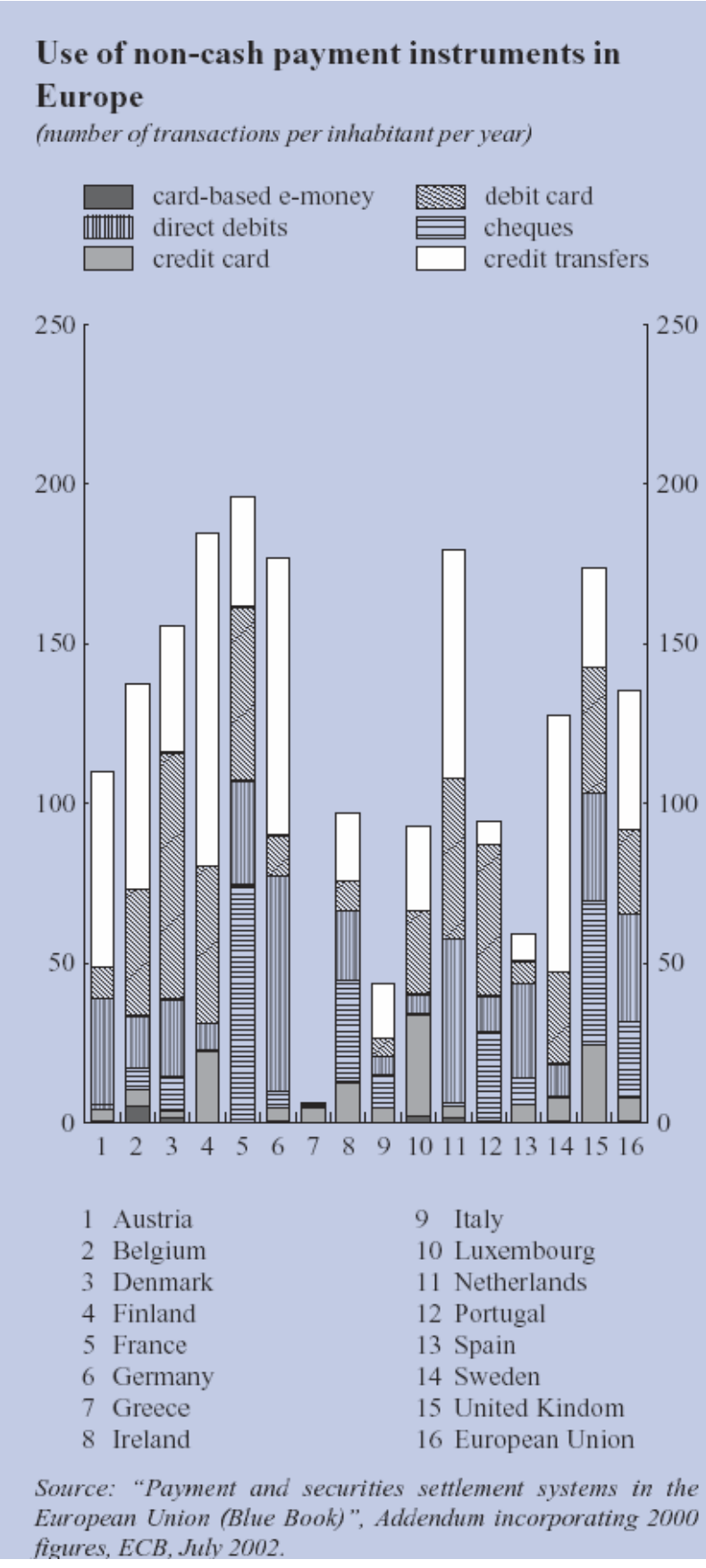
Overigens zijn niet alle introducties van nieuwe betaalsystemen, zoals pinnen, succesvol. Pogingen om in de tweede helft van de jaren negentig kaartgeld in de vorm van de chipper en chipknip in te voeren waren minder fortuinlijk. De consumentenadoptie verliep veel trager dan verwacht en één van de systemen (de chipper) moest het veld ruimen. Pas nu begint het gebruik van de overgebleven chipknip gestaag toe te nemen, ondermeer omdat chippen soms de enige betalingsmogelijkheid is (bijvoorbeeld bij parkeerautomaten in Rotterdam). Hoewel SMS betalingen later doordrongen waren er in 2002 ongeveer 150 miljoen SMS betalingen, terwijl het aantal betalingen per chipknip ongeveer de helft was.[7]

Opmerkelijk aan de markt voor betaalmiddelen is dat ze een uitgesproken nationale statuur kent (zie figuur 3). De verschillende Europese landen, en ook landen daarbuiten, zijn uitgesproken divers waar het om het aandeel van de diverse betaalmiddelen betreft. De verwachtingen voor mobiel betalen in Nederland zijn gematigd. Veel partijen in de financiële sector stellen dat mobiel betalen geen overtuigende voordelen heeft boven de alternatieven, zoals pinbetalingen. Daarnaast zijn de kosten voor de introductie van mobiel betalen aanzienlijk. De introductie is een complexe zaak en als er niet snel een grote schaal wordt bereikt zullen de processing kosten per transactie hoger blijven dan die van andere betaalmiddelen. Alleen in de deelmarkt van betalingen van on-line content wordt mobiel betalen op de korte tot middellange termijn behoorlijke kansen toegedicht. Ook de wat slechtere economische vooruitzichten worden genoemd als een reden waarom de verwachtingen omtrent mobiel betalen naar beneden zijn bijgesteld.

---

[6] Zie onder meer European Central Bank, 2003.

[7] Lelieveldt, 2003.



Figuur 3: Gebruikte betalingsinstrumenten per land, m.u.v. contact geld (overgenomen uit European Central Bank, 2003).

2.4 Ontwikkelingen op het gebied van internetbetalingen

Gestaag neemt het aantal kooptransacties via internet toe. Het kan daarbij gaan om de bestelling van fysieke goederen of diensten, zoals de aanschaf van een boek in een webwinkel of de aanschaf van een vliegticket. Een andere belangrijke categorie betreft (informatie)goederen die ook direct via internet worden afgeleverd, zoals een liedje gekocht in Apple's iTunes winkel of een online geleverd stuk software.

Op internet wordt gebruik gemaakt van een breed scala aan betaalmiddelen. Het gaat daarbij voornamelijk om bestaande betaalmiddelen die al dan niet (beperkt) zijn aangepast aan de internetomgeving. De meest traditionele betaalmiddelen zijn: (1) betaling per bank vooraf, (2) acceptgiro, (3) rembourszending en (4) op rekening leveren. Geen van deze middelen maakt on-line levering met directe betaling mogelijk.

De volgende tabel geeft een niet-uitputtend overzicht van betaalmethoden die wel on-line kunnen worden gebruikt. Een aantal methoden kent meer of minder serieuze problemen. Enkele categorieën lichten we hieronder nog nader toe.

Het grootste probleem voor de verkoper bij creditcardbetalingen (die zonder fysieke handtekening of pincode zijn geplaatst) is dat de kaarthouder een betaling tot zes maanden na de transactie terug kan draaien ('chargeback'). Vervolgens is het aan de verkoper om aan te tonen dat er wel degelijk een dienst of product geleverd is. Klanten kunnen dit mechanisme misbruiken of ze kunnen een chargeback inzetten als er sprake is van vermeende wanprestatie. Deze mogelijkheid tot chargeback leidt tot schade en kosten bij de verkoper van diensten en producten. Bij (doorlopende) machtigingen is iets vergelijkbaars aan de hand. Daar kunnen klanten ook de betaling annuleren (in dit geval tot 35 dagen na de overboeking). De invoering van een elektronische handtekening kan soelaas bieden. De extra zekerheden die een dergelijke handtekening biedt - ook aan de consument - maken het onnodig om ook een recht op chargeback c.q. storneren te verlenen.

Zogenaamde intermediaire partijen spelen een rol tussen verkoper en koper. Dat werkt als volgt:

1. Na het aangaan van de overeenkomst betaalt de afnemer aan de intermediair;
2. De intermediair meldt de betaling aan de leverancier die vervolgens het product levert;
3. De klant bevestigt de ontvangst van het goed;
4. De intermediair maakt het ontvangen bedrag over naar de leverancier.

Deze intermediaire functie – ook aangeduid als escrow - is een elegante manier om het wederzijdse vertrouwensprobleem uit de weg te gaan.

Tabel 1: Methoden voor on-line internetbetalen

Betaalmethode	*Eventueel probleem*	*Mogelijke oplossingen*
Creditcard, zonder handtekening	Chargeback, hoge transactiekosten, vertrouwensprobleem consumenten	Elektronische handtekening
Doorlopende machtiging	Stornering, alleen in Nederlandse context	Elektronische handtekening
Directe on-line bankbetaalopdracht (zoals RaboDirect)	Omslachtig met betaalpas, pincode en/of crypte-rekenmachine, specifieke invulling voor Nederlandse context	Integratie in de website van de dienstverlener, zodat proces zo veel mogelijk automatisch in gang wordt gezet en vereenvoudigd
Pinautomaat bij de PC	Hoge kosten voor de brede uitrol van persoonlijke pinautomaten	Grote schaal bereiken
Intermediairs ('escrows')	Extra partij in de waardeketen, schaal nodig om transactiekosten te beperken bekendheid te krijgen	Zijn reeds een oplossing op zichzelf

Enkele problemen bij betalen via internet betreffen:

- Bij veel betalingsmethoden zijn de transactiekosten zodanig hoog dat betalingen van kleine bedragen (micropayments) geen haalbare zaak is.
- Consumenten zijn huiverig om gevoelige gegevens zoals creditcardgegevens via internet uit te wisselen.
- Betalingen met creditcard of doorlopende machtigingen kunnen door de consumenten herroepen worden, wat leidt tot risico's en kosten bij de leverancier.

Recent is een relatief groot aantal nieuwe betaalsystemen geïntroduceerd die zich (voornamelijk) richten op internetbetalingen zoals Switchpoint (KPN), Tootz (ING), Wallie-card, Firstgate, Moxmo, Way2Pay, Rabo Direct Betalen, Secoin en Minitix. Sommige van deze initiatieven zijn overigens inmiddels gestaakt, wordt ' passief' voortgezet[8] (Way2Pay) of zijn zelfs failliet gegaan Moxmo). Voor een overzicht van initiatieven, zie Bijlage 6.

Sommige systemen worden bekritiseerd, omdat ze onaanvaardbare risico's voor consumenten met zich zouden meebrengen. De Switchpoint Incasso dienst van KPN bijvoorbeeld kwam enkele malen negatief in het nieuws. Zo zou bijvoorbeeld een hacker er in geslaagd zijn in het computersysteem te geraken.[9] Ook stelt aan aantal organisaties vast dat de dienst te gevoelig is voor misbruik. De in de praktijk veelgebruikte draadloze thuisnetwerken zouden het een peulenschil maken om opdracht te verlenen geld van de rekening van de buurman af te

[8] Hiermee wordt bedoeld dat huidige klanten nog wel worden bediend maar dat er geen nieuwe klanten meer worden toegelaten.

[9] *Site SwitchPoint Incasso beklad door hacker*, WebWereld, 8 september 2004.

schrijven. Recent oordeelde het Ministerie van EZ echter dat ze een opt-in regeling, waar organisaties op hadden aangedrongen, niet nodig achtte.[10]

2.5 Basisvormen bij (mobiel) betalen

Mobiel betalen wordt hier gedefinieerd als elke betalingsdienst waarbij een mobiele telefoon en/of een mobiel telefonienetwerk wordt gebruikt. Met een betalingsdienst wordt hierbij bedoeld een financiële transactie ten gunste van een derde partij (niet de aanbieder van de betalingsdienst zelf) voor het leveren van producten of diensten (al dan niet on-line). Merk op dat met deze definitie ook de huidige premium rate telefoniediensten en premium SMS diensten onder het begrip mobiel betalen vallen. Ook wanneer een gebruiker vanaf een mobiele telefoon de girofoondienst gebruikt en een overboeking plaatst, valt dat binnen onze definitie van mobiel betalen. Uiteraard omvat mobiel betalen ook nieuwe en meer geavanceerde vormen.

Hoewel deze definitie op het eerste gezicht helder lijkt, zijn er toch grensgevallen. Als louter in de plastic behuizing van een mobiele telefoon een RFID-chip is aangebracht die vervolgens wordt gebruikt voor een betaling, gaat het dan wel om mobiel betalen? Juist vanwege het explorerende karakter van deze studie hanteren we een brede interpretatie en laten we dat er wel onder vallen.

Bij mobiele betalingssystemen kunnen we onderscheid maken tussen zogenaamde girale en niet-girale systemen. Bij de eerste categorie wordt het bedrag direct ten laste gebracht van de bankrekening van de koper. Dit kan bijvoorbeeld bij mobiel pinnen. Bij de tweede categorie, niet-girale systemen, wordt het bedrag ofwel afgeboekt van een vooruitbetaald bedrag (het prepaid beltegoed of een vooraf opgeladen wallet) of wordt een (leveranciers)krediet verstrekt. Voorbeelden zijn het betalen via de telefoonrekening (prepaid, postpaid of een combinatie daarvan), een wallet, of een creditcard. Vaak, maar niet altijd, wordt een girale transactie gebruikt om het vooruit te betalen bedrag of het achteraf te vergoeden credit te verrekenen. Een groter aantal kleinere of grotere transacties kunnen daarbij worden opgespaard.

In tabel 2 zijn de genoemde categorieën nog een slag verder uitgewerkt.

[10] EZ eist geen aanpassing SwitchPoint Incasso, WebWereld, 7 september 2004.

Tabel 2: Oorsprong van het te betalen bedrag

Giraal	Debet-betaalrekening	Het bedrag wordt direct bij de afwikkeling van een lopende bankrekening afgeboekt
Niet-giraal, postpaid	Credit	Het bedrag wordt ten laste van een creditcard account gebracht. Op het einde van de maand wordt het totale uitstaande krediet in rekening gebracht.
Niet-giraal, prepaid	Server-based e-wallet	Vooraf moet een beurs (ook wel met wallet of purse aangeduid) worden opgeladen. Bij de betaalopdracht wordt opdracht gegeven het betreffende bedrag over te maken naar de begunstigde. De hoogte van het bedrag wordt op een centrale plaats bijgehouden.
Niet-giraal, prepaid	Local e-wallet	Als bij server-based e-wallet. In dit geval wordt het tegoed echter lokaal bijgehouden (zoals op een chipkaart of in een mobiele terminal)
Niet-giraal, prepaid	Pre-paid / belbundel	Feitelijk een vorm van een server-based e-wallet die gebruikt wordt voor het betalen van mobiele telefoniediensten. Kan mogelijk ook gebruik worden voor het betalen voor andere diensten. In het geval van een bundel wordt de beurs op overeengekomen momenten automatisch opgeleden met een bepaald bedrag.
Niet-giraal, postpaid	Telefonie-abonnement	Het betaalde bedragen worden eenmaal per maand in rekening gebracht bij de gebruiker. In feite een debet-systeem, maar het bedrag wordt niet direct van een lopende betaalrekening geboekt. Dit proces wordt ook vaak met *billing* aangeduid.

De keuze voor de hierboven gepresenteerde categorieën is vooral ingegeven door de praktijk. Ze sluiten elkaar dan ook niet volledig uit. Zo is er bij mobiele telefonie vaak sprake van een combinatie tussen een abonnementssysteem en prepaid. Wanneer het tegoed op is, worden extra gesprekken afgerekend alsof het een abonnee betreft.

2.6 Drie categorieën bij mobiel betalen

De omvang van betalingen loopt uiteen. Vaak wordt een onderscheid gemaakt tussen micro- en macrobetalingen, ofwel kleine en grote bedragen. Er is geen algemene consensus bij welk bedrag microbetalingen ophouden en macrobetalingen beginnen. Ook wordt soms een additionele categorie minibetalingen gehanteerd. Voor het doel van dit rapport hanteren we drie categorieën: microbetalingen voor transacties tot 5 euro, macrobetalingen voor transacties van 25 euro of hoger en minibetalingen voor de categorie daartussen.[11]

Net zoals bij het gewone betalingsverkeer ('toonbankbetalingsverkeer') zijn niet alle systemen gelijk geschikt voor grote en kleine betalingen. Dat heeft vooral te maken met transactiekosten. Recent heeft het Maatschappelijk Overleg Betalingsverkeer een analyse

[11] Een van de interviewrespondenten vindt dat de markt een geforceerd onderscheid maakt tussen macro- en microbetalingen. Het gaat in elke situatie gewoon om betalingen. Uiteindelijk ontstaat er volgens deze respondent per definitie een mix van betalingsinstrumenten voor een mix van betalingssituaties. Vergelijk dat met de variatie van betalingsinstrumenten in de huidige portemonnee.

gedaan naar de kosten van diverse betaalproducten.[12] Hieruit blijkt dat de totaal gemaakte kosten voor betaaltransacties op jaarbasis ongeveer 400 euro per Nederlands huishouden bedragen. De in Nederland veelgebruikte pinbetalingen scoren qua kosten relatief gunstig, vandaar de uitspraak 'je kunt niet winnen van pinnen'. Vanaf een omvang van circa elf euro zijn met deze betalingen minder kosten gemoeid dan met betalen met contant geld. De chipknip is altijd het goedkoopste, terwijl de creditcard in alle gevallen het duurste betaalinstrument is. Bij de geschiktheid voor bepaalde betalingen spelen naast kosten ook andere overwegingen een rol. Het is om diverse redenen onwenselijk een chipknip met zeer grote bedragen op te laden.

Tabel 3 is voor diverse *mobiele* betaalmethoden indicatief aangegeven hoe geschikt die zijn voor transacties van een bepaalde omvang.

Tabel 3: Betalingmethoden naar omvang

Betalingsmethode / *Betalingsomvang*	*Giraal*	*Niet-giraal*		
	Mobiele pinbetalingen	Prepaid beltegoed	Wallet	Creditcard
Microbetalingen (Transacties tot 5 euro)	-	+	+	-
Minibetalingen (Transacties van 5 tot 25 euro)	+	0	0	0
Macrobetalingen (Transacties van 25 euro of hoger)	+	-	-	+

- betalingsmethode is niet geschikt / wordt niet gebruikt

0 betalingsmethode heeft geen voorkeur

+ betalingsmethode is geschikt / wordt gebruikt

Een ander onderscheid betreft het moment van de betaling ten opzichte van het moment van de levering. Tabel 4 geeft daarbij drie categorieën weer.

Tabel 4: Betalingsmoment

Betaling vooraf	De levering van het goed, de dienst of de content vindt plaats nadat de begunstigde daadwerkelijk de betaling ontvangen heeft.
Directe betaling	Betaling vindt plaats op (min of meer) hetzelfde moment als de afrekening.
Betaling achteraf	Betaling vindt plaats nadat het goed, de dienst of de content feitelijk geleverd is (zoals bij een remboursdienst).

Een derde onderscheid, naast omvang van de transactie en het betalingsmoment, is de relatie tussen betalingsdienst en locatie. Van onder meer creditcard betalingen kennen we daar al van oudsher de categorieën local en remote payments. Bij mobiele betalingen kan daar een derde

[12] Maatschappelijk Overleg Betalingsverkeer, 2004.

categorie bijkomen: het betalen van een product of dienst die direct via de telefoon wordt geleverd, zoals informatiediensten, content (beeld, geluid), ringtonen en logo's.

Tabel 5: Relatie dienst en locatie

Local payments	Betalen van diensten of goederen op een verkoop- of servicepunt (al dan niet bemand). Voorbeelden: benzinestation, frisdrankautomaat, winkel.
Remote payments	Betalen van diensten of goederen op afstand. Voorbeelden: het vooraf kopen van een concertticket, betalen van een product dat via internet is besteld.
Mobile delivered content payments	Betalen van content of een mobiele dienst die via de mobiele terminal zelf wordt afgeleverd. Ook wel aangeduid als 'digital content' of 'Mobile delivered content'

Een belangrijk element bij mobiel betalen is de authenticatie ten behoeve van de financiële transactie. Voor telecommunicatiediensten is de identiteit van de gebruiker afdoende vastgesteld met de SIM-kaart en de daarmee samenhangende voorzieningen (zoals de pincode). Voor deze telecommunicatiediensten is deze beveiliging afdoende, maar bij betalingstransacties worden meestal hogere eisen gesteld aan de authenticatieprocedure. Dit kan technisch op een aantal wijzen worden ingevuld (paragraaf 4.7 gaat hier dieper op in).

2.7 Samenvatting en conclusies

Betalen, of het nu traditioneel, via internet of mobiel gebeurt, heeft een aantal gemeenschappelijke kenmerken. Er zijn vier partijen betrokken bij een betaaltransactie, namelijk een koper, een verkoper en twee financiële instellingen die de betalingstransactie onderling afhandelen.

Traditionele betalingstransacties worden ondersteund met verschillende betalingsinstrumenten. In Nederland zijn in vergelijking met andere Europese landen pinbetalingen en acceptgiro's populair. De creditcard is minder doorgedrongen en de cheque is uit het straatbeeld verdwenen. Overigens blijkt dat Europese landen grote verschillen kennen ten aanzien van de populariteit van verschillende betalingsinstrumenten.

Het aantal kooptransacties via internet neemt toe. Het gaat daarbij om de bestelling van fysieke goederen of diensten (boeken, vliegtickets, DVD's, etc.) en (informatie)goederen die direct via internet worden afgeleverd (software, games, muziek, etc.). Op internet wordt gebruik gemaakt van een breed scala aan betaalmiddelen. Het gaat daarbij voornamelijk om bestaande betaalmiddelen die al dan niet (beperkt) zijn aangepast aan de internetomgeving. De meest traditionele betaalmiddelen zijn betaling per bank vooraf, acceptgiro, rembourszending en op rekening leveren. Geen van deze middelen maakt online levering met directe betaling mogelijk. Methoden voor betalen via internet zijn creditcard (zonder handtekening), doorlopende machtiging, directe online betaalopdracht (bijv. RaboDirect), pinautomaat bij de PC en intermediairs (zgn. escrows).

Mobiel betalen wordt gedefinieerd als elke betalingsdienst waarbij een mobiele telefoon en/of een mobiel telefonienetwerk wordt gebruik. Met een betalingsdienst wordt hierbij bedoeld een financiële transactie ten gunste van een derde partij (niet de aanbieder van de betalingsdienst zelf) voor het leveren van producten of diensten (al dan niet on-line). Deze definitie omvat ook de huidige premium rate telefoniediensten en premium SMS diensten. Ook wanneer een gebruiker vanaf een mobiele telefoon de girofoondienst gebruikt en een overboeking plaatst,

valt dat binnen onze definitie van mobiel betalen. Uiteraard omvat mobiel betalen ook nieuwe en meer geavanceerde vormen. Bij mobiele betalingssystemen wordt een onderscheid gemaakt tussen girale en niet-girale systemen. Bij girale systeem wordt het te betalen bedrag direct ten laste gebracht van de bankrekening van de koper Dit kan bijvoorbeeld bij mobiel pinnen. Bij niet-girale systemen wordt het bedrag ofwel afgeboekt van een vooruitbetaald bedrag (het prepaid beltegoed of een vooraf opgeladen wallet) of wordt een (leveranciers)krediet verstrekt.

Bij mobiel betalen worden drie categorieën onderscheiden. De eerste categorie betreft de omvang van het bedrag. Hierbij wordt een onderscheid gemaakt tussen micro- en macrobetalingen. De tweede categorie betreft het moment van de betaling ten opzichte van de levering. Hierbij wordt een onderscheid gemaakt tussen betaling vooraf, directe betaling en betaling achteraf. De laatste categorie legt een verband tussen de betalingsdienst en de locatie. Er zijn betalingen bij het verkoop- of servicepunt, zoals een benzinestation (local payments). Er zijn betalingen op afstand, bijvoorbeeld voor producten die via internet zijn besteld (remote payments). Tenslotte zijn er betalingen van content of mobiele diensten die via de mobiele terminal zelf worden afgeleverd (mobile delivered content payments).

De markt voor mobiel betalen toont verwachtschap met de markt voor betalingen via internet, maar er zijn ook belangrijke verschillen. Ten eerste heeft de (consumenten)vraag bij mobiel betalen een ander karakter: internetbetalingen worden bijvoorbeeld regulier gebruikt voor relatief grote, internationale betalingen. Dat is bij mobiel betalen minder het geval. Ten tweede zijn de eisen aan beveiliging anders en daarmee ook de veiligheidsrisico's.

Mobiel betalen heeft enige omvang, maar is in vergelijking met traditioneel betalen en betalen via internet nog gering. Mobiel betalen zal in de toekomst zich nog verder ontwikkelen. De markt voor mobiel betalen omvat veel verschillende verschijningsvormen. Gegeven de door ons gehanteerde definitie, werd er in 2002 alleen al in 150 miljoen keer per SMS betaald, terwijl het aantal betaling per chipknip ongeveer de helft van dit aantal was[13] (zie ook paragraaf 4.4).

[13] Lelieveldt, S. (2003), "De telecommunicatiesector als "nieuwe" aanbieder, *Bank- en Effectenbedrijf*, december, pp. 19-21.

3 Marktpartijen en hun belangen

3.1 Inleiding

We bespreken hieronder de belangrijkste partijen in de waardeketen en de belangen die ze al dan niet hebben bij de ontwikkeling van mobiel betalen. De hier uit volgende posities bepalen de richting van technische ontwikkeling bij mobiel betalen, het onderwerp van de eerste onderzoeksvraag (welke in het volgende hoofdstuk aan bod komt). Omdat de betalingsmarkt een sterk nationaal karakter heeft en omdat dit onderzoek zich specifiek op Nederland richt, wordt hier een Nederlandse perspectief ingenomen. De zes belangrijkste actoren in dit veld zijn achtereenvolgens:

1. Mobiele netwerkexploitanten
2. Banken
3. Creditcard maatschappijen
4. Nieuwe toetreders
5. Product- en dienstenaanbieders ('merchants')
6. Toeleveranciers

Deze partijen worden in paragraaf 3.2 tot en met 3.7 behandeld. Vervolgens wordt in paragraaf 3.8 een model van de waardeketen bij mobiel betalen gepresenteerd. Dat model heeft tot doel de verhouding tussen de partijen aan te geven. Ook de relatie tussen de betaalcomponent en de andere componenten bij een mobiele transactie (zoals het leveren van een goed of dienst) wordt daarmee duidelijker. De laatste paragraaf is een samenvatting en conclusie.

3.2 Mobiele netwerkexploitanten

Een betalingsschema maakt altijd al deel uit van de activiteiten van aanbieders van mobiele telefonie. Het los factureren van iedere individuele afgenomen dienst (telefoongesprekken, SMS berichten etc.) zou immers veel te kostbaar zijn. In eerste instantie hanteerden mobiele telefonieaanbieders abonnementsvormen zoals we die al veel langer kennen van vaste telefonie. Midden jaren negentig zijn betaalschema's met prepaid cards ontwikkeld, in eerste instantie in Italië. Al snel gebruikten meer dan de helft van de klanten prepaid cards. Inmiddels zijn belbundels een veelgebruikte afrekenvorm; feitelijk een combinatie van abonnement en prepaid. Het dienstenaanbod op mobiele netwerken is met ontwikkelingen als SMS, GPRS datadiensten in diversiteit sterk toegenomen. Dat wordt versterkt door de introductie van toegevoegdewaardediensten zoals WAP, i-mode en Vodafone Live. Met name bij deze laatste diensten heeft de betaling ook betrekking op producten die niet tot de typische telecommunicatiediensten behoren, zoals content (sport- en weerberichten, filemeldingen, etc.).

Aan het einde van de jaren negentig zagen mobiele netwerkexploitanten grote belangen bij het (zelf of mede zelf) ontwikkelen van schema's voor mobiel betalen. Dat heeft verschillende oorzaken, zoals:

- Het succes van nieuwe, breedbandige netwerken zoals GPRS en UMTS hangt met name af van de beschikbaarheid van voldoende aantrekkelijke (multimediale) diensten. De beschikbaarheid van een geschikt, on-line betalingsmodel is daarbij een noodzakelijke factor. De enorme bedragen die neergeteld werden op de UMTS veilingen en slechtere marktomstandigheden maakten het noodzakelijk deze diensten tot een groot commercieel succes te maken.

- Mobiel betalen kan een interessante nieuwe inkomstenbron zijn naast de tanende inkomsten van telecommunicatie-transportdiensten. Deze markt kan breder zijn dan alleen de betaling van mobiel geleverde diensten en ook local en remote betalingen omvatten voor fysieke en andere goederen of diensten, al dan niet in combinatie met internet.
- GSM-netwerken beschikken al over een relatief sterke authenticatietechniek, die bovendien zo goed als wereldwijd op een geharmoniseerde manier is ingevoerd. Dit wordt als een uniek asset beschouwd;
- De dekking van de techniek is groot in de zin dat in veel ontwikkelde landen bijna alle bewoners over een mobiele telefoon beschikken. Daarmee is de penetratie hoger dan bijvoorbeeld PC's en creditcards.
- De telefoon wordt als een persoonlijk en vertrouwd object beschouwd, en door de meeste gebruikers continu met zich meegedragen.

In de afgelopen twee jaren is het enthousiasme bij netwerkexploitanten voor de introductie van mobiel betalen afgenomen. Veel operators hebben hun investeringen in UMTS licenties sneller afgeschreven, omdat dat deze investeringen op te hoge verwachtingen waren gebaseerd. Ook de kosten en complexiteit van mobiel betalen worden nu beter onderkend.

Tabel 6 geeft een overzicht van sterke en zwakke punten op mobiel vanuit het perspectief van telecommunicatieaanbieders. De belangrijkste conclusie is dat de invoering van mobiel betalen voor de mobiele operators van heel groot belang is, maar dat ze niet optimaal zijn gepositioneerd om daar de hoofdrol in te spelen.

Tabel 6: Sterkten en zwakten van mobiele telecommunicatieaanbieders in het licht van mobiel betalen

Sterkten	**Zwakten**
Mobiele telefoons hebben een zeer hoge dekking onder de bevolking	Ondersteunen van betalingen is geen core business van telecommunicatieaanbieders
Mobiele telefoons zijn persoonsgebonden en mensen hebben deze vrijwel altijd op zak	Ondersteunen van betalingen vergt extra investeringen in technieken, kennis en vaardigheden
Mobiele telefoons kennen een relatief veilige en geharmoniseerde authenticatietechniek	Hoe groter de rol bij het ondersteunen van mobiel betalen hoe groter de noodzaak om onder enige vorm van financieel toezicht te komen staan (eisen aan solvabiliteit, voldoen aan juridisch regime, etc.)
Mobiele telefoons maken breedbandige diensten (met bijkomende inkomstenstromen) mogelijk en leiden daarmee leiden tot marktvergroting	De in mobiele telefoons aanwezige authenticatie is nog niet voldoende veilig voor veel betaaldiensten
Mobiel betalen kan een extra inkomstenbron worden voor telecommunicatieaanbieders	Klanten hebben nog geen ervaring met en vertrouwen in telecommunicatieaanbieders als financiële partij
	Er zijn meer telecommunicatieaanbieders. Voor voldoende dekking is gecoördineerde invoering in een zeer concurrerende markt nodig
	Zonder voldoende steun van banken, creditcard maatschappijen is het onwaarschijnlijk dat telecommunicatieaanbieders een betalingsdienst kunnen uitrollen

3.3 Banken

Banken spelen een centrale rol in de Nederlandse betalingsinfrastructuur. Deze infrastructuur wordt internationaal als hoogontwikkeld beschouwd. De Nederlandse banksector is relatief geconcentreerd met een viertal zeer grote spelers die samen meer dan zestig procent van de markt bedienen. Betalingsdiensten zijn geen belangrijke inkomstenbron van banken. Ze zijn eerder deel van een standaard dienstenpakket dat nodig is om klanten te binden en meer lucratieve diensten zoals hypotheken en beleggingsproducten in de markt te zetten. Het bieden van betalingsdiensten is daarbij een 'noodzakelijk kwaad'.

Bij banken speelt vervolgens een zeer sterke internationale fragmentatie en in sommige landen een zeer nationale fragmentatie. Landen als Duitsland kennen een zeer versnipperde bancaire sector. Bovendien variëren de betalingsgebruiken enorm tussen verschillende landen (zie paragraaf 2.3), evenals de infrastructuren die daarvoor zijn ingericht. Dit maakt het behalen van een grote schaal door internationale uitrol van mobiel betalen of samenwerking lastig. De Nederlandse markt is dan echter weer aan de kleine klant om een kostbare ontwikkeling van mobiel betalen terug te verdienen.

Het belang van banken voor de invoering van mobiel betalen lijkt relatief klein. Op betalingsdiensten valt niet veel te verdienen, de betalingsbereidheid voor de betaaltransactie is in Nederland nihil. Met invoering van mobiel betalen is weinig te besparen ten opzichte van de bestaande (en deels afgeschreven) infrastructuren zoals die voor pinbetalingen. Daar staat echter tegenover dat banken met het verdwijnen van veel filialen andere kanalen nodig hebben om contact met klanten te onderhouden en diensten aan te bieden, bijvoorbeeld via internet, maar ook via mobiele telefoons.

Tabel 7 geeft een overzicht van de sterkten en zwakten bij mobiel betalen vanuit het perspectief van banken. De belangrijkste conclusie is dat het belang van de banken voor een dergelijke invoering niet zo heel groot is.

Tabel 7: Sterkten en zwakten van banken in het licht van mobiel betalen

Sterkten	**Zwakten**
Banken hebben een sterke positie op de betaalmarkt	Er is een zeer gevarieerde internationale setting. In veel landen is de banksector gefragmenteerd en niet geharmoniseerd
Banken beschikken al over belangrijke onderdelen van de benodigde betalings- en verrekeningsinfrastructuur	Vanwege kleine markt voor mobiel betalen en door netwerkeffecten is samenwerking tussen alle banken noodzakelijk.
Banken voldoen al aan de vereisten van het juridische regime	Banken moeten praten meet veel verschillende mobiele operators om schaal te halen
Mobiel betalen kan nieuwe markten en producten betekenen	Er is veel te verliezen bij mobiel betalen wanneer het misgaat (vertrouwen klant, etc.)
Mobiel betalen biedt een extra communicatiekanaal met de klant	

3.4 Creditcard maatschappijen

Oorspronkelijk zijn creditcards ontwikkeld om grotere lokale betalingen mogelijk te maken, bijvoorbeeld wanneer de klant onvoldoende contant geld bij zich heeft. Zeker in het buitenland, met afwijkende bancaire systemen (weinig mogelijkheid voor pinbetalingen), blijken creditcards nuttig te zijn. Een hoge dekking (acceptatiegraad bij winkels en penetratiegraad bij gebruikers) is van groot belang. Hoewel creditcard maatschappijen in

handen zijn van banken, kunnen ze in een aantal zaken toch een relatief onafhankelijke koers varen.

Het uitvoeren van remote betalingen (telefoon en internet) is in de afgelopen jaren een belangrijke nieuwe markt voor creditcard aanbieders gebleken. Bij het bestellen van een product bij een buitenlandse leverancier (zoals de internet-boekenwinkel Amazon) is het vaak de enige beschikbare betalingsmethode. De risico's op misbruik zijn bij dergelijke transacties relatief groot. De klant is relatief anoniem. Bij transacties zonder een degelijke authenticiteit (handtekening, elektronische verificatie) ligt dat risico vaak bij de ontvanger, zoals de (internet)winkelier (merchant). De houder van de creditcard kan immers de betaling achteraf terugdraaien. De winkel zit dan met het probleem de klant alsnog tot betalen te bewegen of het reeds geleverde product terug te vorderen. Vooral bij buitenlandse klanten is dat lastig. Overigens zijn er ook gevallen waar de creditcard maatschappij dit risico voor haar rekening neemt. Soms tegen een hogere vergoeding voor het gebruik van de kaart (tot zelfs 10% van de transactiewaarde). Ook bij het gebruik van goede authenticatie (handtekening, persoonlijke code) draagt de creditcard maatschappij in de regel het risico bij fraude.

Het veelvuldige gebruik van creditcards bij internetbestellingen roept de vraag op waar creditcards passen in geval van mobiel betalen. Een voor de hand liggend gebied is dat van de hiervoor genoemde internetbetalingen. Mobiel betalen kan frauderisico's bij internetbetalingen beperken en zodoende aantrekkelijk maken voor de partij die dit risico draagt (merchant, creditcard issuer).

Een belangrijk aspect, vanuit de Nederlandse context bezien, is dat Nederland geen creditcard land is. De dekking van creditcards is hier laag en de intensiteit van het gebruik is ook laag. In zowel Finland als in het Verenigd Koninkrijk bijvoorbeeld is het jaarlijkse aantal creditcard transacties ongeveer vijfmaal zo hoog per hoofd van de bevolking.[14] Als creditcard bedrijven geïnteresseerd zijn om mobiel betalen te introduceren dan staat Nederland vermoedelijk achteraan op de lijst van landen.

Tabel 8 geeft een overzicht van de sterkten en zwakten bij mobiel betalen vanuit het perspectief van creditcard maatschappijen. De belangrijkste conclusie is dat mobiel betalen voor creditcard maatschappijen een interessante toevoeging kan zijn op het productaanbod, maar dat in Nederland de kansen laag zijn.

Tabel 8: Sterkten en zwakten van creditcard maatschappijen in het licht van mobiel betalen

Sterkten	**Zwakten**
Creditcard kent een hoge internationale acceptatie bij verkopers	In Nederland is de dekking van creditcards laag
Mobiel betalen met creditcard kan frauderisico's bij internetbetalingen beperken en zodoende aantrekkelijk voor de partij die dit risico draagt (merchant, creditcard issuer)	Transactiekosten zijn hoog en daarom is creditcard niet geschikt voor micropayments
Alternatieve dienst die mogelijke terugloop van bestaande diensten opvangt	Creditcard zijn afhankelijk van de banken voor de uitgifte, en deze banken kunnen andere belangen hebben

[14] ECB (2003).

3.5 Nieuwe toetreders

De opkomst van technologieën als internet en mobiele telefonie hebben geleid tot de oprichting van talloze nieuwe bedrijven op het gebied van infrastructuren en diensten die met wisselend succes een positie in de markt hebben veroverd.

In het geval van mobiel betalen is het niet anders. Talloze nieuwe ondernemingen zagen het daglicht (bijvoorbeeld Moxmo, Way2Pay, Mobile2Pay, Mobipay, Payphone, Payhound en Paypal) en vele ondernemingen hebben in zeer korte tijd het licht weer zien uitgaan (bijvoorbeeld Moxmo).

Vaak worden deze nieuwe bedrijven ondersteund door grote marktpartijen die bewust op de achtergrond blijven om te voorkomen dat een eventuele mislukking uitstraalt op het imago van henzelf. Er zijn echter ook talloze nieuwe marktpartijen die zonder steun van grote bedrijven in staat zijn om mobiele betaaldiensten in de markt te zetten. Zij veroveren daarmee een (bescheiden) plek in de waardeketen. Het is echter zeer goed denkbaar dat enkele van deze kleine nieuwe start-ups zullen uitgroeien tot belangrijke spelers in waardeketen, bijvoorbeeld omdat zij beschikken over diensten die aanslaan bij het grote publiek of doordat zij slimme samenwerking weten te realiseren met marktpartijen die een gevestigde positie innemen. Mobiel betalen is deels een nieuwe markt en het is geen uitgemaakte zaak dat 'traditionele' partijen (banken, telecommunicatieaanbieders en creditcardmaatschappijen) deze onderling zullen verdelen.

Tabel 9 geeft een overzicht van de sterkten en zwakten bij mobiel betalen vanuit het perspectief van nieuwe toetreders. De belangrijkste conclusie is dat nieuwe toetreders relatief onbekend zijn bij consumenten en partijen in de waardeketen. Bovendien hebben nieuwe toetreders last van een relatief laag consumentenvertrouwen als het gaat om betalingen.

Tabel 9: Sterkten en zwakten van nieuwe toetreders in het licht van mobiel betalen

Sterkten	**Zwakten**
Dynamische en diverse markt met talloze toetreders en sterke marktgerichtheid	Moeten vertrouwen van consument en andere partijen winnen, zeker bij betalen (vergelijk dat eens met de status van banken!)
Toetreders zijn gedreven en worden niet gehinderd door bestaande belangen	Lijken vanwege kostenoverwegingen minder nadruk te leggen op veiligheid en andere belangrijke spelregels
Toetreders zijn zijn klein en flexibel	Zijn door schaal vaak niet op de hoogte van wet- en regelgeving
Toetreders kunnen maatwerkoplossingen bieden	Vaak financieel zwak en daardoor weinig geld voor investeringen (veel initiatiefnemers gaan snel failliet)
Er ligt nog een hele markt open. Wie hier het geaccepteerde wiel uitvindt!	Moordende concurrentie
Toetreders kunnen dankzij specifieke kennis aanschuiven bij grote gerespecteerde instellingen	Kampen door onbekendheid met ontwikkelen van acceptatie bij webwinkels en eindgebruikers etc (wie moeten webwinkels kiezen?)
Nieuwe toetreders zijn vaak nichespelers	Toezicht stelt eisen die belasting vormen voor een kleine partij
	Afhankelijk van een specifieke dienst, namelijk mobiel betalen

3.6 Product- en dienstenaanbieders ('merchants')

In de waardeketen kunnen verschillende type producten- en dienstenaanbieders worden onderscheiden. Enerzijds zijn er producten- en dienstenaanbieders die naast mobiel betalen ook andere diensten aanbieden, bijvoorbeeld banken (mobiel beleggen, sparen en verzekeren) en telecommunicatieaanbieders (SMS, MMS, ringtonen, beursinformatie, weer).

Anderzijds zijn er leveranciers die mobiel betalen niet als dienst aanbieden, maar die wel producten en diensten leveren die mobiel betaald kunnen worden. Voorbeelden zijn drankautomaten waar met mobiele telefoons kan worden betaald of specifieke, mobiele informatiediensten (bijvoorbeeld weer en verkeer), waarbij de mobiele operator alleen de informatie van een derde partij (KNMI, ANP, etc.) doorgeeft, bijvoorbeeld via portals. Overigens strijkt de operator in het laatste voorbeeld dan vaak wel een deel van het te betalen bedrag op (zgn. fee). Het bedrag wordt verrekend met het beltegoed en de telecommunicatieoperator verrekent weer met de aanbieder van de dienst.

Er spelen hier verschillende belangen. Wanneer klanten hun beltegoed (prepaid en belbundels) vaker gaan gebruiken voor betalingen aan partijen buiten de telecommunicatieoperator om is de verwachting dat tegoeden die klanten aanhouden groter worden. Belangrijker nog is dat wanneer andere partijen dan telecommunicatieaanbieders deze tegoeden accepteren als geld ontstaat er een situatie ontstaat waarin deze tegoeden wellicht als elektronisch geld aangemerkt moeten worden (zie ook hoofdstuk 9). Telecommunicatieoperator ontvangen als doorgeefluik van deze diensten een relatief groot aandeel van de betaling die de klant moet verrichten. Dat loopt soms op tot 40% van het totale bedrag.[15] De positie van de telecommunicatieaanbieder tussen de merchant (van bijvoorbeeld tickets, nieuwsberichten, voetbalbeelden) en de eindgebruiker is dus zeer lucratief. Zij zullen deze markt niet graag uit handen geven en creëren dus mobiele portals waar verschillende aanbieders hun 'winkeltje' kunnen beginnen.

Voor beheerders van drank- en parkeerautomaten spelen weer andere belangen bij mobiel betalen. Zo zal de factureringsrelatie verschuiven. Beheerders van drankautomaten, bijvoorbeeld Maas International, hebben nu een factureringsrelatie met het bedrijf of de school waar automaten staan. De interne verkoop van drank is vaak geregeld met contact geld, chippers of specifieke bedrijfs- en schoolpassen uitgerust met een chip. Invoering van mobiel betalen betekent dat er nu een rechtstreekse factureringsrelatie met de individuele klant ontstaat. Tabel 10 geeft een overzicht van de sterkten en zwakten bij mobiel betalen vanuit het perspectief van product- en dienstenaanbieders.

Tabel 10: Sterkten en zwakten van product- en dienstenaanbieders in het licht van mobiel betalen

Sterkten	**Zwakten**
Aanbieders beschikken vaak over aantrekkelijke producten voor mobiele consumenten Mobiel betalen opent extra kanaal naar nieuwe markten en nieuwe consumenten	Aanbieders zijn voor verspreiding afhankelijk van de telecommunicatieaanbieders die kunnen bijvoorbeeld een relatief groot deel van de opbrengsten opeisen Vendor machines moeten techniek hebben die geaccepteerd wordt door alle type telecommunicatieaanbieders / gsm's De relatie met de klant wordt meer anoniemer relatie met klanten Toetreding van malafide aanbieders

[15] Natuurlijk kunnen ze er voor kiezen om slechts een 'kale' transportdienst af te nemen. Dan zijn alleen de alleen gebruiksfarieven (per minuut, per kilobyte) van toepassing maar van moet de aanbieders zelf voorzien in een betalingssysteem – en dat is juist vaak erg lastig, zeker op individuele schaal.

3.7 Toeleveranciers

Onder toeleveranciers verstaan we de producenten van hard- en software die benodigd zijn om mobiel betalen mogelijk te maken. Het gaat dus onder meer om fabrikanten van mobiele telefoons, randapparatuur en chips. Ook softwareontwikkelaars en producenten van transactie-verwerkingsystemen vallen onder deze categorie.

Hoewel sterk betrokken bij ontwikkelingen rondom mobiel betalen zien zij voor zichzelf geen rol als trekker weggelegd; ze ambiëren dan ook niet zelf dergelijke diensten zelfstandig te ontwikkelen, uit te rollen of te exploiteren.

Ze ambiëren echter wel deze systemen *mee* te ontwikkelen. Veel van deze leveranciers zijn betrokken bij (internationale) initiatieven rondom mobiel betalen. Zij verkeren daarbij enigszins in de periferie in vergelijking met telecommunicatieaanbieders en financiële instellingen. Desondanks spelen zij een belangrijke rol bij de uitrol van de technologie voor het mobiel betalen. Het is bijvoorbeeld denkbaar dat fabrikanten van mobiele telefoons (Nokia, Siemens, etc.) deze apparaten zullen uitbreiden met extra applicaties (chips, sloten voor chipcards) om mobiel betalen mogelijk te maken.

Belangrijk daarbij is de schaal en de samenwerking met telecommunicatieaanbieders. Schaal speelt een rol, omdat producenten investeringen in extra applicaties willen terugverdienen. Naarmate een markt voor mobiel betalen kleiner is, neemt de kans af dat fabrikanten daar een aparte telefoon voor zullen produceren. Zeker in een situatie waar men in zeer korte tijd nieuwe telefoons introduceert. Een typisch Nederlandse oplossing (of voor een ander klein Europees land) zal dus niet snel door deze fabrikanten worden opgepikt. Vanuit schaaloverwegingen zullen deze fabrikanten eerder pleiten voor een internationale oplossing en standaard. Bovendien hebben fabrikanten vaak contracten met afzonderlijke telecommunicatieaanbieders voor de levering van mobiele telefoons. Er zal dus de nodige samenwerking vereist zijn tussen fabrikanten onderling en met telecommunicatieaanbieders om een (identieke) betaaltechnologie te verwerken.

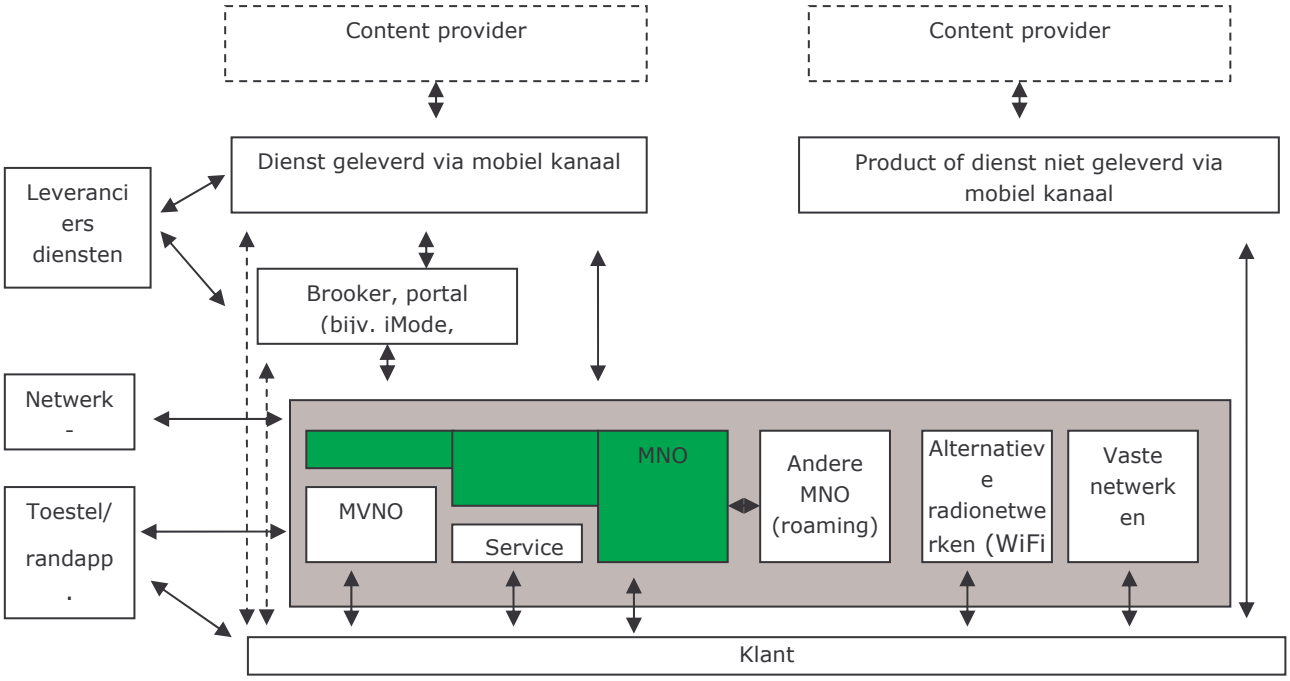
Tabel 11 geeft een overzicht van de sterkten en zwakten bij mobiel betalen vanuit het perspectief van de leveranciers.

Tabel 11: Sterkten en zwakten van toeleveranciers in het licht van mobiel betalen

Sterkten	**Zwakten**
Toeleveranciers beschikken over voldoende investeringsmiddelen	Toeleveranciers zijn ten aanzien van mobiel betalen eerder volgend dan leidend
Toeleveranciers sterk innovatiegedreven en zijn sterk internationaal georiënteerd	Commerciële belangen en fragmentatie belemmeren samenwerking en standaardisatie
Toeleveranciers beschikken over kanalen om een betaaltechnologie daadwerkelijk internationaal uit te rollen	Nadruk op techniek en minder op diensten zoals mobiel betalen
	Extra investeringen vertalen zich niet in hogere betalingsbereidheid van eindgebruiker, terwijl ook de exploitant van mobiel betalen de investeringen niet wil dragen
	Nationale oplossingen zijn moeilijk vanwege kleine schaal

3.8 Waardeketen mobiele diensten en mobiel betalen

Ten behoeve van het onderzoek hebben we een schematisch overzicht gemaakt van de partijen en hun onderlinge relaties (figuur 4). Dit schema kan worden beschouwd als een plattegrond van de waardeketen. Op deze wijze worden de partijen zoals beschreven in de voorgaande paragrafen onderling in verband gebracht. De waardeketen heeft een rol gespeeld bij de selectie van de interviewpartners. Voorts helpt de waardeketen om invulling te geven aan de varianten van mobiel betalen die in het volgende hoofdstuk aan de orde komen. Daar zal immers blijken dat de rol van partijen (bijvoorbeeld omvang en belang), de dominante techniek (bijvoorbeeld single chip en dual chip) en vormen van betalen (micro of macro payments) per variant kan verschillen waardoor 'zwaartepunten' in de gevisualiseerde waardeketen er per keer anders uitzien.



Figuur 4: Waardeketen bij mobiel betalen

3.9 Samenvatting en conclusies

In dit hoofdstuk zijn de belangrijkste partijen uit de waardeketen mobiel betalen en hun specifieke belangen behandeld. Daarbij zijn de volgende partijen onderscheiden: mobiele netwerkexploitanten, banken, creditcard maatschappijen, nieuwe toetreders, product- en dienstenleveranciers en toeleveranciers. Deze partijen beschikken over specifieke sterkten en zwakten en kansen en bedreigingen ten aanzien van mobiel betalen.

Uit de analyse blijkt dat in Nederland exploitanten van mobiele netwerken verreweg de grootste belangen hebben bij (een snelle) invoering van mobiel betalen. De grote uitgaven die ze hebben gedaan bij de aanleg van hun 2.5G en 3G netwerken kunnen ze vermoedelijk alleen terugverdienen met een breed aanbod van betaalde diensten en content. Daarvoor is een goed functionerend betaalsysteem onontbeerlijk.

De andere partijen voelen de prikkel om mobiele betaalsystemen te introduceren veel minder sterk. Terwijl enkele jaren geleden verwachtingen positiever waren, is de teneur nu dat mobiel betalen relatief duur is en dat het zeker in Nederland lastig is om met reeds bestaande en goed presterende alternatieven zoals pinnen en chippen te concurreren. Deze goed

functionerende betaalvormen leiden ertoe dat banken iets minder belang tonen voor mobiel betalen dan de telecommunicatieaanbieders.

In Nederland is de creditcard relatief slecht doorgedrongen. Creditcard maatschappijen hebben daarom een relatief klein belang bij het invoeren van mobiel betalen met creditcard in Nederland. Zij hanteren een internationaal perspectief waarbij Nederland volger is. Hetzelfde geldt voor producenten van mobiele telefoons. Zij zoeken schaalvoordelen voor eventuele extra betaalapplicaties die ingebouwd moeten worden. Nederland is een klein land en kan die schaal dus niet snel bieden. Bovendien is mobiel betalen geen core business voor deze bedrijven.

Nieuwe toetreders die zich louter richten op het product mobiel betalen hebben veel belang bij de introductie van deze betaalvorm, maar zij kampen met een relatieve onbekendheid bij het grote publiek. Onbekend maakt bovendien onbemind. Zeker bij geldzaken zullen consumenten graag zaken doen met vertrouwde partijen zoals banken. Voor aanbieders van diensten (nieuws en informatie) ontstaat een extra kanaal voor betalen dat voor digitaal geleverde diensten onmiddellijk gekoppeld kan worden aan de eindgebruiker. Daartussen staat echter nog vaak de telecommunicatieaanbieder die een deel van deze grote (lucratieve) markt inneemt.

Er zijn veel kleinere initiatieven maar ze zijn weinig kansrijk. Er ontwikkelen zich talloze initiatieven, die worden aangeboden door bestaande partijen maar ook door nieuwe toetreders tot de markt. Deze initiatieven, in Nederland en ook daarbuiten, vinden we zowel bij internetbetalingen als bij mobiel betalen. Veel initiatieven hebben echter moeite enige schaal te bereiken en soms verdwijnen ze niet lang na de introductie. Nieuwe toetreders staat dan regelmatig het failliet in het vooruitzicht.

4 Ontwikkelingsvarianten mobiel betalen

4.1 Inleiding

In dit hoofdstuk wordt een aantal ontwikkelingsvarianten behandeld bij mobiele betalingsdiensten. Deze varianten geven voor een groot deel het antwoord op de eerste drie onderzoeksvragen (zie paragraaf 1.2), te weten:

1. Hoe zien de technologische ontwikkelingen er op hoofdlijnen uit?
2. Wat zijn de gevolgen van deze ontwikkelingen voor de "factureringsrelaties" en voor het opereren van telecommunicatieaanbieders in de markt? Zullen de telecommunicatieaanbieders zich gaan transformeren tot een ander type dienstverlener?
3. Welke (nieuwe) marktpartijen zullen betrokken zijn? Zal er een nieuw type (financiële) dienstverlener ontstaan?

Deze varianten worden vervolgens in delen II en III van dit rapport gebruikt om fraude en het wettelijke instrumentarium verder uit te werken.

Paragraaf 4.2 behandelt de keuze van de indeling van de ontwikkelingsvarianten. Welke (combinatie van) criteria worden gebruikt voor de centrale indeling? Vervolgens worden de vier ontwikkelingsvarianten (kortweg varianten) besproken in paragraaf 4.3 tot en met 4.6.

In paragraaf 4.7 volgt een technische invulling van de varianten. In paragraaf 4.8 staat een vergelijking tussen de varianten centraal. In paragraaf 4.9 wordt tenslotte besproken wat de verwachte kansen bij de verschillende varianten zijn.

4.2 Keuze van de varianten

Er zijn allerlei dimensies waarop de keuze voor de varianten kan worden gebaseerd. Daarbij kan men denken:

- Technisch-functionele indeling van de systemen;
- Indeling naar de hoofdspelers in de waardeketen;
- Indeling naar beoogd type gebruik (micro- en macrobetalingen, content-, local en remote betalingen);
- Indeling naar de (internationale) initiatieven voor ontwikkeling en harmonisatie zoals Mobile Payment Forum (MPF), Simpay; Mobey Forum Mobile Financial Services Ltd, European Committee for Banking Standards (ECBS), Mobile electronic Transactions (MeT) en PayCircle;
- Indeling naar (gezamenlijke) initiatieven die zich in de Nederlandse markt ontplooien.

Elke indeling is discutabel. Zo zijn er indelingen die varianten opleveren die er in de Nederlandse context minder toe doen, of indelingen die varianten opleveren die onvoldoende onderscheidend vermogen hebben[16]

In dit rapport is een pragmatische indeling gekozen, waarbij de nadruk wordt gelegd op die initiatieven waarvan (aan de hand van interviews) wordt verwacht dat ze binnen nu en tien jaar van relevant zijn in de Nederlandse context. Ten tweede hebben we gestreefd naar

[16] Denk aan een indeling naar hoofdrolspelers waarbij banken soms meerdere, soms complementaire technisch-functionele varianten nastreven.

varianten die zich duidelijk onderscheiden ten opzichte van elkaar. De hier onderscheiden varianten zijn dan ook vaak een zekere mix van de hierboven genoemde indelingen. Het spreekt voor zich dat er rondom de gekozen varianten nog allerlei variaties denkbaar zijn.

Op van het bovenstaande maken we onderscheid tussen vier varianten:

- Variant 1: Mobiel pinnen (ontwikkeling van debet-transacties via het internet);
- Variant 2: Prepaid betalingen (telco-centric pre-paid based micropayment model);
- Variant 3: Creditcard betalingen;
- Variant 4: Digitaal muntgeld.

Op de varianten is een *reality check* gedaan. Elke variant wordt door minimaal twee van de geïnterviewde partijen als een reëel toekomstbeeld wordt beschouwd. Overigens is er wel sprake van uiteenlopende beelden over de toekomst. Niet alle varianten worden door alle geïnterviewden onderschreven als kansrijk.

4.3 Variant 1: Mobiel pinnen

Drie Nederlandse banken (ING, ABN Amro en de Rabobank) hebben onlangs besloten een standaard (genaamd Ideal) in te voeren voor betalingen via internet.[17] Het gaat om een systeem dat een verlengde is van de bekende pinbetalingen. Het betreft dus een on-line debet transactie waarbij het bedrag direct wordt afgeboekt van de betaalrekening van de rekeninghouder. Dit wordt ook wel aangeduid met *direct debet*.

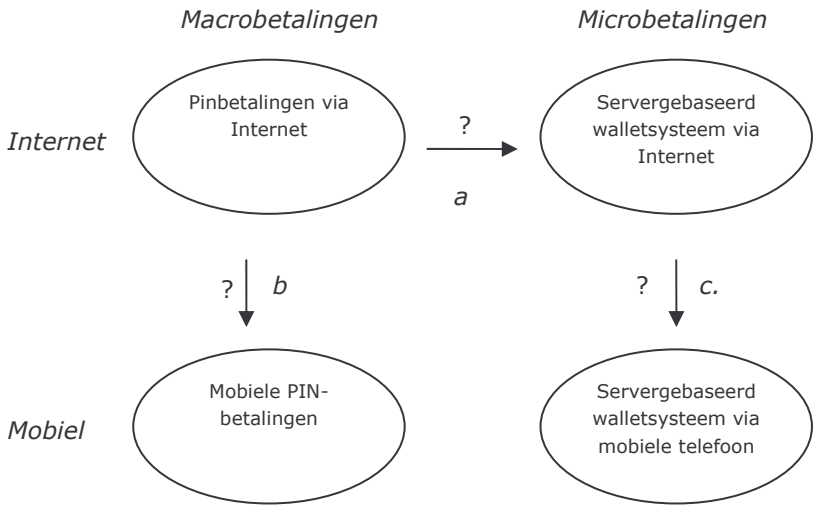
Bijzonder is dat de deelnemende banken de authenticatiefunctie invullen. De individuele banken kiezen daarvoor de techniek die ze eerder al hebben uitgewerkt voor bankieren via internet. Sommige banken gebruiken dus een (aparte) crypto calculator, terwijl andere banken anderen lijsten met unieke codes per post (of per sms op zijn mobiele telefoon) naar klanten versturen. Deze codes worden voor een eenmalige transactie gebruikt.

Deze standaard voor betalen via internet past in de pogingen van EZ om via het initiatief 'betalen via nieuwe media' marktpartijen uit alle delen van de waardeketen stimuleert om de introductie van nieuwe betaalsystemen (via internet en mobiel) te versnellen.

In het verlengde van dit initiatief van de banken is een uitbreiding denkbaar met een systeem voor microbetalingen. Dat systeem gebruikt een (server gebaseerde) wallet. Bij een dergelijk systeem kunnen de gemaakte kosten per transactie worden teruggebracht tot een niveau wat bij kleine betalingen (van een halve tot twee euro) nog acceptabel is. Net zoals er voor de fysieke wereld pinbetalingen en chipcards door de banken worden ingezet, zouden er dan voor internetbetalingen ook twee methoden zijn die ieder aansluiten op een deel van de betalingsmarkt. Dergelijke systemen zijn in Nederland door individuele marktpartijen al geïntroduceerd (zoals de Minitix dienst van de Rabobank) maar er is nog geen sprake van een breder gedragen standaard door meerdere banken.

In beginsel zou het hiervoor geschetste systeem (pinbetalingen eventueel uitgebreid met een systeem voor microbetalingen) ook doorontwikkeld kunnen worden voor mobiel betalen. De mogelijke routes worden weergegeven in figuur 5. We benadrukken nog eens dat het hier om mogelijke en reëel geachte route gaat naar systemen voor mobiel betalen en dat hiermee niet gezegd is dat marktpartijen (hier vooral: banken) inderdaad deze route zullen bewandelen.

[17] Dergelijke diensten waren al wel eerder bij individuele banken beschikbaar, zoals de dienst Rabo Direct Betalen. Nu gaat het echter om een — tot op zekere hoogte—geharmoniseerd product. Een uitgebreidere omschrijving van Ideal is te vinden bij Emerce (http://www.emerce.nl/nieuws.jsp?id=402023).



Figuur 5: Mogelijke ontwikkelingen bij variant 1.

In het onderstaande concentreren we ons verder op de route die aangegeven wordt met de letter (a) die we in deze rapportage als 'variant 1' beschouwen. Deze route betreft de doorontwikkeling van 'pinnen via internet' naar 'pinnen via de mobiele telefoon'. [18] De ratio is dat op dit moment pinnen in de fysieke wereld (toonbankbetalingen, gelddistributeurs) reeds een hoge penetratiegraad kent en dat dit systeem door alle financiële partijen wordt beschouwd als een zeer efficiënt en goedwerkend systeem, zeker in internationaal perspectief.[19] Vanuit het perspectief van de consument is het een vertrouwde methode van betalen, aangeboden door vertrouwde partijen, laagdrempelig (de eigen bijdrage is bescheiden) en het heeft niet de nadelen van sommige andere betaalmethoden zoals de noodzaak tot opladen.

De doorontwikkeling van de huidige standaard voor pinnen via internet richting de mobiele telefoon zal echter nog voor enkele behoorlijke technische uitdagingen zorgen. Dat komt met name omdat de huidige standaard, zoals hierboven aangegeven, gebruik maakt van de diverse verschillende authenticatiemethoden van de individuele deelnemende banken. Deze methoden lenen zich slecht voor mobiel gebruik. De gebruiker zal niet snel bereid zijn om een crypto-calculator of een lijst met unieke codes altijd met zich mee te moeten nemen om mobiele betalingen te verrichten. Ook de betaling zelf wordt er omslachtig van. Iedereen lijkt er van overtuigd dat een mobiel betalingssysteem alleen kans van slagen heeft als het zeer gebruiksvriendelijk is vormgegeven: het toetsen van een wachtwoord en pincode is op dat punt vermoedelijk het maximum dat de gebruiker zal accepteren. Dit alles betekent dat men de bestaande, diverse methoden niet kan inzetten voor mobiel pinnen en er een nieuw, geschikt authenticatiesysteem zal moeten worden ontworpen en ingevoerd. Wellicht is biometrische authenticatie een oplossing.

De authenticatiefunctie zou kunnen worden vormgegeven als een softwareapplicatie in de mobiele telefoon, die vervolgens van een beveiligde mobiele verbinding (zoals SSL) gegevens

[18] Eén van de interviewpartners betitelde deze variant als het Maestro-scenario. In dit scenario zit de pinpas zoals we deze kennen verwerkt in de mobiele telefoon. Dit vraagt om aangepaste en bij voorkeur ook gecertificeerde telefoons. Dit maakt telefoonfabrikanten zoals Nokia weinig gelukkig want zij willen "elke zes weken" een nieuwe telefoon op de markt brengen. FinRead heeft een standaard ontwikkeld voor het certificeren van telefoons die met een dergelijke toepassing worden uitgerust.

[19] Dit wordt onder meer bevestigd in het rapport van het Maatschappelijk Overleg Betalingsverkeer (2004), terwijl ook alle gesproken marktpartijen dit beamen. Ook de slogan 'van PINnen kun je niet winnen' geeft dat doeltreffend aan.

uitwisselt met de systemen van de bankinstantie. Een implementatie in de SIM-chip zelf zou een veiligere aanpak vormen, maar vergt wel veel meer afstemming met alle operators van de nationaal beschikbare mobiele netwerken.

Ter versterking van de veiligheid kan de bank ook overwegen om het Calling Line Identification (CLI), het telefoonnummer van de gebruiker (officieel MSISDN geheten) dat het telecommunicatienetwerk doorgeeft naar de ontvanger, te controleren. Zo kan men (deels) gebruikmaken van veiligheidssystemen die inherent zijn aan de GSM-techniek. Indien er ook verdere afspraken worden gemaakt met de exploitant van het telecommunicatienetwerk kunnen ook andere gegevens worden ingezet om tot een betere beveiliging te komen, zoals IP-nummers, gegevens over de sessie en de gebruikte tunnels, etc.

4.4 Variant 2: Prepaid betalingen

Al vele jaren kennen we op mobiele (en vaste) telefonienetwerken de zogenaamde koopnummers ofwel premium rate nummers. Tegenwoordig zijn dat de zogenaamde 0900-nummers. Bij het bellen van deze nummers betaalt de klant een hoger tarief dan gebruikelijk voor (interlokale) gesprekken. Dat hogere tarief wordt doorbetaald aan de ontvanger van het gesprek (doorgaans een exploitant van een bepaalde dienst). Ook rekent de netwerkexploitant een bepaalde vergoeding die ze in mindering brengt op het door te betalen bedrag.

Marktomvang en marges bij informatiediensten

In 2002 vond er ongeveer 360 miljoen euro plaats aan dienstverlening via 090x nummers. Er is een uitgebreide industrie ontstaan die dienstverleners helpen bij de inrichting van betaallijnen (nummeraanvraag en –beheer, voice response applicaties, incassering, etc.). Een informatiedienstverstrekker is, bij een betaalnummer dat de klant zeventig cent per minuut kost, ongeveer vijftien cent kwijt aan de back-office provider. Ongeveer elf cent gaat naar de belasting. Om winst te maken, moet de aanbieder zorgen dat overige kosten niet hoger worden dat ongeveer 44 cent per minuut. Slimme aanbieders slagen erin om die kosten te beperken tot twintig cent per minuut, zodat een opbrengst resteert van ongeveer 24 cent per minuut, ofwel een marge van ongeveer 34%. (overgenomen uit Lelieveldt S. (2003), De telecommunicatiesector als 'nieuwe' aanbieder, in: *Bank- en Effectenbedrijf*, december, pp. 19-21.)

In wezen is hiermee een betalingsmechanisme gecreëerd dat zich goed leent voor de betaling van diensten die geleverd worden via de mobiele telefoon. In toenemende mate wordt een dergelijk mechanisme ook ingezet voor de betaling van diensten die niet (of niet helemaal) via de telefoon worden geleverd. Zo kan er voor het opvragen van een krantenartikel uit het archief van De Volkskrant betaald worden via de KPN-dienst Switchpoint: door het bellen van een opgegeven 0900-nummer wordt het bedrag aan de telefoonrekening toegevoegd en wordt vervolgens het gevraagde artikel via internet afgeleverd. Een populaire toepassing van premium rate nummers is die door omroepen, waarbij de gebruiker – tegen vergoeding! - bijvoorbeeld een stem mag uitbrengen op een kandidaat van een wedstrijd, bijvoorbeeld Idols of het Eurovisie Songfestival. Dit alles is ook mogelijk via de mobiele telefoon. Inmiddels bestaan dergelijke betaaldiensten ook via SMS.[20] Een vergelijkbare constructie wordt ook gebruikt om diensten af te rekenen die beschikbaar zijn op mobiele platforms als i-Mode, Vodafone Live en T-zones.

[20] Daarbij wordt onder meer gebruik gemaakt van 'reversed billing' SMS-berichten: als de consument deze berichten ontvangt moet deze zelf de kosten ervoor betalen.

In feite gaat het hier steeds om systemen waarbij de vergoeding van diensten (of eventueel producten) plaats vindt via de betalingsrelatie die de klant met de telecommunicatieaanbieder heeft. Bij mobiele systemen is dat mogelijk in combinatie met elk van de drie gebruikte betalingsvormen: prepaid, postpaid ('regulier abonnement') en belbundels. [21] Mobiel opwaarderen van het prepaid tegoed gaat relatief eenvoudig. Dit kan een opstap zijn naar daadwerkelijk mobiel betalen. Telecommunicatie aanbieders verwachten dat dit kan aanslaan bij consumenten. Het betreft dan betalingen tot 10 à 15 euro. Prepaid tegoeden zullen waarschijnlijk niet gebruikt worden voor het doen van macrobetalingen.

De interesse van mobile operators in mobiel betalen is tweeledig:

1. Bij bepaalde categorieën diensten (met name premiumrate diensten) kunnen ze een behoorlijke vergoeding in rekening brengen, soms wel van enkele tientallen procenten van de totale omvang van de transactie).[22]
2. Betalingsdiensten worden als een belangrijke *enabler* gezien voor allerlei diensten die UMTS netwerken tot een succes moeten gaan maken.

Hoewel de huidige systemen al mobiele betalingen mogelijk maken, en zelfs een behoorlijke grote schaal daarin hebben bereikt, zijn de mogelijkheden wat beperkt richting de toekomst. Contentdiensten worden bijvoorbeeld meer geavanceerd. Bij het huidige systeem is van het tarief gekoppeld is aan het aangeroepen nummer (10 eurocent per minuut, 50 eurocent per aanroep). Dit statische, eenvoudige systeem zal voor meer geavanceerde en interactieve diensten onvoldoende zijn. Een gebruiker moet tijdens een sessie content en/of diensten kunnen kiezen en vervolgens een rekening krijgen voor de selectie die hij of zij gemaakt heeft.

Een andere belangrijke beperking van de huidige systemen met betalen via de telefoonrekening is dat dienstenaanbieders voor een voldoende dekking bilaterale afspraken moeten maken met alle netwerkexploitanten (of andersom: netwerkexploitanten afspraken moeten maken met alle dienstenaanbieders). Op dit moment is het meer geavanceerde dienstenaanbod op mobiele telefoons vooral ondergebracht in relatief afgeschermde omgevingen zoals de eerder genoemde i-Mode, Vodafone Live en T-zones. (Deze omgevingen worden ook wel met 'walled gardens' aangeduid). Als de contentontwikkeling echter een brede vlucht neemt, zullen alle benodigde bilaterale afspraken echter tot hoge transactiekosten leiden en ontstaat de behoefte aan een meer geharmoniseerde aanpak.

In deze meer geharmoniseerde aanpak wordt voorzien door het Simpay initiatief (voorheen Mobile Payment Services Association). Deze organisatie is 2003 opgericht door vier mobiele netwerkexploitanten, te weten Orange, Telefónica Móviles, T-Mobile en Vodafone. Andere netwerkexploitanten zijn volgens de organisatie welkom als lid, maar andere partijen uit de waardeketen kunnen zich niet als lid aansluiten bij deze organisatie.

Behalve een technisch schema voorziet Simpay in een organisatorische aanpak, waarbij zogenaamde 'merchant acquirers' [23] een intermediaire rol spelen tussen diensten- en contentaanbieders en andere merchants enerzijds en netwerkexploitanten anderzijds (zie figuur 6). Met name grotere merchant acquirers, die er in geslaagd zijn met veel partijen zaken te doen, kunnen de transactiekosten verminderen. Immers, een netwerkexploitant zal niet met honderden dienstenaanbieders afzonderlijk zaken hoeven te doen, maar slechts met

---

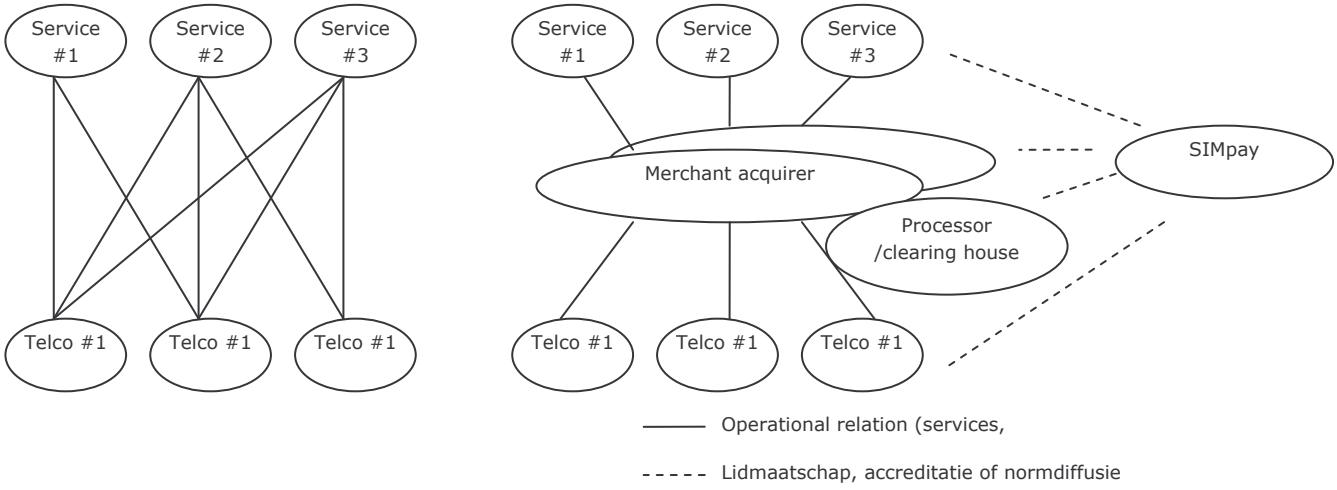
[21] Belbundels zijn betalingsvormen waarbij de gebruiker een vast bedrag per maand betaald en daarmee een tegoed verkrijgt voor het afnemen van diensten. Dit deel heeft dus het karakter van een pre-paid betalingsvorm. Is het tegoed in de bundel echter geheel verbruikt, dan worden de extra gesprekken daarna gefactureerd. Dat laatste deel heeft dus een post-paid karakter.

[22] Dit gegeven is overigens bijzonder; bij de verkoop van een kop koffie uit een automaat moge de kosten van betalingstransactie vermoedelijk niet meer dan enkele procenten van de totale waarde bedragen.

[23] De keuze voor deze naam weerspiegeld goed dat dit initiatief vanuit het perspectief van netwerkexploitanten is opgezet, niet vanuit het perspectief van de dienstenleveranciers.

één of enkele merchant acquirers. Iets vergelijkbaars geldt voor de dienstenaanbieders. Verder is er in het model van Simpay sprake van een partij die alle transactieverwerking voor haar rekening neemt. Hier is onlangs het in Duitsland gevestigde bedrijf Encorus voor geselecteerd.

SIMpay richt zich vooral op micropayments (betalingen van 10 euro of minder). Daarbij denken de initiatiefnemers met name aan games, ringtones, logos, video clips en MP3 muziekbestanden. Bij micropayments is de verwachting dat de mediaan van het bedrag ongeveer een à twee euro bedraagt met uitschieters voor java games naar 5 euro.



Figuur 6: Schets SIMpay-model

4.5 Variant 3: Creditcard betalingen

Deze variant krijgt in de Nederlandse context relatief weinig aandacht. Een belangrijke reden voor deze geringe aandacht is het feit dat de creditcard relatief slecht is doorgedrongen in de Nederlandse betalingscultuur. Bovendien gebruiken de bezitters deze kaart relatief weinig voor het verrichten van betalingen. De penetratie en gebruiksfrequentie zijn laag.

Het is dan ook niet verwonderlijk dat deze mobiele betalingsvariant meer internationaal dan nationaal aandacht geniet. Overigens wordt de creditcard al veel gebruikt voor betalingen op afstand. Denk hierbij aan betalingen via internet en via de telefoon. Hierbij is gebleken dat creditcards fraudegevoelig zijn. Dit heeft ertoe geleid dat zelfs bij betalingen via internet het gebruik van creditcard geen voorkeur geniet onder Nederlandse consumenten. Het is dan ook niet te verwachten dat mobiel betalen andere beelden zal laten zien. Het risico wordt gevormd door de mate waarin men de echtheid van de SIM en de echtheid van de kaarthouder kan bepalen. Bij "card not present" transacties is dat een lastig verhaal. Een gedeelte van het risico wordt (financieel) opgevangen door de transactiekosten die bij creditcard betalingen in rekening worden gebracht.

Doordat de beveiliging voor de gebruiker, het mobiele toestel en de verkoper nooit waterdicht geregeld is, hebben de creditcard maatschappijen een probleem. Bovendien lijken mobiele betalingen zich in eerste instantie te bewegen op de markt van microbetalingen. Dat maakt mobiel betalen met een creditcard minder aantrekkelijk vanwege de hoge transactiekosten.

De initiatieven van creditcard maatschappijen betreffen momenteel een aantal proeven. Zo wordt samengewerkt met Nokia en KPN voor een proef met een 'PKI on SIM' beveiligingssysteem. Bij een grotere uitrol spelen echter afhankelijkheid van zowel banken als telco's een rol: de kaart bevat essentiële gegevens van beiden, en beide partijen zullen er moeite mee hebben om dit belangrijk deel van het proces aan een ander over te laten. Een

dominante partij (of een conglomeraat) kan dat wellicht nog wel afdwingen. Afzonderlijke push/pull krachten krijgen dit niet voor elkaar. Bovendien ervaart de klant een sterke lock-in: het wisselen van bank of telco wordt ermee sterk bemoeilijk. Overigens heeft het enkele jaren oude initiatief van Postbank en Telfort voor een telefoon met m-bankieren geleerd dat ook de logistieke kant niet moet worden onderschat, zeker als het aanbod een groot succes wordt.

Ook in het buitenland vinden initiatieven plaats: in Finland hebben de bedrijven Visa, Nordea en Nokia in 2003 en 2004 een pilot gebouden voor local payments. Daarbij waren echte merchants en klanten betrokken. Deze pilot is volgens de Mobey Forum – een internationaal samenwerkingsverband van banken voor de stimulering van mobiele technologie in financiële diensten - architectuur opgezet.

4.6 Variant 4: Digitaal muntgeld

Er zijn in de afgelopen jaren talloze nieuwe bedrijven opgericht die zich ten doel stellen internet- of mobiele betalingsdiensten te realiseren. Sommige bronnen spreken zelfs van meer dan 300 bedrijven. [24] Enkele voorbeelden zijn Moxmo, Way2Pay, Mobile2Pay, Mobipay, Payphone, Payhound en Paypal. Veel van deze nieuwe bedrijven blijken het hoofd moeilijk boven water te kunnen houden. Zo werd bij Moxmo recent het faillissement uitgesproken. Overigens zijn er ook voorbeelden van meer succesvolle bedrijven: in de VS realiseerde PayPal in 2003 reeds een omzet van 134 miljoen dollar, en in een onderzoek werd verwacht dat dit bedrag voor 2004 bijna met een factor drie zou toenemen.[25]

In verreweg de meeste gevallen gaat het hier om initiatieven die uitgaan van een server-based wallet. De klant vult daarbij een portemonnee (de wallet) met een bepaalde waarde, en kan vervolgens op websites of bij mobiele diensten opdracht geven een verschuldigd bedrag van die ten laste van de portemonnee te brengen. Bevat deze portemonnee onvoldoende geld dan dient de klant de portemonnee opnieuw op te laden. Een alternatief is een zogenaamde autoload feature, waarbij de portemonnee automatisch met een vooraf afgesproken bedrag wordt geladen als deze leeg raakt.

Overigens zijn niet alleen nieuwe toetreders op deze markt actief. Way2Pay is een dienst die door de ING bank is geïntroduceerd, en de Rabobank heeft een server-based wallet dienst onder de naam Minitix. Het is moeilijk om een standaard te zetten in het woud van initiatieven en standaarden. De Rabobank - toch geen kleine partij - lukt het ook niet met Minitix. ING met 'the way u pay' (vergelijkbaar met paypal) is het ook niet gelukt.

Deze wallet-based micropayment system voor mobiele betalingen zijn de vierde variant. Hoewel deze variant een aantal opzichten lijkt op variant 1, zijn ze bewust niet samengevoegd. In variant 1 gaat het specifiek om telecommunicatieaanbieders. Bij deze laatste spelen dan ook specifieke discussies met betrekking tot regelgeving en toezicht.

Elk van de huidige voorstellen gebruikt eigen vormen van authenticatie. Daarbij kan het bijvoorbeeld gaan om een combinatie van gebruikersnaam en wachtwoord. In de regel hangen die samen met de omvang van de transactie: omdat de wallet in de regel maar tot een bepaald maximaal bedrag kan worden opgeladen, is de maximale schade voor de gebruiker beperkt. Ook het bedrag per transactie kan aan een maximum onderworpen zijn. Daarom kan er genoegen worden genomen met een minder zware authenticatie dan een dienst waarmee duizenden euro's kunnen worden overgeschreven.[26]

---

[24] Zie Rabobank Groep (2003), Beloftes en Valkuilen van Mobiel Betalen (presentatie).

[25] Emerce (13 september 2004): "Microbetalingen in VS hebben wel toekomst".

[26] Indien er gebruikt wordt gemaakt van de hierboven besproken autoload functie dan worden de beveiligingsvereisten natuurlijk weer wat zwaarder.

Opgemerkt dient te worden dat het in deze variant niet alleen draait om e-wallets die gebaseerd zijn op een netwerk van een telecommunicatieaanbieder. Het betreft eveneens lokale radioverbindingen (zoals RFID en Bluetooth) en infrarood.

4.7 Technische invulling bij de varianten: authenticatie

Alle varianten vragen om een technische invulling van talloze onderdelen, zoals die reeds het tweede hoofdstuk zijn aangeduid. Een zeer belangrijk onderdeel daarbij is de authenticatie, en wel om de volgende redenen:

- De authenticatie moet voldoende sterk zijn in relatie tot de transactie;
- Wie authenticeert 'bezit de klant';
- Compromiteringen van authenticatiesystemen kunnen enorme financiële consequenties hebben;
- De mobiele omgeving stelt nog meer eisen aan eisen aan authenticatie dan andere omgevingen al doen, en dat staat vaak ook nog eens op gespannen voet met de benodigde gebruiksvriendelijkheid;
- Authenticatiesystemen zijn complex en de invoering kan een kostbare zaak zijn;
- Authenticatiesystemen kunnen de vrijheid van gebruikers om te wisselen naar andere aanbieders soms beperken (wat weer voordelig kan zijn voor de aanbieders).

Authenticatie bij betaaldiensten bestaat in de regel uit het vaststellen van de authentiteit van het gebruikte pasje/apparaat (' to have') en de identiteit van de gebruiker (vaak met een pincode of wachtwoord; ' to know').

Voor de authentiteit van het gebruikte pasje/apparaat bestaan er in de context van mobiel betalen verschillende mogelijkheden. Vooral de mate waarin de eindgebruiker ongehinderd van betalingsaanbieder of van telecommunicatieaanbieder kan wisselen, verschilt aanzienlijk tussen de voorgestelde oplossingen. In dit perspectief is de dual chip slot oplossing vanuit de eindgebruiker bezien de meest aantrekkelijke oplossing. De betrokken bedrijven kunnen weer voordelen zien in een sterkere koppeling. De daarbij horende lock-in van de klant leidt dan tot minder risico om een klant te verliezen. De dual slot oplossing wordt over het algemeen als minder elegant beschouwd, omdat het voor de eindgebruiker omslachtig is meerdere apparaten mee te moeten nemen en/of per transactie een pasje in een kaartlezer te steken.

Tabel 12: Oplossingen voor authenticatie bij een mobiele terminal[27]

Niet-verwijdbaar beveiligingselement	In de vorm van hardware of software in de handset. Weinig flexibel omdat toestel en bank sterk gekoppeld zijn.
Single chip	De SIM wordt uitgebreid met de bankgegevens; mobiele operator en bank delen dus dezelfde fysieke SIM. Wat minder flexibel door deze koppeling.
Dual chip	In de terminal komt een aparte, uitneembare chip met de bankgegevens, naast de reeds aanwezige SIM
Dual Slot	De drager met bankgegevens is los van de mobiele telefoon. Mogelijkheden: (1) kaartlezer in het toestel, (2) draadgebonden kaartlezer, (3) draadloze kaartlezer en (4) handmatige invoer door de gebruiker ('crypto-calculator')

[27] Onder meer gebaseerd op Telematica Instituut (2002).

Het Mobey Forum spreekt een sterke voorkeur uit voor de dual-chip oplossing. Sommige door ons geïnterviewde marktpartijen vinden de komst van dual chip telefoons echter onwaarschijnlijk en hebben meer vertrouwen in een single chip, gecombineerde (SIM-)kaart.

4.8 Vergelijking van de varianten

De varianten vertonen overeenkomsten en verschillen op een aantal aspecten. In de volgende tabel staat een overzicht.

Tabel 13: Vergelijking van de vier varianten bij mobiel betalen

	Variant 1: Mobiel pinnen	*Variant 2:prepaid betalingen*	*Variant 3: Creditcard betalingen*	*Variant 4: Digitaal muntgeld*
Context	Nationaal	Internationaal	Internationaal	Zowel nationaal als internatiaal
Hoofdrolspelers	Nederlandse banken	Netwerkexploitanten	Creditcard maatschappijen	Nieuwe toetreders of banken
Basiskenmerken	Debet, directe koppeling betaalrekening, pinsysteem	Prepaid (evt. combinatie postpaid), buffering	Semi-buffering[28]	Wallet, buffering
Internationaal forum of normalisatiegroep	- geen – (eventueel Mobey/PPA en ECBS)	SIMpay	Mobile Payment Forum	MeT, Paycircle, Mobey
Authenticatie	Nieuw vorm te geven pinsysteem via mobiel kanaal; eventueel aangevuld met CLI-gegevens.	Authenticatie voortbouwend op GSM security	Doorontwikkeling van de systemen die momenteel voor internetbetalingen worden ontwikkeld?	Diverse methoden, aanbieder-specifiek
Focus betalingsomvang	Macrobetalingen	Microbetalingen, met name mobile-delivered content	Macrobetalingen, internationaal betalingsverkeer	Microbetalingen

4.9 De verwachte kansen van de verschillende varianten

Er blijkt in de markt geen eenduidig beeld te bestaan over de kansen die de diverse initiatieven (en daarmee ook de in dit rapport geschetste varianten) hebben voor een succesvolle introductie en gebruik. Alle varianten worden vooralsnog omgeven door veel onzekerheden. Deze onzekerheden betreffen niet alleen technische zaken, maar het ontbreken van een sluitende business case voor de verschillende varianten. Initiatieven die door de ene marktpartij als erg kansrijk worden gezien, beschouwt een andere marktpartij soms weer als zo goed als dood. Met name de kansrijkheid van internationale, op normgeving gebaseerde

[28] In dit geval wordt niet elke transactie gedebiteerd op de betaalrekening gebeurt dat eens per maand voor alle gedane transacties. Echter, bij individuele transacties wordt wel een on-line security controle gedaan waarbij de gemoeide kosten vergelijkbaar zouden kunnen zijn met die van het debiteren van een betaalrekening.

initiatieven is omstreden. Sommige van deze initiatieven bestaan al ettelijke jaren zonder veel concreets te hebben opgeleverd, maar daar kan aan de andere kant niet zonder meer uit worden afgeleid dat ze geen kans van slagen meer hebben. De internationale normalisatie-initiatieven worden door marktpartijen als weinig belangrijk beschouwd. Bijna elk van deze initiatieven wordt gedomineerd door één bepaald type spelers: telecommunicatiebedrijven, banken of creditcard maatschappijen. Nederlandse marktpartijen geven echter aan relatief weinig van dergelijke initiatieven te verwachten; ze staan in hun ogen te ver van de realiteit en kunnen te weinig inspelen op de sterk uiteenlopende nationale context.

Over de vraag hoe de markt voor verschillende type mobiele betalingen zich zal ontwikkelen bestaat weinig overeenstemming. Over één zaak bestaat wel overeenstemming: de goed ontwikkelde infrastructuur voor pinnen belemmert de uitrol van varianten van mobiel betalen. De transactiekosten van het pinsysteem zijn door de schaalgrootte dusdanig laag dat de introductie van elk ander betalingssysteem duurder zal uitvallen door de kleinere beginschaal. "Van pinnen kun je niet winnen".

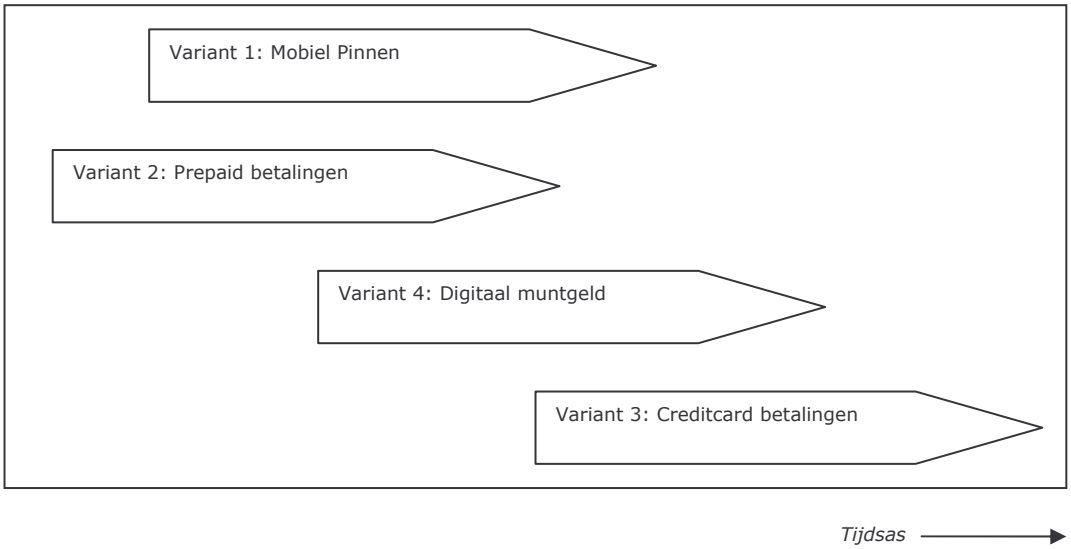
Het ligt voor de hand dat markt voor mobiele betalingen hybride wordt ingevuld en vooralsnog een nationale invulling zal krijgen. De eisen die macrobetalingen respectievelijk microbetalingen aan een systeem stellen[29] lopen zover uiteen dat het onwaarschijnlijk is dat één enkel systeem daaraan voldoende tegemoet kan komen. Naar verwachting zal een gebufferd systeem (met wallets or prepaidtegoeden) de vraag naar micropayments gaan invullen en een on-line systeem met een hoge beveiligingsfactor voor grotere betalingen worden ingezet. Bij micropayments ligt de nadruk op gemak en snelheid en minder op de veiligheid. Voor grotere bedragen zal de nadruk op de veiligheidsaspecten van de betaling gaan en weegt het gebruikersgemak – noodgedwongen – wat minder zwaar mee.

Hieronder volgt een (niet-uitputtende) opsomming van factoren die een rol zal spelen bij de kansrijkheid van een initiatief:

- In welke mate zijn de initiatiefnemers afhankelijk van andere partijen in de waardeketen?
- Hoe groot is de kritische massa van de initiatiefnemers in de nationale of internationale context?
- Hoe groot is de dekking van het initiatief in nationale en internationale termen?
- Hoe ontwikkelt regelgeving zich, en met name de vraag of netwerkexploitanten die werken met prepaid tegoeden onder het EGI-regime zouden vallen?

Verder speelt de vraag op welk deel van de betalingsmarkt de verschillende varianten zich richten. Een gemeenschappelijke noemer in de interviews is dat de mobiele betalingsmarkt naar verwachting ongeveer in de volgende volgorde tot wasdom komt: (1) prepaid betalen (variant 2); (2) mobiel pinnen (variant 1); (3) digitaal muntgeld (variant 4); en creditcard betalingen (variant 3). In figuur 7 is dat in de tijd weergegeven.

[29] Hierbij wordt met name gedoeld op de eisen van beveiliging versus de eisen wat betreft de kostprijs van de transactie.



Figuur 7: Indicatieve tijdsschets voor adoptie varianten

4.10 Samenvatting en conclusies

Er zijn talloze mogelijke invullingen van techniek en waardeketen bij mobiel betalen. Er zijn dus ook talloze initiatieven. In dit hoofdstuk is aan de hand van een aantal criteria een keuze voor een viertal varianten gemaakt:

- Variant 1: Mobiel pinnen;
- Variant 2: Prepaid betalingen;
- Variant 3: Creditcard betalingen;
- Variant 4: Digitaal muntgeld.

Tijdens interviews is gebleken dat deze vier varianten in grote lijnen ook door de betrokken partijen als belangrijkste ontwikkelingsmogelijkheden worden gezien, hoewel partijen verschillen in de kansen die ze de diverse varianten toeschrijven. De ontwikkelingen bij mobiel betalen zijn nog omgeven door veel onzekerheden. Deze zijn primair niet van technische aard. De onzekerheden zijn eerder het gevolg van het ontbreken van een sluitende business case voor mobiel betalen. Juist in Nederland zal mobiel betalen last hebben de markt te veroveren. In Nederland is de (toonbank)betaalmarkt ver ontwikkeld. Het pinsysteem is breed ingevoerd en wordt alom als erg kosteneffectief beschouwd. Chippen begint - na een valse start - ook serieuze omvang te bereiken. Op de meeste deelmarkten voor mobiel betalen vormen deze bestaande systemen geduchte concurrenten, behalve bij de deelmarkt van on-line content.

Door het dilemma tussen nationale en internationale introductie van mobiel betalen zal naar verwachting alleen de deelmarkt van online content betalingen zich snel ontwikkelen. De betalingsmarkt heeft een bij uitstek nationaal karakter. Meer geavanceerde implementaties van mobiel betalen - zoals authenticatie met een additionele chipcard in de mobiele telefoon- vragen echter om een grote (lees: internationale) schaal om op kosteneffectieve wijze ingevoerd te kunnen worden. Dat levert een dilemma op. De verwachting van de meeste marktpartijen is dat mobiel betalen in eerste instantie vorm zal krijgen als nationale, wat minder geavanceerde implementaties. Van internationale initiatieven verwachten marktpartijen nog niet zoveel.

De ontwikkeling van verschillende deelmarkten bij mobiel betalen zal zich over de tijd uitspreiden. De markt voor mobiel betalen zal zich naar verwachting het eerst ontwikkelen als

diensten voor het verrichten van microbetalingen ten behoeven van online content of online diensten (variant 2: prepaid betalingen). Pas wat later in de tijd zullen de andere varianten zich ontwikkelen.

Deel II: Fraude bij mobiel betalen

5 Bestaande vormen van fraude bij telecommunicatiediensten

5.1 Inleiding

Fraude is van alle tijden. De vorm waarin deze verschijnselen plaatsvinden, is vaak een beeld van de tijd. Zo kunnen nieuwe technieken aanleiding geven tot nieuwe vormen van fraude. Ook dit gegeven is natuurlijk niet nieuw, maar het is wel zo dat bij nieuwe, steeds complexere technologieën, het lastiger wordt voor de overheid om deze risico's goed in te schatten en om, anticiperend op deze risico's, eventuele maatregelen in de vorm van beleid en wet- en regelgeving te treffen.

Telecommunicatie en aanverwante gebieden (ICT, elektronisch betalen) is in de laatste decennia een dergelijke complexer technologie geworden. Nieuwe diensten bij vaste telefonie (zoals doorschakelen) en mobiele telecommunicatie hebben tot nieuwe vormen van criminaliteit en fraude geleid. Voor verdere ontwikkelingen, ook op aanverwante gebieden, zal dat opnieuw gelden. We doelen hier op gebieden zoals internet, internettoegang, toegevoegde waardediensten en elektronisch betalen.

In dit hoofdstuk komen de vierde, vijfde en achtste onderzoeksvraag aan bod:

4. Tot welke vormen van (nieuwe) vormen van fraude zouden in de diverse scenario's de technologische ontwikkelingen kunnen leiden?
5. Hoe anticiperen de aanbieders van telecommunicatiediensten en van toegevoeg-dewaardediensten daarop?
8. In hoeverre bieden (parallelle) nieuwe technische ontwikkelingen ook *oplossingen* voor de bestrijding of preventie van de onderzochte vormen van fraude?

Het gaat daarbij steeds om de markt van mobiel betalen. Omdat deze markt echter nog in de kinderschoenen staat, is er voor gekozen om deze vragen éérst te behandelen voor de bestaande markten van telecommunicatiediensten en (reguliere) betaaldiensten. Dit hoofdstuk gaat in op de eerstgenoemde markt, het volgende hoofdstuk van dit rapport gaat in op het de betaalmarkt.

Paragraaf 5.2 vangt aan met een bespreking van de begrippen fraude en telecommunicatiefraude. Paragraaf 5.3 gaat verder met een inventarisatie van allerlei fraudevormen bij huidige netwerken, terwijl paragraaf 5.4 specifiek ingaat op telecommunicatiefraude netwerken die in het verlengde van de GSM-techniek liggen, te weten GPRS en UMTS. Paragraaf 5.5 gaat kort in op andere netwerken, zoals WiFi. Paragraaf 5.6 behandelt maatregelen ter beperking van (reguliere) telecommunicatiefraude. Daarna vervolgt het hoofdstuk met observaties en constateringen uit de markt op basis van de interviews en de expertsessie (paragraaf 5.7).

5.2 Fraude en telecommunicatiefraude

Over het algemeen wordt met de term fraude bedoeld: het doen verkrijgen van goederen en diensten zonder de intentie te hebben hiervoor te betalen. Over de precieze inhoud van het begrip fraude bestaat echter geen overeenstemming. Zodoende zijn ook bij de begrippen telecommunicatiefraude en fraude bij mobiele betalingen verschillende definities mogelijk.

Het Landelijk Expertisecentrum Telecommunicatiefraude hanteert voor telecommunicatiefraude de volgende definitie: '[…] is elke vorm van misbruik van een

telecommunicatievoorziening waardoor de integriteit van de telecommunicatie-infrastructuur kan of wordt aangetast, dan wel het verrichten van enige frauduleuze handeling teneinde een telecommunicatieve dienstverlening te verkrijgen waardoor enig nadeel kan ontstaan en waarbij de gedraging of het nalaten is te kwalificeren las een overtreding van het Wetboek van Strafrecht en/of een bijzondere wet'.

Het gebruik van telecommunicatiediensten als middel om andere vormen van strafbare handelingen te verrichten valt *niet* onder deze definitie. Zaken als het witwassen van crimineel geld en het gebruik van (mobiele) telefoons in de criminele wereld vallen er dus buiten. Dit wil overigens niet zeggen dat er geen verbanden zijn, bijvoorbeeld in de regeling rondom de Melding Ongebruikelijke Transacties (MOT). Die laatste regeling heeft onder meer bij enkele Amsterdamse belhuizen gespeeld.

Fraude kan smal of breed afgebakend worden. Van belang is om in ieder geval onderscheid te maken tussen fraude en het fenomeen dat 'bad dept' wordt genoemd: het niet kunnen betalen van de (telefoon)rekening door de klant, terwijl deze bij het afsluiten van het abonnement wel de intentie had te gaan betalen (en dus geen vervalste gegevens heeft gebruikt). Met andere woorden, klanten die wel willen betalen maar hierin falen. Bad dept verschilt van fraude in die zin dat voor fraude kenmerkend is dat de intentie om te betalen ontbreekt (en altijd heeft ontbroken).

Overigens is fraude een verschijnsel dat absoluut niet uniek is voor de telecommunicatiesector. Allerlei sectoren wordt in meer of mindere mate met fraude geconfronteerd. Wel zijn er enkele redenen aan te wijzen waarom de telecommunicatiesector wellicht wat meer gevoelig is voor fraude:

- De gebruikte technieken in de sector laten een behoorlijk hoge mate van anonimiteit toe, zeker bij hacken en bij mobiele telefonie;
- Telecommunicatiediensten oefenen een bijzondere aantrekkingskracht uit op bepaalde groepen mensen, waarbij het 'kraken' van een systeem als een sport wordt beschouwd;
- Belhuizen blijken gevoelig voor (verwevenheid met of infiltratie door) criminaliteit.[30]

5.3 Huidige vormen van telecommunicatiefraude

Telecommunicatiefraude blijkt allerlei vormen aan te kunnen nemen. Het aantal vormen neemt ook toe. Bij de introductie van nieuwe diensten blijken criminelen snel nieuwe mogelijkheden voor fraude te ontdekken. Kaarten met beltegoed (prepaid) zijn daar een voorbeeld van. In Bijlage 1 is een overzicht gegeven van vormen van telecommunicatiefraude.

De belangrijkste bevindingen met betrekking tot telecommunicatiefraude zijn als volgt:

- Fraude door het gebruik van een valse identiteit staat met stipt op nummer 1, blijkt uit de gehouden interviews. Binnen deze fraudecategorie is er een aantal varianten. Veel van deze varianten zijn niet specifiek voor telecommunicatie en treffen we ook in allerlei andere sectoren aan. Ze zijn vaak in de context van (mobiele) telecommunicatie wel relatief aantrekkelijk voor fraudeurs, omdat ze minder goed te traceren zijn. Bij de afname van een fysiek goed (zoals een tijdschriftabonnement) ligt dat lastiger voor de fraudeur.
- Een tweede belangrijke categorie is fraude die inspeelt op technische tekortkomingen of tekortkomingen in het dienstenconcept.

[30] Dit is de hoofdconclusie van Van Traa-team, 2003.

- Vooral de introductie van premium rate diensten (0900 betaalnummer, premium rate SMS) heeft geleid tot een scala van fraudevarianten. Deze constatering is van bijzonder belang voor dit onderzoek, omdat het hier om een ontwikkeling gaat die de opmaat is voor mobiel betalen.
- Een aantal fraudevormen is specifiek gerelateerd aan mobiele communicatie. Ze maken gebruik van het feit dat de gebruiker gemakkelijk van netwerk kan wisselen (roaming), dat de gebruiker niet eenvoudigweg geïdentificeerd kan worden gebruik van de fysieke aansluitlijn. Andere vormen van fraude spelen in bij abonnementsvormen die we specifiek bij mobiele netwerken tegenkomen, zoals prepaid.[31]
- Bijzonder illustratief bij fraudevormen zijn de zogenaamde autodialers. Dit zijn computerprogrammaatjes die – zonder dat de eindgebruiker dat eigenlijk wil - een betaalnummer aanroepen. Autodialers laat zien hoe een nieuwe fraudevorm in relatief korte tijd om zich heen kan grijpen.

5.4 Fraude bij 2.5G/3G netwerken

Met de introductie van GPRS-netwerken (vaak met 2.5G aangeduid – de twee-en-een-halfde generatie mobiele netwerken) en van UMTS netwerken (met 3G aangeduid) ontstaan nieuwe frauderisico's. Deze hangen enerzijds samen met de centrale rol die het internetprotocol (IP) krijgt in deze nieuwe netwerken (en dat specifieke zwakheden kent) en anderzijds met specifieke implementaties en eigenschappen van 2.5G/3G netwerken zelf. We bespreken deze twee categorieën kort in de onderstaande paragrafen.

Om risico's op fraude niet onnodig te vergroten, bespreken we in het onderstaande alleen fraudevormen die al min of meer 'als algemeen' bekend kunnen worden beschouwd. Onbekende vormen zijn bewust weggelaten uit onderstaande analyse.

5.4.1 Algemene risico's bij IP-gebaseerde netwerken

Belangrijk is dat 2.5G/3G netwerken het internetprotocol (IP) als belangrijkste, onderliggende transporttechniek gebruiken. Dat was nog niet het geval bij de bestaande, circuitgeschakelde GSM netwerken. Het gebruik van IP impliceert ook dat er een IP-nummer moet worden toegekend aan een mobiele terminal. De beperkte adresruimte die mobiele netwerkexploitanten bij IPv4 tot hun beschikking hebben, laat (nog) niet toe iedere mobiele terminal een vast IP-adres toe te wijzen. Daarom gebeurt dit op dynamische wijze: voor een specifieke sessie wordt een bepaald nummer toegewezen. Als IPv6 eenmaal algemeen is ingevoerd dan is er wel de mogelijkheid alle terminals vaste adressen toe te kennen. Overigens zijn er in het geval van roaming zonder meer extra, tijdelijke IP-adressen nodig.

Het gebruik van IP introduceert een aantal risico's en zwakheden die we reeds uit de internetwereld kennen, plus een aantal nieuwe risico's die samenhangen met de specifieke implementatie van IP in deze mobiele netwerken. Het betreft hier vooral Denial-of-Service (DoS) aanvallen en binnendringen van het systeem. In het eerste geval legt een hacker een (mobiel) netwerk deels of volledig plat. In het tweede geval weet een hacker ongeautoriseerd toegang tot informatie te verkrijgen. We noemen hier een aantal voorbeelden van aanvallen die bekend zijn in de internetwereld en die ook een risico vormen bij 2.5G/3G netwerken:

- IP spoofing: aanvallen die een vervalst adres van de afzender gebruiken (een afzender die de firewall als betrouwbaar beschouwt).

[31] Prepaid komt overigens ook voor bij vaste netwerken, in de vorm van de zogenaamde calling cards.

- Smurf: het sturen van zogenaamde IP broadcastberichten naar systemen die geconfigureerd zijn om daarop te antwoorden. Een voorbeeld is PING.[32] Als deze berichten in grote hoeveelheden worden verstuurd, levert dat een zware netwerkbelasting op en kan een netwerk overbelast raken. Het netwerk slaagt er dan niet meer in andere gebruikers de diensten tegen de gewenste kwaliteit te bieden.
- SYN flood: het bestoken van een systeem met berichten en daarbij misbruik makend van een zwakheid in het handshaking systeem bij het internetprotocol.[33]
- Ethernet sniffing: de interceptie van pakketjes die onderweg zijn in het transitnetwerk. Zo kunnen wachtwoorden afgeluisterd worden. Bij internet is dat transitnetwerk groot en zijn de routes niet eenvoudig voorspelbaar.
- Port scanning: het systematisch benaderen van zogenaamde 'poorten' bij een ontvangend systeem om het gedrag te analyseren en eventuele openstaande poorten te identificeren.[34]
- Buffer overflow: Door het met opzet sturen van niet-valide berichten (zoals een tekstveld van 256 ipv. 255 karakters) kunnen systemen op abnormale wijze hun werking afbreken en vastlopen.
- TCP Hijack. De hacker identificeert een gebruiker die zich net aanmeld, legt het systeem van die gebruiker vervolgens plat (bijv. door een DoS aanval) en neemt de verbinding over. Er is dan meestal geen nieuwe authenticatie met een password e.d. nodig.

5.4.2 Specifieke risico's bij 2.5G / 3G netwerken

Er schuilen ook risico's in het complexer worden van de verkeersgegevens en de analyse daarvan in het netwerk. Afname van een enkele dienst kan veel meer CDR's[35] opleveren dan nu het geval is. Deze CDR's kunnen bovendien van veel meer netwerkelementen afkomstig zijn, waarbij bovendien de eindgebruiker vaak op verschillende wijzen wordt geïdentificeerd (IMSI[36], IP-nummer, tunnel). Dit maakt de zogenaamde mediation systems[37] veel complexer en gevoeliger voor fraude.

Juist om de voor mobiele netwerken essentiële mobiliteit van de eindgebruiker (hand-over, roaming) mogelijk te maken, kennen 2.5G/3G netwerken het concept van *tunneling*. In een dergelijke tunnel kunnen meerdere (IP)-sessies worden ondergebracht, terwijl een IP-sessie ook over meerdere verschillende tunnels verdeeld kan zijn of in de tijd (bijvoorbeeld bij een

---

[32] Het PING commando bij het internet verzoekt de geadresseerde computer een korte reactie te sturen. Het is een voor technici essentiële functie om configuraties te controleren en fouten op te sporen.

[33] Handshaking is een essentieel onderdeel van een communicatiesessie, bij welk communicatiesysteem dan ook. Bij het internetprotocol (TCP/IP) stuurt de ontvanger een bevestiging van goed ontvangen pakketjes. De zender moet dan met een bepaald bericht (RST) reageren. Als de zender nu gespooft is (zie hierboven) komen de bevestigingen nooit aan. Door op deze wijze de ontvanger te bestoken met pakketjes zonder deze ooit het RST bericht te laten ontvangen lopen de interne buffers op een gegeven moment vol en werkt het systeem niet meer naar behoren.

[34] Illustratief is de website https://grc.com/x/ne.dll?bh0bkyd2. Deze site stelt de gebruiker zelf in staan om vanaf afstand een port scan op te starten en om zo eventuele zwakheden in zijn eigen system te ontdekken.

[35] Een Call Detail Record (CDR) is een berichtje dat wordt aangemaakt bij iedere afgenomen dienst (zoals een telefoongesprek of een SMS). In het CDR staan gegevens die van belang zijn voor het opstellen van de factuur, zoals de duur van het gesprek en de bestemming.

[36] IMSI: International Mobile Subscriber Number.

[37] Mediation systems zijn systemen die data voor het billingproces verzamelen, bewerken en in één of meer genormaliseerde formaten aanleveren aan de systemen die de uiteindelijke rekeningen opmaken.

handover) kan 'overstappen' van de ene tunnel naar de andere. Juist dit tunnelconcept introduceert een aantal belangrijke zwakheden wat de beveiliging betreft. Enkele voorbeelden:

- Aanvallen via de roaming-interface tussen twee netwerken: het UMTS-protocol kent op dat algemeen gedefinieerde punt namelijk geen security.[38]
- Aanvallen op de SGSN / GGSN[39] of de communicatie tussen deze netwerkelementen (met GTP[40] aangeduid). Omdat het hier relatief onvolwassen systemen betreft en de 'netwerkinterne' procedures meestal geen authenticatie behoeven, liggen er hier zwakheden.
- De eindgebruiker betaalt in een aantal gevallen voor ongevraagd verkeer. Door het sturen van ongevraagde pakketten naar een eindgebruiker (zoals dubbele pakketten) kan de laatste met ongewenste rekeningen worden geconfronteerd ('overbilling'). Er bestaan hierbinnen meerdere varianten.

Verder moet er op worden gewezen dat software bij netwerkelementen vaak nog relatief onvolwassen is. In de praktijk blijkt dat zelfs relatief onschuldige configuratiefouten kunnen leiden tot uitval van onderdelen in het netwerk; veel specialisten zijn er van overtuigd dat dergelijke netwerken heel slecht bestand zijn tegen een gerichte aanval van buitenaf.

Netwerkexploitanten hebben inmiddels een groot aantal frauderisico's geanalyseerd en bereiden zich voor op een efficiënte bestrijding ervan. Gegeven het complexe karakter van de gebruikte technieken is de kans groot dat veel vormen van (technische) fraude niet door exploitanten vooraf geïdentificeerd worden en dat ze reactief moeten ingrijpen nadat een fraudeur ze heeft ontdekt.

5.5 Fraude bij andere typen mobiele netwerken

De betekenis van alternatieve netwerktypen als WiFi en WiMAX neemt toe. Deze netwerken hebben wellicht ook specifieke fraudevormen. Aangezien de implementatie van deze netwerken varieert - ook binnen hun eigen categorie - is het binnen de strekking van deze studie onmogelijk een uitputtend overzicht te presenteren van fraudevormen. Het merendeel van de nieuwe netwerken is wel gebaseerd op het internetprotocol dus er kan wel geconcludeerd worden dat de in de vorige paragraaf besproken algemene risico's bij IP-gebaseerde netwerken ook bij deze netwerken spelen. Een voorbeeld hiervan betreft ongeautoriseerd toegang tot netwerken, mede als gevolg van zwakke software.

5.6 Maatregelen ter beperking van (reguliere) telecommunicatiefraude

De huidige omvang van telecommunicatiefraude is aanzienlijk: een recente schatting van de Communication Fraud Control Association stelt dat wereldwijde schade door fraude ongeveer 35 - 40 miljard dollar zou bedragen, en dat de groei daarvan met 11-25% veel hoger is dan de groei van de industrie zelf. In een ander bericht uit het jaar 2000 wordt gesteld dat telecommunicatiefraude de branche wereldwijd in totaal meer dan 22 miljard dollar per jaar kost. Daarvan bestaat ruim 18 miljard dollar uit fraude met vaste lijnen, en ruim 4 miljard dollar uit mobiele telefonie.[41] De onderzoekers wijten de fraude aan het gebrek aan personeel

---

[38] Dit blijkt uit de betreffende specificaties van de UMTS norm: 3GPP TS 09.60.

[39] De SGNS (Serving GPRS Support Node) en GGSN (Gateway GPRS Support Node) zijn twee zeer belangrijke netwerkelementen in een GPRS of UMTS network.

[40] GTP: GPRS Tunneling Protocol.

[41] De cijfers op basis van onderzoek door Chorleywood Consulting, genoemd op Total Telecom en daarna aangehaald op Zeeburgnieuws (www.zeeburgnieuws.nl/rubriek/internet/internet-week29.html)

met expertise bij nieuwkomers op de markt. Zij besteden geld aan alles dat het netwerk snel dichter bij de klant kan brengen.

Overigens is het niet eenvoudig om de schade voor de sector als gevolg van fraude goed vast te stellen. Enerzijds blijven veel vormen van schade weer onzichtbaar. Dat komt omdat:

- De schade niet alleen geleden kan worden door telecommunicatiebedrijven maar ook door andere partijen, zoals grote ondernemingen wiens telefooncentrale is gekraakt
- Fraude soms niet gemeld wordt uit angst voor schade aan de reputatie. Aanknopend aan het hierboven genoemde voorbeeld zal een bank niet graag naar buiten brengen dat haar telefooncentrale is gekraakt.
- De schade kent vaak een buitenlandkarakter. Onderlinge afspraken en de gebruikte technische infrastructuur bepalen daarbij voor wiens rekening de schade komt.
- Fraudezaken zijn complex, vereisen specialistische kennis en worden lang niet altijd waargenomen of opgelost.[42]

Anderzijds hebben veel bedrijven moeite om het onderscheid te maken tussen bad dept en fraude, wat dan weer leidt tot een overschatting van de schade door fraude. Alles bij elkaar genomen is de algemene verwachting echter dat de uitgedragen fraudecijfers veel te laag zijn; volgens sommige analisten is dat slechts een derde van het werkelijke bedrag.[43]

Met de introductie van een aantal nieuwe technieken ontstaan er ook nieuwe risico's voor fraude. Het betreft hier met name risico's voor technische fraude: handelingen die gebruik maken van onvolkomenheden ('gaten') in het systeem.

Uit het voorgaande blijkt dus dat telecommunicatiefraude een forse omvang kent. Operators hebben dan ook allerlei maatregelen getroffen om deze schade te beperken. Het proces van het detecteren en voorkomen van fraude en wanbetaling wordt in de marktsector telecommunicatie veelal aangeduid met de term 'Revenu Assurance Process'. Het is een verzamelbegrip voor allerlei maatregelen die een aanbieder van telecommunicatie binnen zijn bedrijf kan nemen teneinde omzetverlies door fraude en wanbetaling te voorkomen dan wel beheersbaar te maken. Ze realiseren zich daarbij dat onmogelijk zal zijn om fraude in zijn totaliteit uit te roeien.

Er is een groot aantal tools beschikbaar ter ondersteuning van fraudebestrijding. Deze tools/systemen zijn onder te verdelen in een aantal categorieën, waaronder:

- Producten ter bepaling van de authenticiteit van een beller;
- Risico-evaluatie producten voor acceptatie van nieuwe klanten;
- producten voor spraakherkenning ter identificatie van een beller;
- RF handtekening producten ter identificatie van de radiofrequentie (RF) 'fingerprint';
- PIN's ter identificatie van een beller;
- Producten voor patroonherkenning ten behoeve van het evalueren van bel- en betalingsprofielen.[44]

---

[42] Zo kan een zeer groot bedrijf het niet doorhebben dat maandelijks een zeker bedrag kwijtraakt als gevolg van telecommunicatiefraude.

[43] Ibid.

[44] Zie Benedick, 2002, p.102. On-line monitoring van *verandering* van het gedrag van de klant. Veel klanten vertonen een vast patroon, bijvoorbeeld het aantal transacties, frequentie, hoogte van betalingen, duur van de telefoongesprekken en bestemmingen van telefoongesprekken. Op basis van dit gedrag wordt vastgesteld wat *gebruikelijk* is voor een specifieke klant. Een fraudeur - bijvoorbeeld iemand met een gestolen GSM - heeft er niet zoveel aan om dezelfde bestemmingen te bellen of dezelfde bedragen over te maken naar dezelfde rekeningen om niet op te vallen. Deze vertoont dus afwijkend gedrag. Monitoring kan binnen Nederland op near-real-time basis (0-5 minuten). Buiten Nederland is er bij monitoring een vertraging mogelijk die kan oplopen tot 48 uur. Dat komt door onderlinge clearing activiteiten op gezette

Een aantal van deze tools is specifiek voor het vaste netwerk ontwikkeld, andere voor mobiele netwerken en weer andere kunnen voor beide netten worden ingezet. Elk product heeft zijn eigen type toepassing. Zo zullen RF- en producten voor spraakherkenning met name van belang zijn ter bestrijding van 'cloning' (en daarmee vooralsnog alleen interessant voor de bestijding van fraude in analoge netwerken). Voor GSM en volgende standaarden zijn met name de producten voor patroonherkenning (profilers) van belang.

Fraudemanagement systemen vormen een onmisbare tool bij de preventie en detectie van fraude en wanbetaling. Het functioneren van dergelijke systemen hangt in sterke mate af van de mogelijk te raadplegen bestanden. Hoe meer bronnen uiteindelijk geraadpleegd worden, hoe groter de kans dat slechte betalers en fraudeurs in een vroeg stadium worden geïdentificeerd.[45]

- *Controle door middel van interne klantgegevens*; toetsing van de klantgegevens vindt plaats aan de hand van bepaalde criteria; of en hoe een klant bekend is binnen de eigen database van het bedrijf en of op basis van deze criteria de klant in aanmerking komt voor een volgende aansluiting. Hierbij kan gedacht worden aan een betalingsachterstand, een verstrekt abonnement dat tot financiële schade heeft geleid alsmede een maximum aantal aansluitingen dat is bereikt.
- *Controle door middel van externe klantgegevens*; dit is de controle waarbij gebruik gemaakt wordt van externe bronnen waaronder: het huisnummer en postcodebestand, CD-foongids, het Verificatie Informatie Systeem (VIS) en Bureau Krediet Registratie (BKR), handelsinformatiebureaus.
- *Controle door middel van order en planningsgegevens*; Geaccepteerde aanvragen door klanten worden verwerkt in een werkorder. In geval van afsluitingen wordt de klant fysiek afgesloten aan de hand van een interne order. Door middel van periodieke integriteit checks kan een telecommunicatieoperator vaststellen of de aansluitgegevens nog juist en volledig zijn. Daarnaast kan door middel van bestandsvergelijking periodiek worden vastgesteld of de technische aansluitbestanden consistent zijn met het commercieel bestand.
- *Controle door middel van reconciliation*; aan de hand van controletotalen dient te worden vastgesteld of alle gespreksrecords (call detail records) vanaf de telefooncentrales zijn verwerkt en alle gesprekken (air usage time) hebben geleid tot een externe en interne (kosten)verrekening.
- *Controle door middel van dynamische risico-analyse*; Verdachte gesprekken of transacties worden naar (potentiële) schade gerangschikt. Met behulp van elektronische checklists (workflow management) worden risico's vanuit verschillende perspectieven geanalyseerd: naar gesprekken of transacties, naar subjecten (bellers), naar objecten (centrales, routers) en naar bedrijven. Naar aanleiding van de verschillende (real-time) waarschuwingssignalen kunnen de fraude-experts al dan niet besluiten direct actie te ondernemen. Expert opinies en follow-up acties worden opgeslagen in een casemanager. Daardoor zijn ze beschikbaar voor hergebruik door andere onderzoekers en risico-analisten.
- *Controle door middel van verkeersanalyse*; Door middel van verkeersanalyses controleert een operator de toerekening van de kostencomponenten naar de

---

tijden. De schade kan dan erg snel oplopen, vooral bij inbellen naar premiumrate diensten (zie fraudegeval).

[45] Belangrijke informatiebronnen zijn: Call detail records (CDR's), SS7 signalling informatie, belprofielen van individuen of groepen, betalingsprofielen; de betalingsgeschiedenis van een bepaalde klant uit het CC&B systeem, centrale klantenregistratie, fraude database, Bureau Krediet Registratie, klantgegevens vaste net en MOSAIC (informatie over huishoudens in Nederland).

uitgevoerde diensten. Enerzijds is het van belang voor de vaststelling van de telecommunicatietarieven. Anderzijds is het van belang voor de tariefberekening aan andere telecommunicatiebedrijven volgens de 'open network provision', die door de toezichthouder OPTA wordt bewaakt.

- *Controle door middel van integriteits checks*; Door middel van periodieke tabelcontroles wordt vastgesteld of de gehanteerde tarieven, kortingen en pakketafspraken in overeenstemming zijn met geautoriseerde prijsstellingen. Met behulp van proceduretesten wordt met steekproeven vastgesteld of de facturering en administratieve verwerking juist plaatsvindt.
- *Controle door middel van afloopcontroles op vorderingen*; Door middel van analyses op openstaande vorderingen (in combinatie met call center en klachtbehandeling) wordt het betaalgedrag van de abonnee gecontroleerd. Waar mogelijk wordt actueel belgedrag vergeleken met betaalgedrag te minimalisering van schade van fraude of van fouten.
- *Controle door middel van fraudedetectie*; Door middel van transaction monitoring kan een operator alle gesprekrecords online bewaken op verdacht belgedrag. Transaction monitoring gaat niet primair uit van vooraf gedefinieerde profielen en voorspelbaar (frauduleus) gedrag, maar baseert de techniek zich op feitelijke transacties en de afwijkingen daarop in vergelijking met het historische bel- en betalingsprofiel. Afwijkingen daarop vergroten de risico's van fraude, fouten en mistoestanden, ook als die niet vooraf aangemerkt zijn als frauduleus. De ontwikkeling van fraudedetectietechnieken wordt hieronder beknopt besproken.
- *Controle door middel van slimme vragen*; de klant wordt (telefonisch) benaderd met een aantal handig geformuleerde vragen, waarbij antwoorden helpen om vast te stellen of er wellicht sprake kan zijn van een fraudeur.

Telecommunicatiefraude blijkt in de praktijk echter moeilijk te detecteren. In feite is fraudedetectie – mede gelet op de grote hoeveelheden Call Detail Records, die binnen een bedrijf van een aanbieder van telecommunicatie(diensten) worden gegenereerd- alleen mogelijk met behulp van elektronische hulpmiddelen.

In de jaren tachtig werd het detecteren van ongewone gesprekken als afdoend middel beschouwd in de fraudebestrijding. In die periode was de elektronische communicatie nog relatief beperkt. Identificatie van bellers (en fraudeurs) was goed te doen. In de jaren negentig, toen internet, e-mailing, mobiele telefonie (met name prepaid en SMS) en breedband alsmede de privatisering hun intrede deden, werd de elektronische communicatie steeds meer vervlochten met het dagelijks (bedrijfs)leven. Het werd steeds moeilijker ongewone transacties te koppelen aan personen om deze vervolgens te kunnen identificeren. De bestaande fraudedetectiesystemen voldeden niet meer; meer intelligente systemen werden noodzaak in de fraudebestrijding.

Een belangrijke trend in mobiele telecommunicatie is het feit dat de relatie met de klant steeds minder face-to-face geschiedt, waardoor de afstand tussen het telecommunicatiebedrijf en de klant steeds anoniemer wordt. Het fysiek identificeren van een beller (met behulp van een legitimatieplicht) wordt in belangrijke mate overgenomen door het vastleggen van belpatronen, duur van de gesprekken, starttijden, type gesprekken (lokaal, sms, data), bestemmingen, enzovoort kortom een elektronisch profiel of fingerprint van de klant. Het 'ken-je-klant' principe gaat dus niet verloren maar wordt ingevuld volgens het 'ken-het elektronische-profiel (van je klant)' principe. In onderstaande box wordt nader ingegaan op 'fingerprinting'.

Box 1: Fingerprinting

De identiteit van de persoon achter een aansluitnummer wordt door fingerprinting niet bepaald aan de hand van zijn identiteitsbewijs maar aan de hand van zijn contacten op het netwerk (fingerprint). Door deze identiteiten te bewaren - en zeker die van bij de dienstenaanbieder bekende fraudeurs - kan later onderzocht worden of het gedrag en dus ook de identiteit van andere, nog niet bekende contractanten overeenkomt met die van reeds bekende fraudeurs. Of dat de persoon in kwestie een intensieve relatie heeft met een bekende fraudeur. Op deze manier kan actie ondernomen worden teneinde financiële schade bij de betreffende provider te voorkomen.

Een nieuwe klant kan bijvoorbeeld al als verdacht worden aangemerkt als twee bestemmingen in zijn 'fingerprint' overeenkomen met de bestemmingen van een bij de dienstenaanbieder bekende fraudeur. Deze techniek wordt ook gebruikt om reeds bekende non-incasso klanten, die onder een andere naam opnieuw geactiveerd worden, vroegtijdig te kunnen detecteren. Daarnaast worden de profielen bijvoorbeeld vergeleken met het belgedrag in voorgaande periodes zodat de mate van afwijking in de tijd kan worden vastgesteld.

Vanaf eind jaren negentig is bovenop het identificatievraagstuk de behoefte aan sporenonderzoek - tracking & tracing -, casemanagement maar bovenal snelheid van detectie, analyse en navigatie (ophalen brontransacties) ontstaan. Elektronische identificatie van personen en elektronische fingerprints zijn belangrijke systeemeisen geworden ter ondersteuning van bedrijfsbeheer, risicomanagement alsmede opsporing en vervolging. Deze ontwikkeling heeft geleid tot een intelligent transaction monitoring systeem op basis van database technieken.[46]

Het fraudedetectiesysteem is in de afgelopen twee decennia geëvolueerd van een mechanisch, rechttoe rechtaan fraudedetectiesysteem tot een intelligent, integraal risicomanagementsysteem. Ook de scope van fraudedetectiesystemen is verbreed waardoor deze systemen niet meer alleen fraud- en riskmanagers zijn bestemd maar ook ondersteunend kunnen zijn voor forensische onderzoeken, opsporing en controle-/accountancywerkzaamheden.

De belangrijkste lessen uit de huidige vorm van fraude en fraudebestrijding zijn dat de subscription en identify fraud de grootste bronnen van fraude blijven (dit wordt in verschillende interviews bevestigd). Bovendien vormt de fraude een aanzienlijke schadepost op de balans.

Het fingerprinting principe is krachtig maar werkt reactief: de fraude is al gepleegd. De fraudeur heeft niks aan bellen naar de schoonmoeder of geld overmaken naar de dezelfde bankrekeningen van de oorspronkelijke eigenaar van de mobiele telefoon. De afwijkende transacties vallen op en de fraude kan in een vroegtijdig stadium gedetecteerd en gevolgd worden. Verder zijn er een heleboel aangrijpingspunten zijn om de fraude lastiger te maken (in inbouwen van allerlei beveiligingselementen en controlemechanismen) en sneller te detecteren. Hierdoor lijkt het mogelijk de omvang van de schade door telecommunicatie terug

[46] Voorbeelden van objectgeoriënteerde technieken zijn dynamische risico-analyse, profilering, patroonherkenning, signalering hoogverbruik, signalering gesprekken zonder abonnee, call back gesprekken en gesprekken korter dan 2 seconden, signalering corrupte en incomplete gespreksrecords, oorzaak analyse (root cause analysis), signalering gesprekken met een onbekende servicecode, signalering gesprekken van en naar verdachte landen, navigatie en MS Windows gebaseerde opvraagtechnieken en case management.

te brengen naar een acceptabel niveau. Overigens is er zoals eerder vastgesteld weinig bekend over de exacte omvang van fraude (de interviewrespondenten kunnen daar ook geen inzicht in verschaffen).

5.7 Observaties en constateringen uit de markt

Op basis van interviews en desk research is een aantal bevindingen gedaan betreffende telecommunicatiefraude.

In het verleden is gebleken dat bij de introductie van nieuwe diensten en systemen vooral technische fraude toeneemt. Fraudeurs ontdekken gaten in het systeem waar ze handig gebruik van weten te maken. Deze gaten zijn niet altijd even gemakkelijk te voorspellen door de aanbieders. Voorbeelden betreffen de introductie van doorschakelen op het vaste net. Enige tijd daarna ontdekten fraudeurs slimme manieren om geld te verdienen aan de mogelijkheden die doorschakelingen kunnen bieden, zoals het activeren van deze dienst op een telefoontoestel in een café of restaurant. Als het een doorschakeling naar een koopnummer betreft, krijgt de houder van het establishment een forse rekening gepresenteerd. Door maatregelen van de netwerkexploitant (in dit geval de mogelijkheid bepaalde categorieën doorschakelingen uit te schakelen op een bepaalde aansluitlijn) werd de fraudevorm weer bestreden. Een meer recent voorbeeld betreft de groei van fraude met behulp van de zogenaamde autodialers. Momenteel brengt de introductie van 2.5G en 3G veel technische vernieuwingen met zich mee. Met name het daarin centraal staande internetprotocol kent een aantal zwakten die (technische) fraude in de hand werken. Verwacht wordt dan ook dat bij deze introductie er weer diverse vormen van technische fraude de kop op zullen steken.

Door de groeiende complexiteit van de markt en waardeketen is fraude steeds lastiger te bestrijden. Het bovengenoemde voorbeeld van de autodialer kan daarbij als illustratie worden gebruikt. De klant heeft onbedoeld een autodialer binnengekregen als bijlage bij een emailbericht (in de vorm van een trojan horse). Dat bericht werd gerouteerd door een aanbieder van emaildiensten (bijv. Hotmail of Gmail). Het bericht werd vervolgens getransporteerd door een internetaanbieder (bijv. Chello of Cistron), die eventueel diensten inkocht van een aanbieder van aansluitnetwerken (bijv. UPC of BBned). Vervolgens installeert de autodialers zich op de computer van de gebruiker, en belt – onbedoeld – via een telefoon (bijv. geleverd door KPN) naar een 0900-nummer. Daarbij zijn zowel een platformaanbieder als een dienstenexploitant betrokken.

Niet alleen maakt een complexer waardeketen het lastig om fraude te bestrijden. De kans op fraude neemt ook toe door (malafide) bedrijven die tot deze waardeketen toetreden. Ook nu zijn er bij premium rate nummers talloze min of meer malafide partijen actief. Dat varieert van diensten die het klanten amper mogelijk maken om hun abonnement op te zeggen tot 0900-nummers die alleen maar – onbedoeld - aangeroepen worden door autodialers. Deze praktijken waren reeds de aanleiding tot een code voor zelfregulering in de sector. Deze ontwikkeling zal zich mogelijk voortzetten en versterken als de waarketen complexer wordt en als de diversiteit van diensten (en mogelijkheden daartoe) toeneemt.

Zoals al blijkt uit het voorstaande zijn fraudevormen slechts in beperkte mate te voorspellen. Hoewel marktpartijen zich inspannen om ex-ante deze risico's in kaart te brengen en hun systemen afdoende tegen misbruik te beschermen zijn lang niet alle technische en niet-technische risico's vooral te voorspellen. Aanbieders zijn dan ook in belangrijke mate aangewezen op een reactief fraudebeleid. Het is een gegeven dat deels achter de feiten zult blijven aanlopen.

Verder blijkt uit de ervaringen bij telecommunicatiefraude dat het niet alleen om individueel opererende fraudeurs gaat, maar dat er ook goed georganiseerde bendes actief zijn. Deze hebben vaak internationale vertakkingen. Deze bendes richten zich momenteel vooral op fraude met betaalnummers (waarbij ze zelf de exploitant/'dienstenaanbieder' van dat nummer

zijn), fraude via belhuizen en met (grensoverschrijdende) fraude met mobiele telefoonkaarten. Wellicht gebruiken bendes telecommunicatiediensten ook voor het witwassen van geld, maar dit onderzoek geeft daar onvoldoende zicht op.

Nieuwe toetreders tot de telecommunicatiemarkt lopen een verhoogd risico op schade door fraude. De aandacht voor fraude en de effectiviteit van de bestrijding daarvan is noodgedwongen lager dan bij gevestigde spellers. Plegers van fraude zullen inspelen op deze zwakte en zich juist op deze partijen richten.

Uit gesprekken en de literatuur mag worden opgemaakt dat ook interne fraude een aanzienlijke omvang heeft. Het gaat daarbij om fraude door (of met behulp van) medewerkers. Sommige bedrijven rekenen fraude door dealers ook tot interne fraude. Gezien het karakter van deze studie gaan we echter niet dieper in op interne fraude.

5.8 Samenvatting en conclusies

Om zicht te krijgen op de vraag welke vormen van fraude er spelen bij mobiele betaaldiensten en hoe aanbieders daar op kunnen anticiperen, bespreekt dit hoofdstuk deze vragen eerst voor de 'reguliere' telecommunicatiemarkt. Deze markt kent in de vorm van Premium Rate Services (PRS) een behoorlijk aantal vormen van betaaldiensten. Fraude met deze betaaldiensten is een startpunt voor de bestudering van fraude bij mobiel betalen.

Belangrijk is de definitie van het begrip fraude. Deze definitie is in dit hoofdstuk verder uitgewerkt. Van groot belang is de vaststelling dat fraude iets is dat met intentie vooraf plaatsvindt. De schadepost die bekend staat als bad dept (gebruikers die wel willen maar niet kunnen betalen) hoort daardoor niet tot fraude, hoe groot de inkomstenderving door dit verschijnsel in de praktijk ook is.

De belangrijkste conclusies bij dit hoofdstuk zijn als volgt:

- Er bestaat een grote diversiteit aan fraudevormen. Deze zijn vaak terug te brengen naar fraude met betrekking tot de identiteit van de gebruiker (valse naam, vervalste aanvraag, etc.) en fraude waarbij men gebruik maakt van technische tekortkomingen.
- De categorie met betrekking tot de identiteit van de gebruiker wordt bij interviews genoemd als de belangrijkste fraudecategorie in de zin van geleden schade.
- Door een onverminderde aandacht voor fraude en door geavanceerde detectiesystemen kunnen de financiële gevolgen van fraude binnen acceptabele proporties worden gehouden. Zeker bij de introductie van nieuwe diensten of technieken wordt er veel aandacht besteed aan fraudeanalyses. Geïnterviewden geven echter aan dat fraude nooit te voorkomen valt en dat er zich elke keer weer nieuwe vormen aandoen, zeker bij de introductie van nieuwe diensten of technieken.
- Nieuwe toetreders tot de telecommunicatiemarkt lopen een verhoogd risico op schade door fraude. De aandacht voor fraude en de effectiviteit van de bestrijding daarvan is noodgedwongen lager dan bij gevestigde spelers.
- De introductie van 2.5G en 3G neemt veel technische vernieuwingen met zich mee. Met name het daarin centraal staande internetprotocol kent een aantal zwakten die (technische) fraude in de hand kunnen werken.

6 Bestaande vormen van fraude bij betaaldiensten

6.1 Inleiding

Het voorgaande hoofdstuk omvatte een analyse van fraudevormen bij telecommunicatiediensten om zicht te krijgen op vormen van fraude die bij mobiel betalen relevant kunnen zijn. In dit hoofdstuk gebeurt hetzelfde voor (bestaande) vormen van fraude bij betaaldiensten. De opgebouwde inzichten dienen als input voor hoofdstuk 7, dat verwachte vormen van fraude bij mobiel betalen behandelt.

In dit hoofdstuk komen wederom om de vierde en vijfde onderzoeksvraag aan de orde, maar de beantwoording richt zich nu specifiek op bestaande vormen van fraude die met betaaldiensten te maken hebben (en hoe aanbieders hierop anticiperen). In het vorige hoofdstuk was de beantwoording gericht op telecommunicatiefraude over het algemeen en in het volgende hoofdstuk komen dezelfde vragen aan de orde, maar staan *nieuwe* vormen van fraude centraal. De te beantwoorden onderzoeksvragen zijn:

4. Tot welke (nieuwe) vormen van fraude zouden in de diverse varianten van mobiel betalen de technologische ontwikkelingen kunnen leiden?
5. Hoe anticiperen de aanbieders van telecommunicatiediensten en van toegevoegdewaardediensten daarop?
8. In hoeverre bieden (parallelle) nieuwe technische ontwikkelingen ook *oplossingen* voor de bestrijding of preventie van de onderzochte vormen van fraude?

Opnieuw vangt dit hoofdstuk aan met een verkenning van fraudevormen, maar nu specifiek voor betaaldiensten (paragraaf 6.2). Daarna worden maatregelen besproken die worden genomen ter beperking van betaalfraude (paragraaf 6.3). Daarna vervolgt het hoofdstuk met observaties en constateringen uit de markt op basis van de interviews en de expertsessie (paragraaf 6.4).

6.2 Fraude bij betaaldiensten

Analoog aan het vorige hoofdstuk zijn tijdens dit onderzoek ook fraudevormen bij betaaldiensten geïdentificeerd. Dit heeft plaatsgevonden op de basis van literatuuronderzoek, interviews en een expertworkshop. Het doel van de inventarisatie is om kennis op te bouwen met betrekking tot fraudevormen en wat daar om heen speelt. Bij deze brede inventarisatie is nog niet stilgestaan bij de precieze afbakening van fraude die we verderop in dit rapport zullen hanteren.

In Bijlage 2 wordt een overzicht van fraudevormen gepresenteerd. Sommige van de daar besproken fraudevormen hangen specifiek samen met bepaalde betaalmiddelen; zo speelt misbruik bij card-not-present betalingen alleen bij creditcards. Als daar sprake van is, wordt dat in de bijlage aangegeven.

Ook hier kunnen we een onderscheid maken tussen fraude met betrekking tot de identiteit van gebruikers of partijen (relatiefraude) en wat we 'technische fraude' kunnen noemen. Opmerkelijk is dat er heel veel fraudevormen in de eerste categorie vallen, en maar enkele in de tweede. Dat is een groot verschil met de in het vorige hoofdstuk besproken telecommunicatiefraude. Daar zijn verschillende verklaringen voor te bedenken. De eerste is dat veel bancaire systemen zeer verfijnd zijn en dat bancaire authenticatiesystemen veel beter zijn dan bij telecommunicatie dat technische fraude beperkt is. Het kan echter ook zo zijn dat

financiële instellingen er beter slagen om fraudegevallen en fraudevormen binnenshuis te houden. Ze delen dergelijke informatie wellicht minder snel met de buitenwereld.

6.3 Maatregelen ter beperking van betaalfraude

De bestrijding van betaalfraude krijgt al lang veel aandacht. Dat heeft te maken met de vertrouwensrelatie tussen bank en rekeninghouder: waar een gewone marktpartij (zoals ook een telecommunicatieaanbieder) nog kan redeneren dat een bepaalde fraudelast acceptabel is, wordt van een bank verwacht dat deze "zonder ook maar een cent te verliezen" zich hoedt over het kapitaal dat rekeninghouders storten. Banken staan bovendien onder een streng wettelijk toezichtregime.

Uitgevers van creditcards hebben inmiddels allerlei instrumenten ontwikkeld om fraude te detecteren en te voorkomen. Zo kunnen geavanceerde systemen bepaalde patronen van gebruik herkennen, zowel bij kaarthouder als bij merchants.

De te nemen maatregelen verschillen per betaalsysteem. We bespreken kort de twee belangrijkste systemen:

- Bij het pinsysteem (direct debit toonbankbetalingen en geldautomaten) is de beveiliging deels vormgegeven door eisen aan de betreffende apparatuur, zoals Interpay die heeft opgesteld. De behandeling van fraude en rechten en plichten van bank en rekeninghouder zijn geharmoniseerd vastgelegd in algemene bepalingen die zijn opgesteld in een proces van zelfregulering, met inspraak van consumentenorganisaties.
- Bij creditcard betalingen speelt fraude een grotere rol. Omdat creditcard maatschappijen betalingen toestaan zonder dat de kaart fysiek wordt getoond aan de merchant ('card not present' betalingen, zoals telefonische bestellingen én internetbetalingen) is er een groter risico. Een fraudeur kan zich relatief gemakkelijk voordoen als klant, de klant kan een gedane transactie proberen te ontkennen, en de merchant kan een transactie vervalsen. Door privaatrechtelijke overeenkomsten heeft de creditcard maatschappij de financiële risico's bij card-not-present fraude bij de merchant neergelegd. Naast een relatief hoge afdracht per transactie loopt deze ook de bewijslast en het risico bij een chargeback. Na een valste start de twee belangrijkste aanbieders van creditcards, Mastercard en Visa, een systeem voor internetbetalingen introduceren dat een hoger beveiligingsniveau kent.

Ook zijn er meer algemene maatregelen, die alle partijen nemen. Zo worden kaarten in toenemende mate voorzien van chips, die een betere controle en authenticatie mogelijk maken. Met name het klonen van kaarten wordt daarmee bemoeilijkt.

Uit de interviews komen nog andere maatregelen naar voren zoals:

- Alerts. Klanten krijgen een SMS-je bij grote transacties (bijvoorbeeld wanneer het salaris gestort wordt), maar ook bij transacties die "ongebruikelijk" zijn. Met software is het mogelijk betalingsgedrag bij te houden van individuen en wanneer er een afwijking is, kan iemand gewaarschuwd worden.
- Het gebruik van digitale technieken vergroot de traceerbaarheid van daders.
- Het eerder toegelichte fingerprinting principe is ook van toepassing op betalingstransacties. Wanneer er ten opzichte van het historische profiel duidelijke afwijkende betalingen (in omvang, bestemming, frequentie etc) verricht worden, worden deze als verdachte transacties aangemerkt. Deze methode kan dus niet alleen ingezet worden bij belfraude, maar ook bij betaalfraude.

Overigens blijft het veelal een kat en muis spel tussen fraudeurs en partijen uit de waardeketen. Nieuwe technieken worden snel bestudeerd door criminelen die eventueel

capabele cryptologen en technici inschakelen om beveiligde systemen te kraken. De hoge werkloosheid onder dergelijke specialisten in Oost-Europese landen is daarbij een serieus risico.

Het is als aanbieder soms ook lastig om aan te tonen dat een klant een kaart misbruikt heeft. Dan wordt men soms gedwongen gegevens prijs te geven voor een rechtbank die liever niet bekend worden gemaakt.

6.4 Observaties en constateringen uit de markt

Op basis van interviews en desk research is een aantal bevindingen gedaan betreffende betaaldiensten.

Bij de creditcard betalingen zijn er verschuivingen in verantwoordelijkheden waarneembaar. De retailer krijgt meer verantwoordelijkheid in het nagaan van de identiteit (betere check handtekening, navraag legitimatie, aanschaf duurdere terminals waarbij online verbindingen gelegd worden). Bovendien is de positie van de kaarthouder bij fraude met de creditcard waarbij de juiste pincode is gebruikt niet erg sterk.

Financiële partijen maken zich met name zorgen om de toenemende vaardigheden bij criminele organisaties. Scherpere regels betreffende ongebruikelijke transacties en witwassen vormen voor deze organisaties een uitdaging om op nieuwe manieren justitie en banken te slim af te zijn. De criminele wereld toont een duidelijke interesse in technische beveiligingen zoals chipontwikkelingen. Door het vergaren van geavanceerde kennis hopen ze op grotere schaal fraude te kunnen plegen. Een heel directe dreiging daarbij vormt het relatieve gemak waarmee criminele organisaties de benodigde kennis kunnen halen uit Oost-Europese landen, bijvoorbeeld bij voormalige veiligheidsmedewerkers of academici. Geïnterviewden geven bijvoorbeeld aan dat de criminele wereld toegang heeft tot zeer goed ingewijde cryptologen.

De ervaringen van banken met diensten als telebankieren heeft ze geleerd dat de PC een relatief onaantrekkelijke omgeving is voor veilige toepassingen. Juist door de openheid van het besturingssysteem en het intensieve gebruik voor andere toepassingen maakt het systeem kwetsbaar voor applicaties die een hoog niveau van veiligheid vereisen. Aanbieders zijn er in geslaagd het benodigde niveau te behalen, maar dat ging wel gepaard met de noodzaak van relatief onelegante oplossingen als de crypto calculator of lijsten met unieke codes die per post worden verstuurd. Dit is een belangrijke constatering met betrekking tot mobiel betalen (waarop we in het volgende hoofdstuk dieper ingaan), juist omdat mobiele telefoons steeds meer op kleine PC's gaan lijken.

Een andere constatering is dat de mens in toenemende mate de zwakke schakel vormt. De technieken waarvan fraudeurs zich bedienen zijn steeds geavanceerder. Het wordt voor de eindgebruiker steeds lastiger de benodigde zorgvuldigheid in acht te nemen: een slim geschreven malafide applicatie is zelfs door de meest ervaren gebruiker niet meer te herkennen als zodanig, en malafide applicaties weten de gebruikersinterface bonafide (betaal)diensten op een zo overtuigende wijze te imiteren dat het de gebruiker eigenlijk niet meer aan te rekenen valt dat deze zijn pincode heeft ingevoerd. Recente voorbeelden zijn de Phising-aanval op de Duitse Postbank[47] (zie voor dit fenomeen ook bijlage 3) en aanvallen waarbij fraudeurs een code uitgevoerd weten te krijgen op de computers van reguliere eBay-gebruikers.[48]

Locatiegebonden diensten lijken zich overigens in eerste instantie niet te lenen voor nieuwe vormen van criminaliteit. Het gaat vaak immers om diensten waar de klant zelf expliciet om vraagt. De verzameling en doorverkoop van klantgegevens aan derden kunnen leiden tot

[47] Zie *Grabber – Phising-Welle schockt Grossbanken* op www.domain-recht.de/magazin/article.php?id=324

[48] C'T, 'Uit vissen: Diefstal van wachtwoorden op internet wordt steeds geraffineerder', oktober 2004.

misbruik. Bijvoorbeeld informatie dat meneer X altijd in een bepaald gebied is en bepaalde informatie en diensten tot zich neemt. Dat betreft dus vooral een privacyvraagstuk.

6.5 Samenvatting en conclusies

In dit hoofdstuk is een overzicht van bestaande fraudevormen bij betaaltransacties gepresenteerd. Hoewel het ook hier een diverse lijst betreft, valt het op dat relatiefraude (dus fraude met gebruik van valse identiteit etc.) een nog prominentere rol speelt dan bij telecommunicatiefraude. De opgestelde lijst biedt een goede input voor te verwachten fraudevormen bij mobiel betalen, te behandelen in het volgende hoofdstuk.

Financiële organisaties besteden nog meer aandacht aan fraudebestrijding van telecommunicatiebedrijven. Dat wil echter niet zeggen dat fraude niet voorkomt. Vooral creditcard bedrijven, die in de (grensoverschrijdende) betalingen via internet een interessante markt hebben aangeboord, blijken veelvuldig gevallen van fraude tegen te komen. Ze hebben de financiële risico's daarbij overigens wel bij andere partijen neergelegd, zoals de merchants.

Andere bevindingen zijn:

1. Financiële partijen maken zich vooral zorgen om de toenemende vaardigheden bij criminele organisaties.
2. De ervaringen met diensten als telebankieren leren dat systemen met open besturingssystemen kwetsbaar zijn in het licht van veilige applicaties.
3. Met het geavanceerder worden van de techniek en van de methoden waarvan fraudeurs zich bedienen vormt de mens steeds vaker de zwakste schakel.

7 Verwachte vormen van fraude bij mobiel betalen

7.1 Inleiding

In de voorgaande twee hoofdstukken werden bestaande vormen van fraude bij respectievelijk telecommunicatiediensten en betaaldiensten besproken. In dit hoofdstuk wordt deze kennis vertaald naar toekomstbeelden voor fraude bij mobiele betaaldiensten.

Dit hoofdstuk beoogt wederom een antwoord te geven op de vierde, vijfde en achtste deelvraag bij dit onderzoek. Het hoofdstuk richt nu op *nieuwe* vormen van fraude:

4. Tot welke (nieuwe) vormen van nieuwe fraude zouden in de diverse scenario's de technologische ontwikkelingen kunnen leiden?
5. Hoe anticiperen de aanbieders van telecommunicatiediensten en van toegevoeg-dewaardediensten daarop?
8. In hoeverre bieden (parallelle) nieuwe technische ontwikkelingen ook *oplossingen* voor de bestrijding of preventie van de onderzochte vormen van fraude?

Paragraaf 7.2 presenteert een definitie van het begrip fraude. Paragraaf 7.3 bespreekt vervolgens de verschillende vormen van fraude die te verwachten zijn bij mobiel betalen en een bijbehorende indeling. In paragraaf 7.4 bespreken we ten slotte observaties en constateringen uit de markt op basis van de interviews en de expertsessie.

7.2 Definitie van fraude in de context van mobiel betalen

Zoals bij de eerder besproken fraude bij telecommunicatiediensten en bij betaaldiensten is het van belang om af te bakenen wat we in deze context onder fraude verstaan. Daarbij moeten we direct vaststellen dat de term 'fraude' geen juridisch begrip is. De wet- en regelgever heeft natuurlijk wel een aantal begrippen die omvatten wat we in de alledaagse taal met het woord fraude aanduiden. Juist omdat het hier een explorerend onderzoek betreft, willen we een brede definitie van fraude hanteren. We hanteren de volgende definitie:[49]

Fraude bij mobiele betalen betreft handelingen die
- een (persoonlijk) geldelijk gewin beogen,
- intentioneel worden uitgevoerd,
- een element van misleiding in zich hebben;
- gebruikmakend van een mobiel betaalsysteem.

In aanvulling op deze definitie:

- Kijken we naar de gehele transactie rondom het afnemen van een goed of dienst; de betalingstransactie vormt daar een onderdeel van; Onze aandacht gaat dus ook uit naar voorbereidingshandelingen (zoals het aanmelden voor een abonnement, wellicht onder een valse naam);

[49] Gegeven de vraagstelling bij deze studie kan het begrip fraude niet eenvoudigweg gedefinieerd worden als het handelen in strijd met relevante wet- en regelgeving; dat zou het opsporen van nieuwe vormen van fraude die nog niet door de wet worden afgedekt onmogelijk maken (deze zijn dan immers per definitie geen fraude).

- Verstaan we onder mobiel betalen elke betalingsdienst waarbij een mobiele telefoon en/of een mobiel telefonienetwerk wordt gebruik (zoals reeds in 2.5 is besproken);
- Verstaan we onder een mobiel betaalsysteem het technische én organisatorische systeem dat mobiele betaaldiensten mogelijk maakt;
- Rekenen we ook activiteiten als witwassen tot ons onderzoeksgebied (waarbij de misleiding zich niet richt tot de dienstenaanbieder maar tot andere zoals de Staat).

In de regel gaat het bij de door ons bedoelde vormen van fraude om handelingen die vallen onder de reikwijdte van de volgende juridische begrippen:

- Valsheidsdelicten;
- Vormen van bedrog (inclusief de specifieke bedrogsbepalingen met betrekking tot de telecommunicatiesector die opgenomen zijn in art. 326c Sr);
- Witwasdelicten.

Het element van misleiding houdt in wezen in dat gebruik wordt gemaakt van een dienst op een op een manier die anders is dan de aanbieders daarvan beogen. Het kan dan gaan om het uitbuiten van tekortkomingen, beperkingen of andere eigenschappen van het (betaal)systeem. Maar het kan ook gaan om 'slim' gebruik van bijvoorbeeld de tariefstructuur of andere organisatorische aspecten. Als oplichtingsmiddel noemt de wetgever ook 'listige kunstgrepen', en dit middel kan in deze context van belang zijn. Het betreft hier echter wel een wat grijs gebied: Wanneer is iets een listige kunstgreep? Wat is dan precies datgene wat de aanbieder beoogt? Als klanten inspelen op een mogelijkheid die de gekozen tariefstructuur van de aanbieder gewoon toelaat, is er dan wel sprake van een listige kunstgreep?

7.3 Mogelijke fraudevormen bij mobiel betalen

In hoofdstukken 5 en 6 is bij de bespreking van fraudevormen een grote diversiteit aan bod gekomen. Deze paragraaf start met de introductie van een model dat zich leent om bestaande èn nieuwe vormen van fraude onder te verdelen. We maken daarbij een onderverdeling naar:

1. Relatiefraude. Dit is fraude door moedwillig een valse identiteit te hanteren, zich voor iemand anders uit te geven of (intentioneel) afspraken of verplichtingen niet na te komen. Het richt zich dus op de relatie tussen partijen uit de betalingscirkel, inclusief de relatie tussen aanbieder en klant;
2. Technische fraude. Dit is fraude waarbij gebruik wordt gemaakt van technische onvolkomenheden in het systeem.

Verder maken we ook een onderverdeling naar:

1. Fraude door de (beoogde) eindgebruiker
2. Fraude door partijen in de waardeketen

Met deze twee onderverdelingen ontstaan er vier hoofdcategorieën fraude.

We willen er hier op wijzen dat bij de categorie fraude door de (beoogde) eindgebruiker het ook kan gaan om een (criminele) organisatie. Kenmerkend voor deze categorie is echter dat de manier waarop de fraude plaatsvindt door de eindgebruiker of iemand die zich als eindgebruiker voordoet. Ook is het van belang te onderkennen dat er soms overlap bestaat.

Sommige vormen van fraude combineren verschillende categorieën van fraude.[50] Ook is het onderscheid tussen relatiefraude en technische fraude niet altijd even scherp te trekken.

Ondanks deze beperkingen zijn we er echter van overtuigd dat de voorgestelde indeling in hoofdcategorieën een werkbare methode is om fraude te relateren aan juridische aspecten. Bijvoorbeeld: daar waar immers sprake is van eindgebruikers speelt consumentenrecht en –bescherming een rol. Bij fraude door partijen in de waardeketen staan dan weer privaatrechtelijke aspecten centraal.

Bij het opstellen van een lijst van voorbeelden hebben we ons laten inspireren door fraudevormen die nu spelen bij mobiele telefonie en fraudevormen die bekend zijn bij betaaldiensten (creditcard en banktransacties, al dan niet via internet).

Een aantal vormen van mobiel betalen is nu in gebruik. Het gaat dan om:

- Het aanroepen van koopnummers (ook bekend als betaalnummers, premium rate nummers, betaalde telefonische informatienummer of '0900- nummers');
- Het afnemen van betaalde diensten via platforms als i-Mode, Vodafone Live of T-Zones;
- Het gebruiken van reguliere betaaldiensten via de telefoon zoals het aanroepen van Girofoon;
- Het gebruik van internetbankieren via een mobiele (telefonie)verbinding.

Bovendien zijn we geïnspireerd door mogelijke vormen van fraude die bij deze methoden optreden.

Tijdens het onderzoek zijn 24 vormen van mogelijke fraude bij mobiel betalen geïdentificeerd. Deze vormen zijn in tabel 14 opgesomd, met gebruikmaking van de hierboven beschreven vier hoofdcategorieën. In Bijlage 3 wordt elk van de genoemde fraudevormen nader besproken.

[50] Ter illustratie: bij het ongeautoriseerd bellen vanaf kantoortelefoons naar een 0900-nummer van een malafide partij wordt eindgebruikerfraude en fraude door een partij in de waardeketen gecombineerd. Gezien het karakter van deze vorm brengen we deze onder bij fraude door een partij in de waardeketen.

Tabel 14: Inschatting relatief belang van fraude door experts

	Gepleegd door (beoogd) eind-gebruiker	*Gepleegd door partij in waardeketen*
Relatiefraude	*RE. Relatiefraude door eindgebruiker* • **Verloren/gestolen toestel/ongeautoriseerd gebruik** • Abonnementsfraude; frauduleuze aanmelding • Account take-over / identiteitsdiefstal	*RW. Relatiefraude door partij in waardeketen* • **Merchant bust-outs** • **Interne fraude** • **Witwassen (money-laundry)** • Homepage masking • Naamnummerkaping, naamnummerfraude • **Consumentenmisleiding** • Foute afrekeningen en salamifraude
Technische fraude	*TE. Technische fraude door eindgebruiker* • Teeing-in • Text messaging fraud • Mobile terminal cloning; vervalsing (counterfeit) • Gecompromitteerde account data • **Phishing** • **Malicious software ('Pacman-fraude', phone hacking, virusses, trojan horses)** • Remote phone hacking • Denial-of-Service (DoS) attacks • Sessieovername • Aanval op systeemelementen en netwerkinterne processen	*TW. Technische fraude door partij in waardeketen* • Fraude met inconsistente tariefstructuren • **Premium rate service fraud** • Achterdeuren (back-doors) • **Autodialers**

Vanzelfsprekend verschillen de diverse fraudevormen van belang. Tijdens de expertworkshop is gevraagd om het relatieve belang de verschillende vormen van (toekomstige) fraude te beoordelen. Dat belang is hier bedoeld in de zin van de mogelijke omvang van de fraude. Deze omvang is groot omdat ofwel de schade per geval omvangrijk is, ofwel omdat het aantal gevallen zeer groot is en tezamen tot een grote totaalomvang leiden. De acht fraudevormen waarvan het relatieve belang door de experts het hoogst werd ingeschat zijn in tabel 14 vetgedrukt weergegeven. Hoewel we deze resultaten moeten relatieveren (het betreft immers een *inschatting* bij een nog wat onzekere ontwikkeling door een kleine groep experts) valt wel op belangrijke vormen in elk van de vier hoofdcategorieën voorkomen.

Opmerkelijk is dat de fraudevorm die bij telecommunicatie met stip op nummer één stond, fraude door het gebruik van een valse identiteit, niet bovenaan deze lijst voorkomt. Dat is mogelijk zo omdat men deze bestaande vorm van fraude steeds beter onder controle krijgt (onder meer door verbeterde controle bij klantacceptatie). Nieuwere vormen van fraude, onder meer samenhangend met nieuwe technische ontwikkelingen, trekken meer de aandacht.

7.4 Observaties en constateringen uit de markt

Mobiel betalen – welke variant ook centraal staat – is een fenomeen dat in veel opzichten nog in de kinderschoenen staat. Dat maakt een betrouwbare inschatting van nieuwe vormen van fraude lastig. Het is immers nog niet bekend waar nieuwe kansen voor nieuwe fraude zich zullen voordoen. Het is daarom onmogelijk om nu alle risico's in te schatten. De markt voor mobiele betalingen worden door criminelen gezien als een zeer interessante markt om fraude in te plegen. In het verleden bleken zowel de (mobiele) telecommunicatiemarkt en de markt voor betalingsverkeer interessante slachtoffers. Beide markten bieden bijvoorbeeld interessante mogelijkheden tot het witwassen van geld. Uiteindelijk geldt ook hier: "the proof of the pudding is in the eating". Nieuwe vormen van fraude zullen wellicht pas bekend raken na echte uitrol van mobiel betalen.

In ieder geval zien marktpartijen de kans op nieuwe vormen van fraude - en de bestaande vormen van fraude die zich ongetwijfeld zullen vertalen naar varianten van mobiel betalen – niet als een reden om de ontwikkeling van mobiel betalen (en de marktintroductie) te stoppen. Er spelen wel risico's bij mobiel betalen, maar de huidige situatie levert voor marktpartijen geen waarneming op die zorgen baart, maar constante alertheid wordt uiteraard betracht.

Eén van de interviewrespondenten zegt dat omvang van nieuwe fraude niet anders zal zijn dan normaal. In vergelijking met de fysieke wereld is mobiel betalen zelfs misschien nog wel relatief veilig, want het is onmogelijk om via internet of mobiel betalen geld na te maken. Uiteraard doen zich in de virtuele wereld wel nieuwe vormen van criminaliteit voor. Denk aan hackers, bewuste softwarefouten, virussen en inbrekers op systemen (de virtuele pendanten van bankovervallen).

De geluiden van marktpartijen verschillen overigens wel. Banken zijn geneigd te melden dat zij minder last van fraude hebben. Telecommunicatieaanbieders ondervinden wel fraude, maar geven (uit bedrijfseconomische of strategische overwegingen) weinig inzicht in de feitelijke omvang. Zoals eerder is vastgesteld, is het soms ook erg lastig om te bepalen of er sprake is van fraude. Creditcardmaatschappijen hebben wel duidelijk last van fraude.

Uiteraard geeft de combinatie van betalingsverkeer en mobiele communicatie fraudevormen een nieuwe dimensie. Dat wordt versterkt met de mogelijke aansluiting naar andere sectoren die gevoelig zijn voor criminaliteit. Zo kan een mobiele kansspeldienst (inclusief een betalingscomponent) ingezet worden voor grootschalige witwasoperaties.

De bestaande fraude-detectiesystemen zijn tot op zekere hoogte bruikbaar in de nieuwe wereld. De huidige systemen van zowel telecommunicatie-exploitanten als van financiële partijen kunnen onder meer door geavanceerde patroonherkenning fraudes aan het licht brengen. Veel van de huidige technieken zijn ook bruikbaar in de nieuwe context van mobiel betalen. Er zullen naar verwachting echter ook vormen van fraude worden bedacht die niet goed door bestaande systemen kunnen worden opgespoord.

Men kan zich natuurlijk afvragen in hoeverre er sprake is van werkelijk *nieuwe* fraudevormen. De meeste geraadpleegde experts delen de mening dat het – voor zover nu te overzien – gaat om vormen van fraude die een equivalent kennen in andere markten. Ze krijgen echter wel een nieuwe vorm en dimensie, wat bijvoorbeeld kan betekenen dat ze in impact toenemen, eenvoudiger zijn uit te voeren en dat de dader minder gemakkelijk gevonden en aangepakt kan worden.

7.5 Samenvatting en conclusies

In dit hoofdstuk stonden twee onderzoeksvragen centraal: tot welke (nieuwe) vormen van nieuwe fraude zouden in de diverse scenario's de technologische ontwikkelingen kunnen leiden? En hoe anticiperen de aanbieders van telecommunicatiediensten en van toegevoegdewaardediensten daarop? In tegenstelling tot het vorige hoofdstuk draait het nu om nieuwe (of verwachte) vormen van fraude.

Allereerst is de definitie van fraude opnieuw aan bod gekomen, nu in het licht van mobiel betalen en in de context van het onderhavige onderzoek. (Eerdere hoofdstukken behandelde de definitie van fraude al specifiek voor telecommunicatiediensten.)

In de markt bestaan nog geen vast omlijnde beelden van mogelijke fraude met mobiel betalen. De meeste partijen verwachten dat veel bestaande vormen van fraude in een nieuw jasje terugkeren bij mobiel betalen. Ongetwijfeld geeft de combinatie van betalingsverkeer en telecommunicatie nieuwe kansen voor fraude, maar deze zijn niet volledig te voorspellen. Uiteindelijk zal fraude pas blijken bij daadwerkelijke start van mobiel betalen. Ook is het onduidelijk of fraude zal toenemen. Er zijn geluiden die dat tegenspreken. Bovendien is omvang bestaande fraude niet goed bekend (of wordt liever niet bekend gemaakt).

Wij hebben in dit hoofdstuk een model geïntroduceerd dat zich leent om bestaand en nieuwe vormen van fraude in te delen. Daarbij wordt een onderscheid gemaakt tussen:

1. Relatiefraude. Dit is fraude door moedwillig een valse identiteit te hanteren, zich voor iemand anders uit te geven of (intentioneel) afspraken of verplichtingen niet na te komen. Het richt zich dus op de relatie tussen partijen uit de betalingscirkel;
2. Technische fraude. Dit is fraude waarbij gebruik wordt gemaakt van technische onvolkomenheden in het systeem.

Voorts kan er een onderscheid worden gemaakt tussen:

1. Fraude door de (beoogde) eindgebruiker;
2. Fraude door partijen in de waardeketen.

Een combinatie van beide indelingen levert vier hoofdcategorieën op, namelijk relatiefraude door de eindgebruiker, relatie door partij in de waardeketen, technische fraude door de eindgebruiker en technische fraude door een partij in de waardeketen.

Andere constateringen in dit hoofdstuk zijn:

- Op basis van literatuuronderzoek, interviews en expertsessie worden er in dit rapport in totaal 24 vormen van fraude bij mobiel betalen geïdentificeerd. Deze vormen zijn verdeeld over de vier hoofdcategorieën. De gevonden vormen van fraude spelen een centrale rol bij de juridische analyse in de volgende hoofdstukken. Vanzelfsprekend is de lijst met fraudevormen niet uitputtend; in de toekomst kunnen ook nieuwe vormen van fraude opduiken. Met behulp van raadpleging van experts is een inschatting gemaakt welke vormen van fraude de grootste omvang hebben. Deze blijken zich in alle hoogcategorieën te bevinden.
- Mobiel betalen is een fenomeen dat in veel opzichten nog in de kinderschoenen staat, wat een betrouwbare inschatting van nieuwe vormen van fraude lastig maakt. Nieuwe vormen van fraude zullen wellicht pas bekend raken na echte uitrol van mobiel betalen. De inschattingen van marktpartijen betreffende fraude lopen erg uiteen.
- In ieder geval zien marktpartijen de kans op nieuwe vormen van fraude niet als een reden om de ontwikkeling van mobiel betalen (en de marktintroductie) te stoppen. Constante alertheid is echter wel van belang. De bestaande fraude-detectiesystemen zijn tot op zekere hoogte bruikbaar in de nieuwe wereld, maar echter zullen ook vormen van fraude ontstaan die niet goed door bestaande systemen kunnen worden opgespoord.
- Marktpartijen verwachten dat er slechts in beperkte mate sprake zal zijn van werkelijk nieuwe vormen van fraude. Het gaat om bestaande vormen, die echter wel een nieuwe vorm en dimensie krijgen, wat bijvoorbeeld kan betekenen dat ze in impact toenemen, eenvoudiger zijn uit te voeren en dat de dader minder gemakkelijk gevonden en aangepakt kan worden.

Deel III: Juridisch kader en instrumenten

8 Het juridische kader

8.1 Inleiding

In dit hoofdstuk wordt de wet- en regelgeving in kaart gebracht die van belang is voor (financiële) fraude via mobiele telecommunicatie. Daarmee wordt een begin gemaakt met de beantwoording van de zesde onderzoeksvraag die als volgt luidt: Is het bestaande wettelijke instrumentarium toereikend om deze (nieuwe) vormen van fraude adequaat te bestrijden? Achtereenvolgens worden de volgende rechtsgebieden behandeld: het strafrecht (paragraaf 8.2), het telecommunicatierecht (paragraaf 8.3), het financieel recht (paragraaf 8.4), het privacyrecht (paragraaf 8.5) en regels rond elektronische handel (paragraaf 8.6). In paragraaf 8.7 worden nog enkele algemene aspecten met betrekking tot de verschillende handhavingregimes behandeld. De laatste paragraaf is een conclusie.

8.2 Strafrecht

Voor financiële criminaliteit speelt de traditionele strafbaarstelling van valsheid in geschrift (art. 225 Sr) nog altijd een centrale rol. Deze bepaling kan toegepast worden op gegevens die op moderne (elektronische optische etc.) media zijn vastgelegd. De Hoge Raad heeft reeds in 1991 bepaald dat onder een geschrift mede verstaan kan worden een op een magneetschijf vastgelegd bestand. Ter onderbouwing van dit oordeel overwoog de Hoge Raad – in navolging van het Hof: 'dat het bestand bestond uit met enige duurzaamheid op een magneetschijf vastgelegde gegevens omtrent betalingsopdrachten welke op tamelijk eenvoudige wijze leesbaar konden worden gemaakt.'[51]

Om echter eventuele bewijsproblemen voor te zijn, heeft de wetgever bij de Wet Computercriminaliteit I een aparte strafbaarstelling over fraude met betaalpassen en waardekaarten in het Wetboek van Strafrecht opgenomen (art. 232 Sr).[52] Deze bepaling wordt gewijzigd bij Wetsvoorstel Computercriminaliteit II.[53] De parlementaire behandeling van dit wetsvoorstel ligt overigens de facto stil sinds 2000. De behandeling van dit wetsvoorstel wordt weer opgenomen bij de implementatie van het cybercrime verdrag in de Nederlandse wetgeving (zie hierna). In zijn huidige vorm heeft de bepaling betrekking op passen en kaarten waarmee betalingen verricht kunnen worden. Dit betekent dat de toepasbaarheid van de bepaling onzeker kan worden indien betwist wordt dat de prestatie die met behulp van de kaart of pas verkregen kan worden gekwalificeerd kan worden als een betaling. Om deze twijfel weg te nemen stelt de voorgestelde wetswijziging buiten kijf dat de bepaling ook van toepassing is als de kaart bedoeld is voor het verrichten of verkrijgen van andere prestaties dan betalingen. Tevens wordt de werking van de bepaling uitgebreid tot multi-purpose kaarten.[54] Bij wetsvoorstel 29025 wordt de strafbaarstelling van voorbereidingshandelingen met betrekking tot betaalpassen en waardekaarten (art. 232 lid 2 Sr) uitgebreid.[55]

---

[51] Zie HR 15 januari 1991 NJ 1991, 668, m.nt. Corstens.

[52] Wet Computercriminaliteit I, Stb. 1993, 33.

[53] Zie Kamerstukken II, 1998/99, 26671, nrs. 1-2.

[54] Zie Kamerstukken II, 1998/99, 26671, nr. 3, p. 46.

[55] Kamerstukken II, 2002/03, 29025, nrs. 1-2, Wijziging van het Wetboek van Strafrecht in verband met de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten (fraude niet-chartaal geldverkeer).

Naast de valsheidsdelicten, zijn ook vermogensdelicten zoals bedrog van belang voor het onderwerp van deze studie. In het bijzonder kan gewezen worden op art. 326c Sr dat specifiek toegerust is op bedrog in de telecommunicatie.

Voorts zijn strafbare feiten die typisch tot het domein van de computercriminaliteit behoren van belang. Hierbij is te denken aan strafbare feiten zoals computervredebreuk (art. 138a Sr), DoS-aanvallen (het in wetsvoorstel 26671 voorgestelde art. 138b Sr) en de opzettelijke/culpose vernieling van computergegevens (art. 350a/350b Sr).

Op 28 mei 2001 heeft de Raad van de Europese Unie een kaderbesluit genomen over de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten.[56] Het kaderbesluit verplicht de Lidstaten te voorzien in strafbepalingen met betrekking tot strafbare feiten in verband met materiële betaalinstrumenten[57] en (betaalinstrumenten die gebruik maken van) computers. Zo moeten lidstaten in de sfeer van computer gerelateerde betaalinstrumenten o.a. strafbaar stellen: het opzettelijk uitvoeren of veroorzaken van een overdracht van geld of monetaire waarde waardoor een derde op ongeoorloofde wijze in zijn eigendom wordt aangetast, met het oogmerk zichzelf of anderen een onrechtmatig economisch voordeel te verschaffen door: - het onrechtmatig invoeren, wijzigen, wissen of verwijderen van computergegevens, met name identificatiegegevens of - het onrechtmatig ingrijpen in de werking van een computerprogramma of –systeem (art. 3). Daarnaast moet voorzien worden in strafbaarstelling met betrekking tot werktuigen die bedoeld of bestemd zijn om eerdergenoemde strafbare feiten te plegen (art. 4). In september 2003 heeft de Minister van Justitie een wetsvoorstel aan de kamer aangeboden.[58] Dit voorstel past de Nederlandse wetgeving aan aan de eisen van het kaderbesluit. De aanpassingen die nog nodig zijn hebben vooral betrekking op voorbereidingshandelingen en strafbare feiten met betrekking tot eerdergenoemde werktuigen.

Op 23 november 2001 is in Boedapest het zogenaamde cybercrimeverdrag getekend.[59] De Minister van Justitie heeft 10 februari 2004 een concept wetsvoorstel gepubliceerd voor aanpassing van de Nederlandse wetgeving aan het verdrag.[60] De bepalingen over fraude en bedrog (inclusief de voorgestelde wijzigingen) voldoen reeds aan de verplichtingen die voor Nederland uit het Cybercrime verdrag voortvloeien.

8.3 Telecommunicatierecht

Het telecommunicatierecht omvat volgens het handboek van Dommering en anderen de volgende gebieden:

- De verdeling en toewijzing van schaarse hulpbronnen en de fysieke ruimte om telecommunicatie tot stand te brengen;

---

[56] 2001/413/JBZ: Kaderbesluit van de Raad van 28 mei 2001 betreffende de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten, Publicatieblad Nr. L 149 van 02/06/2001 blz. 0001 – 0004.

[57] In het kaderbesluit wordt onder een "betaalinstrument" verstaan, een materieel instrument, met uitzondering van wettige betaalmiddelen (zijnde bankbiljetten en munten) dat door zijn specifieke karakter, alleen of in combinatie met een ander (betaal)instrument, de houder of gebruiker in staat stelt geld of monetaire waarde over te dragen, zoals creditcards, eurochequekaarten, andere door financiële instellingen uitgegeven kaarten, reischeques, eurocheques, andere cheques en wissels, en dat is beschermd tegen namaak of bedrieglijk gebruik, bijvoorbeeld door ontwerp, code of handtekening.

[58] Kamerstukken II, 2002/03, 29025, nrs. 1-2, Wijziging van het Wetboek van Strafrecht in verband met de bestrijding van fraude en vervalsing in verband met andere betaalmiddelen dan contanten (fraude niet-chartaal geldverkeer).

[59] Verdrag inzake de bestrijding van strafbare feiten verbonden met elektronische netwerken,

Boedapest, 23 november 2001, Trb. 2002, 18.

- De toetreding tot de telecommunicatiemarkt;
- De ordening en correctie van het functioneren van de telecommunicatiemarkt;
- Het gebruik van de telecommunicatie-infrastructuur en -diensten.[61]

Voor het onderwerp van deze studie is met name het laatste aspect van belang. Zo regelt het telecommunicatierecht aspecten van de bescherming van eindgebruikersbelangen (art. 7 TW) en van de persoonlijke levenssfeer (art. 11 TW), bevoegd aftappen (art. 13 TW) en beveiligingsaspecten (art. 18.8 TW).

In het kader van de bescherming van eindgebruikersbelangen dient een aanbieder van een openbare elektronische communicatiedienst voor of bij het sluiten van een overeenkomst met een consument bepaalde gegevens aan hem te verstrekken (art. 7.1 TW). De gegevens betreffen onder andere zaken als de naam en het adres van de aanbieder, de geldende tariefstructuur en informatie over de duur, verlenging en beëindiging van de overeenkomst. Deze verplichting rust niet op de informatiediensten, i.e. waarbij met behulp van elektronische communicatienetwerken en -diensten overgebrachte inhoud wordt geleverd of redactioneel wordt gecontroleerd (art. 1 sub f TW).

8.4 Financieel recht

Het toezicht op kredietinstellingen is geregeld in de Wet Toezicht Kredietwezen 1992 (hierna: WTK 1992). Dit toezicht is opgedragen aan de De Nederlandsche Bank (hierna: DNB). De WTK 1992 richt zich met name op traditionele kredietinstellingen. Eind jaren negentig van de vorige eeuw, bestond onduidelijkheid over de toepasselijkheid van de WTK 1992 op het aanbieden van bancaire diensten via internet. Ter vermindering van de onduidelijkheid heeft de DNB in 1999 een beleidsregel gepubliceerd over de toepasselijkheid van de WTK 1992: Beleidsregel Media WTK 1992.[62] De DNB behandelt in dit beleidsdocument vooral de vraag of activiteiten 'op internet' in of vanuit Nederland plaatsvinden dan wel of zij op Nederland gericht zijn. Het antwoord op deze vraag is relevant voor toepasbaarheid van een aantal bepalingen in de WTK 1992.

In 2000, werd de e-geld richtlijn (2000/46/EG) van kracht.[63] Deze richtlijn is in het Nederlandse recht geïmplementeerd in de Wet Toezicht Kredietwezen 1992.[64] De aanpassingswet is op 1 juli 2002 in werking getreden.[65] Bovendien heeft DNB in juni 2002 de

---

[60] Zie http://www.justitie.nl/images/11_45832.pdf.

[61] E.J.Dommering, N.A.N.M. van Eijk, J.A.M. Nijhof en M.L. Verberne, *Handboek Telecommunicatierecht. Inleiding tot het recht en de techniek van de telecommunicatie*, Den haag: SDU 1999, p. 4.

[62] Beleidsregel Media WTK 1992, Nederlandse Staatscourant van 23 juli 1999 – nr 139,< http://www.dnb.nl/dnb/bin/doc/hbwtk3210_tcm7-16493.pdf >.

[63] Richtlijn 2000/46/EG van het Europees Parlement en de Raad van 18 september 2000 betreffende de toegang tot, de uitoefening van en het bedrijfseconomisch toezicht op de werkzaamheden van instellingen voor elektronisch geld, Publicatieblad Nr. L 275 van 27/10/2000 blz. 0039 – 0043.

[64] Wet van 20 juni 2002 tot wijziging van de Wet toezicht kredietwezen 1992 in verband met de invoering van bedrijfseconomisch toezicht op instellingen voor elektronisch geld, Stb. 2002, 330.

[65] Besluit van 25 juni 2002, houdende vaststelling van het tijdstip van inwerkingtreding van de wet.

tot wijziging van de Wet toezicht kredietwezen 1992 in verband met de invoering van bedrijfseconomisch toezicht op instellingen voor elektronisch geld (Stb. 2002, 330) en het besluit van 28 mei 2002 (Stb. 2002, 273), houdende aanwijzing van diensten in het kader van de Wet melding ongebruikelijke transacties en tot wijziging van het koninklijk besluit van 29 juli 1994, houdende aanwijzing van financiële instellingen en financiële diensten in het kader van de Wet identificatie bij financiële dienstverlening 1993, Stb. 2002, 336.

'regeling elektronisch geldinstellingen' gepubliceerd waarin richtlijnen en aanbevelingen voor het toezicht van de DNB op elektronisch geldinstellingen worden gegeven.[66]

In de richtlijn wordt elektronisch geld gedefinieerd als "elektronisch geld": een monetaire waarde vertegenwoordigd door een vordering op de uitgevende instelling, welke

i) is opgeslagen op een elektronische drager,

ii) is uitgegeven in ruil voor ontvangen geld dat ten minste dezelfde waarde vertegenwoordigt als de uitgegeven monetaire waarde,

iii) als betaalmiddel wordt aanvaard door andere ondernemingen dan de uitgever.

In april 2003 heeft DNB haar voorlopige standpunt gepubliceerd over de kwalificeerbaarheid van prepaid beltegoeden als elektronisch geld:

"De Nederlandsche Bank (de Bank) is vooralsnog van oordeel dat een beltegoed bij een mobiele operator, waarmee ook kan worden betaald voor PRS-diensten, niet is aan te merken als elektronisch geld in de zin van de Wtk 1992. Mobiele operators die prepaid mobiele telefonie aanbieden waarmee dergelijke PRS-diensten kunnen worden afgenomen, vallen uit dien hoofde niet onder de reikwijdte van de Wtk 1992."[67] Of dit standpunt houdbaar zal zijn, moet nog blijken.[68] [69]

De e-geld richtlijn introduceert de zogenaamde elektronisch geld instellingen (hierna: EGI's). Voor EGI's geldt een apart regime voor bedrijfseconomisch toezicht dat op een aantal punten afwijkt van het regime dat voor traditionele kredietinstellingen geldt.[70]

Tenslotte kan nog gewezen worden op Aanbeveling 97/489/EG.[71] Ter bescherming van consumenten, bevat de aanbeveling een aantal informatieplichten voor de uitgever van elektronische betaalinstrumenten (art. 3 & 4). Tevens regelt zij een aantal verplichtingen en aansprakelijkheden van de houder en de uitgever (art. 5 - 8) en bevat zij bepalingen over de regeling van geschillen (art. 9 & 10). De aanbeveling heeft zowel betrekking op betaalinstrumenten met toegang op afstand[72] als op elektronische geldinstrumenten.[73]

---

[66] Regeling elektronisch-geldinstellingen, Staatscourant 28 juni 2002, nr. 121, p. 31-38.

[67] Prepaid mobiele telefonie; reikwijdte Wet Toezicht Kredietwezen 1992, 15 april 2003, < http://www.11a2.nl/docs/dnb1504.doc >.

[68] Zie T. Schudelaro, Electronic Payment Systems and Money Laundering. Risks and Countermeasures in the Post-Internet Hype Era, Nijmegen: Wolf legal Publishers 2003, p. 211 – 224.

[69] Het standpunt is mede afhankelijk van de uitkomst van discussie op Europees niveau. De verwachting is dat het DNB standpunt niet houdbaar is. Toepassing van EGI richtlijnen op telecommunicatieaanbieders zal hen voor grote problemen plaatsen. Zo zullen zij met hun grote schulden niet kunnen voldoen aan eisen van solvabiliteit en liquiditeit die aan uitgifte van elektronisch geld worden gesteld. Tevens zullen vele andere regels van toepassing worden die telecommunicatieaanbieders het leven zuur maken (denk aan eisen van transparantie, streng prudentieel/accountantstoezicht, toepasselijkheid van de wet melding ongebruikelijk transacties etc.). De oplossingen waaraan wordt gedacht bij telecommunicatieaanbieders zijn lobbyen voor verlichting van het EGI regime en oprichting van aparte entiteiten waarin de prepaid tegoeden worden ondergebracht en die onder prudentieel toezicht komen. Banken willen geen oneerlijke concurrentie en verwachten dat uitgevers van elektronisch geld ook onder toezicht komen te staan en daarmee ook dezelfde investeringen, rapportages en solvabiliteitseisen vervullen. Zie ook paragraaf 9.2.

[70] Voor de traditionele kredietinstellingen, zie Richtlijn 2000/12/EG.

[71] 97/489/EG: Aanbeveling van de Commissie van 30 juli 1997 betreffende transacties die met een elektronisch betaalinstrument worden verricht, in het bijzonder inzake de betrekking tussen uitgever en houder, Publicatieblad Nr. L 208 van 02/08/1997 blz. 0052 – 0058.

[72] Een "betaalinstrument met toegang op afstand" is een instrument waarmee een houder toegang kan krijgen tot geldmiddelen die zich op diens rekening bij een instelling bevinden, waarbij een betaling aan een begunstigde wordt toegestaan en waarvoor gewoonlijk een persoonlijk identiteitsnummer (PIN-code) en/of een ander soortgelijk bewijs van identiteit benodigd is. Hieronder zijn met name betaalkaarten

8.5 Privacy

In deze paragraaf wordt eerst aandacht besteed aan de bescherming van persoonsgegevens. Vervolgens komt het 'telecommunicatiegeheim' aan de orde en tenslotte nog een enkel overgeschoten onderwerp.

8.5.1 Bescherming van persoonsgegevens

In 1995 heeft de Europese Commissie een richtlijn uitgevaardigd ter bescherming van persoonsgegevens (Richtlijn 95/46/EG). Deze richtlijn is in Nederland geïmplementeerd in de Wet bescherming Persoonsgegevens (hierna: WBP).[74]

Voor de telecommunicatiesector gelden echter aanvullende regels. Deze regels vloeien voort uit richtlijn 2002/58/EG.[75] Deze richtlijn is geïmplementeerd bij de 'Wet implementatie Europees regelgevingskader voor de elektronische communicatiesector 2002'[76], in werking getreden op 19 mei 2004.[77] Het College bescherming persoonsgegevens (hierna: CBP) heeft in november 2002 een advies uitgebracht over het concept voor deze wet.[78] De richtlijn geeft regels voor de vertrouwelijkheid van communicatie, over de omgang met verkeersgegevens en locatiegegevens, over de facturering[79], over de nummerweergave, over abonneelijsten, ongewenste communicatie en techniek en normalisatie.

De Raad van Europa heeft in het verleden twee Aanbevelingen gepubliceerd die voor deze studie van belang zijn: 1. Recommendation No.R(95) 4 on the protection of personal data in the area of telecommunication services, with particular reference to telephone services (7 February 1995) en 2. Recommendation No.R(90) 19 on the protection of personal data used for payment and other operations (13 September 1990).[80]

Tenslotte moet nog gewezen worden op een sectorregeling: de Gedragscode Verwerking Persoonsgegevens Financiële Instellingen van de Nederlandse Vereniging van Banken en het

---

(krediet-, debet-, uitgestelde debiterings- of bankkaarten) en toepassingen voor telefonisch en thuisbankieren begrepen.

[73] Een "elektronisch-geldinstrument" is een oplaadbaar betaalinstrument niet zijnde een betaalinstrument met toegang op afstand, bestaande in een kaart waarop waarde is opgeslagen of in een computergeheugen, waarop waarde-eenheden elektronisch worden opgeslagen hetgeen de houder ervan in staat stelt bepaalde transacties te verrichten, zoals het overmaken van gelden of het opnemen van contanten.

[74] Stb. 2000, 302.

[75] Richtlijn 2002/58/EG van het Europees Parlement en de Raad van 12 juli 2002 betreffende de verwerking van persoonsgegevens en de bescherming van de persoonlijke levenssfeer in de sector elektronische communicatie (richtlijn betreffende privacy en elektronische communicatie), Publicatieblad Nr. L 201 van 31/07/2002 blz. 0037 – 0047.

[76] Wet van 22 april 2004 tot wijziging van de Telecommunicatiewet en enkele andere wetten in verband met de implementatie van een nieuw Europees geharmoniseerd regelgevingskader voor elektronische communicatienetwerken en -diensten en de nieuwe dienstenrichtlijn van de Commissie van de Europese Gemeenschappen, Stb. 2004, 189.

[77] Besluit van 7 mei 2004, houdende vaststelling van het tijdstip van inwerkingtreding van de Wet implementatie Europees regelgevingskader voor de elektronische communicatiesector 2002, Stb. 2004, 207.

[78] CBP, Advies concept wetsvoorstel implementatie nieuwe richtlijnen telecommunicatiewet, < http://www.cbpweb.nl/ >.

[79] Zie ook CBP, Advies Besluit afscherming nummers notaspecificatie, < http://www.cbpweb.nl/>

[80] Zie http://www.coe.int/.

Verbond van Verzekeraars. Het CBP heeft deze gedragscode op 27 januari 2003 goedgekeurd.[81]

8.5.2 Het telecommunicatiegeheim

Het brief-, telefoon- en telegraafgeheim zijn in Nederland grondwettelijk verankerd (art. 13 GrW). De formulering in de grondwet is echter techniekafhankelijk, waardoor onduidelijkheid bestaat over het toepassingsbereik van de bepalingen en de wijdte van het telecommunicatiegeheim. Een eerder initiatief om art. 13 GrW bij de stand van de techniek te brengen is mislukt.[82] Daarop is een Commissie ingesteld (de Commissie Grondrechten in het digitale tijdperk) die een nieuwe techniekonafhankelijke formulering voorstelde. De regering heeft laten weten dat zij positief staat tegenover het advies van de commissie, maar zij heeft nog geen voorstel voor grondwetswijziging aan het parlement aangeboden.[83] Overigens kan men voor het telecommunicatiegeheim wel terugvallen op art. 8 EVRM: het EVRM erkent het recht op bescherming van correspondentie. Dit artikel is ook toepasbaar op nieuwe media.

Tegelijkertijd staat het telecommunicatiegeheim door allerlei feitelijk/technische en wettelijke ontwikkelingen onder druk. Bij feitelijk/technische ontwikkelingen is bijvoorbeeld te denken aan Echelon.[84] Voor wat betreft wettelijke ontwikkelingen kan gedacht worden aan de Wet Inlichtingen- en Veiligheidsdiensten. In deze wet zijn nieuwe bevoegdheden opgenomen die de grenzen van het telecommunicatiegeheim verkennen. Hierbij is met te denken aan de bevoegdheid tot searchen (art. 26 Wiv).[85] Bovengenoemde richtlijn 2002/58/EG geeft aan onder welke voorwaarden registratie van communicatie en verkeersgegevens mogelijk is.

8.5.3 Overige aspecten van privacy

Het CBP heeft advies uitgebracht over het conceptwetsvoorstel tot implementatie van het Cybercrime Verdrag: 'Het CBP is van mening dat het Cybercrime Verdrag in Nederland maatgevend dient te zijn voor het opsporen van criminaliteit waarbij elektronische netwerken (met inbegrip van private en openbare telecommunicatienetwerken) worden gebruikt, alsmede het vergaren van elektronisch bewijsmateriaal.'[86]

Uit de gesprekken met partijen in de waardeketen is gebleken dat er enige onduidelijkheid bestaat over privacywetgeving. Telecommunicatieaanbieders wijzen op het feit dat fraude in hun sector dusdanig is gestegen dat men bij het afsluiten van abonnementen een beroep doet op de BKR en dat er zelfs een apart bestand is aangelegd met wanbetalers in deze sector. Zwarte lijsten zijn dus wel degelijk mogelijk, maar er zijn meestal problemen over wie deze lijsten moet beheren (in verband met kosten, etc.).[87] Er zijn meer problemen in internationaal verband. Privacywetgeving legt beperkingen op aan het opzetten van internationale databases waarin fraudeurs (bijvoorbeeld oprichters van malafide ondernemingen) zijn opgenomen. Indien het gebruik van een internationale database vereist dat persoonsgegevens naar landen

---

[81] Zie http://www.cbpweb.nl/

[82] Voorstel: Kamerstukken II, 1996/97, 25443, nrs. 1-2. Intrekking: Kamerstukken I, 1998/99, 25443, nr. 40d.

[83] Kamerstukken II, 2000/01, 27460, nr. 1.

[84] Zie Kamerstukken II, 2000/01, 27591, nr. 1, Brief van de Minister van Defensie 'Grootschalig afluisteren van moderne telecommunicatiesystemen'. Zie ook de vervolgstukken in deze reeks (27591).

[85] Zie Kamerstukken II, 1997/98, 25877, nr. 3, p. 44 e.v.

[86] CBP, Advies conceptwetsvoorstel Aanpassing aan het Cybercrime Verdrag, < http://www.cbpweb.nl/ >.

[87] Op de website van CBP staan zelfs handleidingen voor het aanleggen van zwarte lijsten (en waar dan aan voldaan moet worden). Zie artikel 43 WBP. Vergelijk in dit verband ook het Werkdocument over zwarte lijsten van de Groep Gegevensbescherming Artikel 29, 11118/02/NL/def.WP 65, beschikbaar op: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp65_nl.pdf.

buiten de Europese Unie worden verstrekt, dient verzekerd te zijn dat dat land een adequaat niveau van bescherming van persoonsgegevens kent (art. 76 WBP). Een adequaat niveau van bescherming kan ook door middel van zelfregulering gerealiseerd worden. Bij doorgifte van persoonsgegevens naar de VS dient de betreffende vorm van zelfregulering te voldoen aan de zogenaamde Safe Harbour Principles.[88] De WBP kent daarnaast ook een aantal uitzonderingen op het beginsel dat persoonsgegevens alleen doorgegeven mogen worden naar landen met een adequaat beschermingsniveau. Zo noemt art.76 lid 1 WBP een aantal (categorieën) doorgiften die uitgezonderd is en schept art. 76 lid 2 WBP de mogelijkheid dat het College Bescherming Persoonsgegevens een vergunning verleent voor een doorgifte naar derde landen zonder adequaat beschermingsniveau. Een ander obstakel bij het aanleggen van databases met fraudeurs ligt in de discrepantie tussen het bedrijfje dat fraude pleegt en de personen (oprichters, bestuurders) achter deze bedrijfjes. Het is uiteraard interessanter de personen te registreren dan de bedrijfjes; laatstgenoemden hebben in het algemeen slechts een korte levensduur. Van eerstgenoemde personen staat vaak niet vast wat hun betrokkenheid (if any) is geweest bij de fraude, waardoor het moeilijk wordt te rechtvaardigen dat zij als fraudeurs geregistreerd mogen worden.

8.6 Elektronische handel

Rond de Millenniumwisseling zijn enkele Europese richtlijnen tot stand gekomen die het recht harmoniseren met betrekking tot het verrichten van rechtshandelingen via moderne communicatiemedia – m.n. internet. In het kader van deze studie zijn de volgende richtlijnen relevant: de richtlijn koop op afstand (97/7/EG), de richtlijn financiële diensten op afstand (2002/65/EG), de richtlijn elektronische handtekeningen (1999/93/EG) en de richtlijn inzake elektronische handel (2000/31/EG).

8.6.1 De richtlijn koop op afstand[89]

De richtlijn is geïmplementeerd in het Nederlandse recht.[90] De aanpassingswet is op 1 februari 2001 in werking getreden.[91] Centraal begrip in deze richtlijn is de overeenkomst op afstand. Daarmee wordt bedoeld elke overeenkomst tussen een leverancier en een consument inzake goederen of diensten die wordt gesloten in het kader van een door de leverancier georganiseerd systeem voor verkoop of dienstverlening op afstand waarbij, voor deze overeenkomst, uitsluitend gebruik gemaakt wordt van een of meer technieken voor communicatie op afstand tot en met de sluiting van de overeenkomst zelf. De richtlijn is echter niet van toepassing op overeenkomsten die worden gesloten met telecommunicatie-exploitanten door het gebruik van publieke telefoon (art. 3 Richtlijn 97/7/EG). Financiële diensten, waarop de richtlijn financiële diensten op afstand van toepassing is, zijn eveneens

---

[88] F.A.M. Van der KLaauw-Koops en J.E.J. Prins, Internationale privacyregulering: belangen, problemen en mogelijkheden, in: J.E.J. prins en J.M.A. Berkvens, *Privacyregulering in theorie en praktijk*, Deventer: Kluwer 2002, p. 497 – 501.

[89] Richtlijn 97/7/EG van het Europees Parlement en de Raad van 20 mei 1997 betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten, Publicatieblad Nr. L 144 van 04/06/1997 blz. 0019 – 0027.

[90] Wet van 21 december 2000 tot aanpassing van Boek 7 van het Burgerlijk Wetboek aan richtlijn nr. 97/7/EG van het Europees Parlement en de Raad van de Europese Unie van 20 mei 1997 betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten (PbEG L 144), Stb. 2000, 617.

[91] Besluit van 11 januari 2001 tot vaststelling van het tijdstip van inwerkingtreding van de Wet van 21 december 2000, houdende aanpassing van Boek 7 van het Burgerlijk Wetboek aan richtlijn nr. 97/7/EG van het Europees Parlement en de Raad van de Europese Unie van 20 mei 1997 betreffende de bescherming van de consument bij op afstand gesloten overeenkomsten (PbEG L 144) (Stb. 2000, 617), Stb. 2001, 24.

van de werking van de richtlijn uitgesloten (art. 3 Richtlijn 97/7/EG, zoals gewijzigd door Richtlijn 2002/65/EG).

Ter bescherming van consumenten legt de richtlijn (althans de aanpassingswet) een groot aantal informatieplichten op aan aanbieders van diensten op afstand (art. 4 & 5). De consument heeft het recht om een overeenkomst binnen een bepaalde termijn te herroepen (art. 6). De richtlijn geeft regels over de nakoming van de overeenkomst (art. 7). De consument moet voorts kunnen verzoeken om betalingen ongedaan te maken die als gevolg van frauduleus gebruik van een *betaalkaart* hebben plaatsgevonden. In geval van frauduleus gebruik van de betaalkaart moet de consument zijn 'geld' terugkrijgen (art. 8).

8.6.2 De richtlijn financiële diensten op afstand[92]

Ten tijde van het schrijven van deze studie had de Nederlandse regering nog geen wetsvoorstel ter implementatie van deze richtlijn aan het parlement aangeboden. De implementatietermijn is verstreken op 9 oktober 2004. De definitie van overeenkomsten op afstand is vrijwel gelijkluidend aan die gegeven in de richtlijn 97/7/EG, zij het dat zij slechts betrekking heeft financiële diensten. Onder financiële diensten wordt verstaan iedere dienst van bancaire aard of op het gebied van kredietverstrekking, verzekering, individuele pensioenen, beleggingen en betalingen. In geval van overeenkomsten betreffende financiële diensten die een initieel akkoord over diensten omvatten, gevolgd door opeenvolgende verrichtingen of een reeks in de tijd gespreide aparte verrichtingen van dezelfde aard, is de richtlijn alleen van toepassing op het initiële akkoord (art. 1 Richtlijn 2002/65/EG). Onder een "initieel akkoord over diensten" wordt bijvoorbeeld verstaan het openen van een bankrekening, het aanschaffen van een kredietkaart, of het afsluiten van een portefeuillebeheerscontract. Onder "verrichtingen" wordt bijvoorbeeld verstaan geld op een bankrekening deponeren of ervan opnemen, betalen met een kredietkaart, transacties verrichten in het kader van een portefeuillebeheerscontract. Het toevoegen van nieuwe elementen aan een initieel akkoord over diensten, zoals de mogelijkheid om een instrument voor elektronisch betalen te gebruiken in combinatie met een bestaande bankrekening, vormt geen "verrichting", maar een aanvullende overeenkomst, waarop deze richtlijn van toepassing is (overweging 17 Richtlijn 2002/65/EG).

De aanbieder van een financiële dienst is de persoon die de diensten op afstand verricht. De richtlijn dient echter ook van toepassing te zijn indien bij een of meer stadia van de verkoop een tussenpersoon betrokken is. Gelet op de aard en de mate van deze betrokkenheid, dienen de desbetreffende bepalingen van de richtlijn ook op een dergelijke tussenpersoon van toepassing te zijn, ongeacht diens juridische status (overweging 19 Richtlijn 2002/65/EG).

De richtlijn vestigt een groot aantal informatieplichten op aanbieders van financiële diensten op afstand (art. 3, 4 & 5). De consument kan een financiële overeenkomst op afstand binnen een bepaalde termijn herroepen (art. 6 & 7). De consument kan in geval van frauduleus gebruik van zijn *betaalkaart* in het kader van overeenkomsten op afstand om annulering van een betaling vragen en moet de ter betaling overgemaakte bedragen teruggestort of terugbetaald krijgen (art. 9).

[92] Richtlijn 2002/65/EG van het Europees Parlement en de Raad van 23 september 2002 betreffende de verkoop op afstand van financiële diensten aan consumenten en tot wijziging van de Richtlijnen 90/619/EEG, 97/7/EG en 98/27/EG van de Raad, Publicatieblad Nr. L 271 van 09/10/2002 blz. 0016 – 0024.

8.6.3 De richtlijn elektronische handtekeningen[93]

De richtlijn is inmiddels geïmplementeerd in het Nederlandse recht.[94] De aanpassingswet – de Wet elektronische handtekeningen - is op 21 mei 2003 in werking getreden. Onder elektronische handtekening wordt een handtekening verstaan die bestaat uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authenticatie (art. 3:15a lid 4 BW).[95] De wet regelt onder welk condities een elektronische handtekening juridisch gelijkgesteld kan worden met een handgeschreven handtekening. De wet kiest daarin – in navolging van de richtlijn – een tweesporen benadering. Een geavanceerde elektronische handtekening die is gebaseerd op een gekwalificeerd certificaat en die door een veilig middel is aangemaakt, wordt vermoed voldoende betrouwbaar te zijn om met een handgeschreven handtekening gelijk gesteld te worden (art. 3:15a lid 2 BW). In de praktijk betreft dit uitsluitend digitale handtekeningen. Voor andere elektronische handtekeningen, geldt dat het aan degene is die zich op de handtekening beroept om aan te tonen dat de gebruikte techniek voldoende betrouwbaar is als middel van authenticatie (art. 3:15a lid 1 BW). De wet geeft ook regels voor certificatiedienstverleners[96] en voor degenen die een veilig middel voor het aanmaken van elektronische handtekeningen op de markt brengen.[97]

8.6.4 De richtlijn inzake elektronische handel[98]

De richtlijn is inmiddels geïmplementeerd in het Nederlandse recht.[99] De aanpassingswet is op 30 juni 2004 in werking getreden.[100] De richtlijn is van toepassing op zogenaamde aanbieders van diensten van de informatiemaatschappij. Diensten van de informatiemaatschappij worden

---

[93] Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen, Publicatieblad Nr. L 013 van 19/01/2000 blz. 0012 – 0020.

[94] Wet van 8 mei 2003 tot aanpassing van Boek 3 en Boek 6 van het Burgerlijk Wetboek, de Telecommunicatiewet en de Wet op de economische delicten inzake elektronische handtekeningen ter uitvoering van richtlijn nr. 1999/93/EG van het Europees Parlement en de Raad van de Europese Unie van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG L 13) (Wet elektronische handtekeningen), Stb. 2003, 199.

[95] De wet gebruikt de term 'authentificatie'. In deze studie wordt de meer gangbare term 'authenticatie' gebruikt. Er is geen verschil in betekenis bedoeld.

[96] Zie o.a. art. 6:196b BW (aansprakelijkheid), art. 2.1 & 2.2. TW (registratie), art. 11.5a TW (informationele privacy) en art. 18.15 & 18.16 TW (kwaliteitseisen en toetsing).

[97] Zie o.a. art. 18.17 TW (kwaliteitseisen en conformiteit).

[98] Richtlijn 2000/31/EG van het Europees Parlement en de Raad van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt ("Richtlijn inzake elektronische handel"), Publicatieblad Nr. L 178 van 17/07/2000 blz. 0001 – 0016.

[99] Wet van 13 mei 2004 tot aanpassing van het Burgerlijk Wetboek, het Wetboek van Burgerlijke Rechtsvordering, het Wetboek van Strafrecht en de Wet op de economische delicten ter uitvoering van richtlijn nr. 2000/31/EG van het Europees Parlement en de Raad van de Europese Unie van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (PbEG L 178) (Aanpassingswet richtlijn inzake elektronische handel), Stb. 2004, 210.

[100] Besluit van 18 juni 2004, houdende vaststelling tijdstip van inwerkingtreding van de wet van 13 mei 2004 tot aanpassing van het Burgerlijk Wetboek, het Wetboek van Burgerlijke Rechtsvordering, het Wetboek van Strafrecht en de Wet op de economische delicten ter uitvoering van richtlijn nr. 2000/31/EG van het Europees Parlement en de Raad van de Europese Unie van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel, in de interne markt (PbEG L 178) (Aanpassingswet richtlijn inzake elektronische handel) (Stb. 210), Stb. 2004, 285.

gedefinieerd als iedere dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van een afnemer van diensten wordt verricht. Onder diensten van de informatiemaatschappij worden mede verstaan diensten voor het doorgeven van informatie via een communicatienetwerk, voor het verschaffen van toegang tot een communicatienetwerk of het toegankelijk maken van informatie die verstrekt is door een afnemer van een dienst (overweging 18 Richtlijn 2000/31/EG). De richtlijn heeft ook betrekking op de online levering van financiële diensten (overweging 27 Richtlijn 2000/31/EG).

De richtlijn behandelt een groot aantal uiteenlopende zaken. In het kader van deze studie zijn met name de bepalingen over het contracteren langs elektronische weg van belang (art. 6 :227a BW). Indien uit de wet voortvloeit dat een overeenkomst slechts in schriftelijke vorm geldig of onaantastbaar tot stand komt, is aan deze eis tevens voldaan indien de overeenkomst langs elektronische weg is totstandgekomen en

a. raadpleegbaar door partijen is;

b. de authenticiteit van de overeenkomst in voldoende mate gewaarborgd is;

c. het moment van totstandkoming van de overeenkomst met voldoende zekerheid kan worden vastgesteld; en

d. de identiteit van de partijen met voldoende zekerheid kan worden vastgesteld.

Behalve de gelijkstelling van geschriften en elektronische equivalenten, vestigt de richtlijn ook een aantal informatieplichten, regelt zij de aansprakelijkheid van tussenpersonen, vestigt zij het 'land-van-oorsprong' beginsel en raakt zij kort aan geschiloplossing.

8.7 Handhaving

De voorgaande paragrafen richten zich voornamelijk op de materiële normstellingen met betrekking tot fraude met mobiele betaalsystemen. Het gaat om vragen als welke gedragingen zijn strafbaar, wat zijn de rechten en plichten van consumenten en partijen uit de waardeketen, en wat is de status van partijen uit de waardeketen. Kenmerk van deze regels is dat zij wel aangeven hoe de normadressanten zich behoren te gedragen en ook welke consequenties rechtens aan bepaalde (non-conforme) gedragingen verbonden behoren te zijn. Wat zij echter niet regelen is hoe de consequenties geëffectueerd dienen te worden. Vele consequenties treden immers niet automatisch in, maar behoeven nadere actie van overheidsinstanties of betrokken partijen. We spreken in dit verband van handhaving van het recht. Het recht voorziet in een drietal basisvormen van handhaving: strafrechtelijke handhaving, bestuursrechtelijke handhaving en civielrechtelijke handhaving. De drie onderscheiden vormen worden hier kort besproken.

Strafrechtelijke handhaving is punitief van karakter. Bij strafrechtelijke handhaving ligt het initiatief bij het Openbaar Ministerie (hierna: OM). Een Officier van Justitie beslist op gronden aan het algemeen belang ontleend of hij tot vervolging van een (fraude)verdachte overgaat. De vervolgingsbeslissing heeft zowel een beleidsmatige kant als een juridisch technische. Het OM stippelt een eigen vervolgingsbeleid uit. Daarbij kan het OM onder andere aangeven welke feiten in het bijzonder aandacht zullen krijgen, onder welke voorwaarden een transactie wordt aangeboden of welke strafeis gevorderd zal worden.[101] Bij een concrete beslissing om tot vervolging over te gaan spelen behalve beleidsmatige overwegingen ook juridisch technische kwesties een rol zoals de bewijsbaarheid van het feit. Bij fraude met mobiele betaalsystemen

[101] Voor het vervolgingsbeleid ten aanzien van Valsheid in geschrift met betrekking tot bankcheques en/of girobetaalkaarten, zie http://www.om.nl/?p=pg&s=414.

kunnen in het bijzonder bewijsproblemen voortvloeien uit het feit dat de fraude met tussenkomst van apparatuur plaatsvindt en het vaak moeilijk is om aan te tonen wie die apparatuur ten tijde van het plegen van het feit bediende. Om de beslissing over de vervolging goed te kunnen nemen en een eventuele strafvervolging met succes te kunnen afronden is onderzoek nodig. Te dien einde is voorzien in een ruim arsenaal aan wettelijke bevoegdheden die bij de opsporing en het onderzoek van feiten aangewend kunnen worden. In het verband van deze studie kan bijvoorbeeld gewezen worden aan bevoegdheden om verkeersgegevens op te vragen bij telecommunicatieaanbieders, de bevoegdheid om telefoons af te luisteren, om huiszoeking te doen etc. Voor het onderzoek van sommige vormen van criminaliteit is hoog specialistische kennis vereist. Dat is onder andere het geval met telecommunicatiefraude. Om deze reden is in 1998 het Landelijk Expertisecentrum Telecommunicatiefraude opgezet. In het algemeen geraakt de politie of een Officier van Justitie op de hoogte van fraude door middel van een aangifte. Een bottleneck hierbij is dat bedrijven enigszins terughoudend zijn in het doen van aangifte van fraude waarvan zij slachtoffer zijn geworden. De mogelijke reputatieschade die ontstaat door het enkele feit dat bekend wordt dat het bedrijf slachtoffer is geworden van fraude weegt kennelijk zwaarder dan het vrijuitgaan van de dader.

Bestuursrechtelijke handhaving richt zich vooral op toezicht op de naleving van wet- en regelgeving. De overheid kan onder andere door het weigeren van vergunningen of het stellen van voorwaarden aan vergunningen invloed uitoefenen op de activiteiten die aan haar bestuur zijn onderworpen. Ter handhaving van door haar gestelde regels kan de overheid zich bedienen van bestuursdwang of boetes opleggen. Bij bestuursdwang wordt met behulp van de sterke arm een onrechtmatige feitelijke situatie beëindigd. In de context van dit onderzoek zijn vooral de toezichthouders de OPTA en de DNB van belang. De OPTA houdt toezicht op de markten voor elektronische communicatiediensten en post.[102] De DNB houdt prudentieel toezicht op kredietinstellingen en elektronisch geldinstellingen.

Bij civielrechtelijke handhaving ligt de handhaving in handen van burgers. De benadeelde partij dagvaardt de veroorzaker van het kwaad waaronder hij lijdt voor de burgerlijke rechter. Bij toewijzing van de eis kan de burgerlijke rechter de gedaagde veroordelen tot het betalen van een schadevergoeding, tot alsnog nakoming (van een overeenkomst), tot een gebod of verbod, etc. Zo heeft degene die het slachtoffer is geworden van fraude een vordering op de fraudeur, die hij via de burgerlijke rechter geldend kan maken (verondersteld dat de fraudeur gevonden kan worden en verhaal biedt).

8.8 Conclusie

Dit hoofdstuk beoogt voorwerk te verrichten voor de beantwoording van de juridische onderzoeksvragen in het volgende hoofdstuk. Dit hoofdsstuk brengt het recht in beeld dat van toepassing is op feiten die als fraude met mobiel betalen kunnen worden opgevat. Behalve het strafrecht , zijn hier eveneens van belang het financieel recht, het telecommunicatierecht, het privacyrecht en het recht rond elektronische handel. Het is gebleken dat het niet steeds eenvoudig uit te maken welke set van soms conflicterende regels van toepassing is op een specifiek feitencomplex.

[102] Zie http://www.opta.nl/

9 Inventarisatie van juridische knelpunten en de doeltreffendheid van het juridische instrumentarium

9.1 Inleiding

In dit hoofdstuk worden de juridische knelpunten die zich bij mobiel betalen kunnen voordoen geïnventariseerd en waar nodig aangegeven of wijziging van regelgeving is geïndiceerd zodat doeltreffendheid van fraudebestrijding kan worden vergroot. In het vorige hoofdstuk is enig voorwerk verricht voor onderzoeksvraag zes: Is het bestaande wettelijke instrumentarium toereikend om deze (nieuwe) vormen van fraude adequaat te bestrijden? Daartoe is in het vorige hoofdstuk in den brede geïnventariseerd welke regelingen van belang zijn voor fraude met mobiel betalen. In dit hoofdstuk gaan we in op de logische (en zevende) onderzoeksvraag: Zo niet, op welke terreinen bestaan lacunes? Hoe kunnen deze lacunes gedicht worden? Hierbij is er niet voor gekozen alle regelingen die in het vorige hoofdstuk aangestipt zijn uit te diepen, maar om vooral in te zoomen op die problemen die tijdens interviews en de expertsessie naar voren zijn gekomen. Daarom is vooral de veronderstelling getoetst dat de voorziene delicten al strafbaar zijn op basis van bestaande strafbepalingen en belicht op welke wijze zelfregulering een aanvullende rol kan spelen.

9.2 De strafbaarstellingen van fraude

In deze paragraaf wordt onderzocht of de onderscheiden fraudevormen gedekt worden door bestaande strafbaarstellingen en welke tekortkomingen daarbij aan het licht komen.

9.2.1 Bedrogbepalingen

Een groot aantal van de onderscheiden fraudevormen kwalificeren strafrechtelijk als bedrog. De relevant strafbaarstellingen zijn te vinden in art. 326 Sr (oplichting) en art. 326c Sr (misbruik van telecommunicatie).

> Art. 326 Sr
>
> 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 drie jaren of geldboete van de vijfde categorie.

> Art 326c.
>
> 1. Hij die, met het oogmerk daarvoor niet volledig te betalen, door een technische ingreep of met behulp van valse signalen, gebruik maakt van een dienst die via telecommunicatie aan het publiek wordt aangeboden, wordt gestraft met gevangenisstraf van ten hoogste drie jaren of geldboete van de vijfde categorie.
>
> 2. Met gevangenisstraf van een jaar of geldboete van de derde categorie wordt gestraft hij die opzettelijk een voorwerp dat kennelijk is bestemd, of gegevens die kennelijk zijn bestemd, tot het plegen van het misdrijf, bedoeld in het eerste lid,

a. openlijk ter verspreiding aanbiedt;

b. ter verspreiding of met het oog op de invoer in Nederland voorhanden heeft of

c. uit winstbejag vervaardigt of bewaart.

3. Hij die van het plegen van misdrijven als bedoeld in het tweede lid, zijn beroep maakt of het plegen van deze misdrijven als bedrijf uitoefent wordt gestraft hetzij met gevangenisstraf van ten hoogste drie jaren en geldboete van de vijfde categorie, hetzij met één van deze straffen.

Hierna worden de verschillende in hoofdstuk 5 onderscheiden fraude vormen doorlopen met het oog op strafbaarheid. De nadruk zal daarbij liggen op bedrog en gedragingen die als voorbereiding op bedrog gezien kunnen worden.

9.2.2 Abonnementsfraude

Het afsluiten van een abonnement of het openen van een (krediet-)rekening onder andermans naam en het afnemen van diensten voor rekening van die ander levert bedrog, aangenomen dat de ander daarmee niet heeft ingestemd. Het enkele aanmelden onder een valse naam zonder dat het abonnement of de rekening is gebruikt levert echter geen bedrog op. Op de vraag of het aanmelden onder een valse naam niettemin strafwaardig is, wordt hieronder in paragraaf 9.1.17 nader ingegaan.

9.2.3 Identiteitsdiefstal en account take-over

Identiteitsdiefstal is in wezen een voorportaal voor fraudevormen zoals abonnementsfraude. Het enkele verzamelen van gegevens over een persoon is niet strafbaar. Wel is vereist dat voorgenomen verwerkingen van persoonsgegevens worden gemeld bij het College bescherming persoonsgegevens (art. 27 en 28 WBP), voor zover zij niet onder een categorale vrijstelling vallen (art. 29 WBP). Het verzamelen van persoonsgegevens is een verwerking en behoort dus in beginsel gemeld te worden. Het achterwege laten van een melding dan wel het onjuist melden van verwerkingen van persoonsgegevens is strafbaar (art. 75 WBP). Zodra de ‘gestolen’ identiteit gebruikt wordt om betalingen te verrichten (account take-over) betreden we weer het terrein van bedrog.

9.2.4 Merchant bust-out

Ondernemingen die handelen met het vooropgezette doel gelden te innen van afnemers en met de noorderzon te vertrekken zodra de afnemers aanspraak beginnen te maken op hun tegenprestaties plegen uiteraard bedrog. Mogelijkerwijze is het bewijs van het opzet om te bedriegen niet eenvoudig te leveren. Indien de personen achter deze ondernemingen deze handelwijze vaker hanteren, kan wellicht een patroon aangetoond worden. Uit het patroon kan dan opzet afgeleid worden. Dit vergt echter het een en ander van het Openbaar Ministerie.

9.2.5 Interne fraude

Dit is een verzamelbegrip voor vormen van fraude waarbij medewerkers van een geldinstelling of een telco betrokken zijn. Onder welke delictsomschrijvingen de betrokken gedragingen te brengen zijn hangt af van de specifieke modus operandi.

9.2.6 Teeing in

Teeing-in is een specifieke werkwijze om identiteits- en authenticatiegegevens van een ander te weten te komen. Het verzamelen van de gegevens kan strafbaar zijn door de wijze waarop dit gebeurt. Dit is bijvoorbeeld het geval indien daartoe een vertrouwelijke

gegevensoverdracht wordt afgetapt of opgenomen (artt. 139a – 139c Sr) of indien daartoe in een computersysteem wordt ingebroken (art. 138a Sr). Indien de gegevens gebruikt worden om transacties voor rekening van een ander genereren, is dan sprake van bedrog.

9.2.7 Text messaging fraud

Text mesaging fraud levert bedrog op. Het kan eveneens afgedaan worden onder art. 326c Sr.

9.2.8 Gecompromitteerde account data

Gecompromitteerde accountdata betreft in wezen het geval dat account data zoals die aanwezig zijn bij een partij uit de waardeketen terecht zijn gekomen bij anderen die daartoe geen toegang hadden mogen krijgen. Hierbij kan zowel sprake zijn van strafbare feiten gepleegd door degenen bij wie de gegevens terecht zijn gekomen als van strafbare feiten door partijen uit de waardeketen dan wel hun personeel. Degenen die de beschikking hebben gekregen over de account data hebben daarvoor wellicht strafbare feiten moeten plegen, zoals hacking (art. 138a Sr), aftappen of opnemen van 'vertrouwelijke' gegevensoverdrachten (artt. 139a – 139c Sr), het omkopen van personeel (art. 328ter lid 2 Sr) of het helen van gegevens (art. 273 Sr). Personeel van telco's of krediet- of geldinstellingen heeft zich in verband met het uitlekken van de account data wellicht schuldig gemaakt aan het bekend maken van bedrijfsgeheimen (art. 273 Sr) of omkoping (art. 328ter lid 1 Sr). De telco zelf heeft wellicht haar beveiligingsplicht met betrekking tot account gegevens verzaakt (vgl. art.18.8 TW, geen strafbaarstelling). Ook andere partijen in de waardeketen die geen telco zijn dienen de persoonsgegevens van hun accounthouders te beveiligen (art. 13 en 14 WBP, geen strafbaarstelling).

9.2.9 Phishing

Phishing is het onder valse voorwendselen ontfutselen van authenticatiegegevens aan de houder van deze gegevens. Kan Phishing als bedrog in de zin van art. 326 Sr gekwalificeerd worden? Blijkens de delictsomschrijving kan de prestatie waartoe de bedrieger zijn slachtoffer probeert te bewegen ook bestaan in het ter beschikking stellen van gegevens met geldswaarde in het handelsverkeer. Zijn authenticatiegegevens zulke gegevens? Het beschikbaar stellen van gegevens met geldswaarde in het handelsverkeer is in 1993 bij de Wet Computercriminaliteit opgenomen in art. 326 Sr. Destijds heeft de regering aangegeven dat '[i]n concrete gevallen zal moeten worden nagegaan of in de maatschappelijke werkelijkheid de betreffende gegevens reguliere handelswaar vertegenwoordigen.'[103] De GPV-fractie in de Tweede Kamer had de regering gevraagd de strekking van de betreffende gegevens te verruimen. Zij noemde in concreto dat zonder verruiming het afstaan van privacygevoelige gegevens niet door de bepalingen (over bedrog en afpersing) gedekt zou zijn. De regering vond echter dat het bereik van strafbepaling daarmee te ruim zou worden.[104] Als argument hanteerde de regering daarbij dat het vermogensdelicten betreft en een uitbreiding tot andere gegevens dan die geldswaarde in het handelsverkeer vertegenwoordigen niet zou passen bij de aard van de delicten. In de Nota naar aanleiding van het Eindverslag heeft de regering bovendien nog aangegeven dat gegevens die op onrechtmatige wijze worden verstrekt en geld opleveren, bijvoorbeeld het illegaal verstrekken van bedrijfsgegevens eveneens van de bepaling zijn uitgesloten.[105] Gezien het feit dat de handel in authenticatiegegevens hooguit op een zwarte markt plaatsvindt en het geen reguliere handelswaar betreft, is het zeer twijfelachtig of phishing strafbaar is als bedrog in de zin van art. 326 Sr. Niettemin lijkt ons

[103] Kamerstukken II 1989/90, 21551, nr. 3, p. 8.

[104] Kamerstukken II 1990/91, 21551, nr. 6, p. 18-20.

[105] Kamerstukken II 1991/92, 21551, nr. 11, p. 12.

dat phishing als een belangrijke voorbereidingshandeling op met name vermogensdelicten wel degelijk strafbaar zou moeten zijn.

9.2.10 Malicious software

De categorie van de malicious software betreft in wezen vormen van gegevensmanipulatie. Wordt malicious software gedekt wordt door de strafbaarstelling over virussen (art.350a lid 3 Sr)? De huidige bepaling wordt gewijzigd bij de voorgestelde wet computercriminaliteit II. Na de voorgestelde wijziging komt het betreffende artikellid als volgt te luiden:

Hij die opzettelijk en wederrechtelijk gegevens ter beschikking stelt of verspreidt die zijn bestemd om schade aan te richten in een geautomatiseerd werk, wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie.

In wezen zou men het onbevoegd veranderen van de functionaliteit van bestaande in de computer aanwezige programma's inderdaad kunnen karakteriseren als een vorm van schade aanrichten in een geautomatiseerd werk. De schade bestaat immers daarin dat de computer zonder nadere maatregelen niet meer gebruikt kan worden door de rechtmatige gebruiker. Zodra deze de computer aanzet, loopt hij immers het risico dat de computer ten behoeve van de derde gegevens lekt, transacties aangaat etc. Onduidelijk is nog in hoeverre de volgende tegenargumentatie hout snijdt. Het toevoegen van nieuwe functionaliteiten aan de computer zonder aantasting van de oude is niet een vorm van 'schade aanrichten'. De computer is immers nog volledig functioneel voor de rechtmatige gebruiker. Onzes inziens zou een dergelijke redenering verworpen moeten worden. De functionaliteit van een computer is meer dan een optelsom van de individuele functionaliteiten, maar omvat ook elementen als een bepaalde zekerheid dat een computer geen onverwachte extra functionaliteiten ten toon zal spreiden. Of de rechter deze redenering zal volgen, moet afgewacht worden.

Daarnaast zou men nog kunnen betogen dat een vervolging op basis van deze bepaling niet helemaal bevredigend is. De kern van het delict dat wij met malicious software aanduiden is immers dat de dader via de gemanipuleerde computer transacties aangaat met derden ten koste van de rechtmatige gebruiker van de computer en de daarop aanwezige programma's en gegevens. Het is veeleer een vermogensdelict dan een delict dat de CIA-belangen aantast.[106] Dat is echter op zich geen argument om te stellen dat de huidige wetgeving te kort schiet. Vermogensdelicten die met behulp van malicious software worden gepleegd kunnen meestal al op basis van de bedrogbepaling van art. 326 Sr vervolgd worden.

9.2.11 Remote phone hacking

Remote phone hacking kan aangepakt worden op basis van de bepalingen over computervredebreuk (art. 138a Sr). Deze bepaling vereist weliswaar enige beveiliging, maar aangenomen kan worden dat telefoons doorgaans van een meer dan symbolische beveiliging zijn voorzien. Indien na het binnendringen in de telefoon gegevens worden gewist, gewijzigd, of toegevoegd kan men ook nog bij art. 350a Sr (opzettelijke gegevensvernieling) terecht. Het tweede lid van art. 350a Sr stelt als gekwalificeerde vorm van gegevensvernieling strafbaar, de gegevensvernieling die plaatsvindt nadat via hacking toegang is verkregen tot het betreffende computersysteem.

9.2.12 Inconsistente tariefstructuur

Er zijn enkele vormen van asociaal gedrag die wellicht niet door de bedrogbepalingen worden gedekt. Een voorbeeld vormt de inconsistente tariefstructuur. Soms zijn tariefstructuren op een merkwaardige manier opgezet. Zo kan het gebeuren dat een carrier voor PRS-diensten

[106] CIA staat voor Confidentiality, Integrity and Availability.

meer moet afdragen aan de aanbieder van die dienst dan hijzelf ontvangt van degene die de dienst afneemt. Dat kan bijvoorbeeld het geval zijn bij oproepen die maar heel korte tijd – bijvoorbeeld slechts een seconde - duren. De aanbieder van de PRS-dienst kan hiervan misbruik maken door op grote schaal zijn eigen dienst te bellen. Het is kwestieus of dit bedrog oplevert. Het is immers maar de vraag of hier sprake is van misleiding van de carrier. Dit gedrag is uiteraard asociaal. Onzes inziens is er echter geen noodzaak om strafrechtelijk in te grijpen. De carrier kan dit probleem gemakkelijk ondervangen door zelf verantwoordelijkheid te nemen voor een consistente tariefstructuur.

9.2.13 Premium Rate Service Fraud

De inkomsten van PRS diensten zijn groot. Dienovereenkomstig is ook de verleiding groot gebleken om mensen via enige vorm van misleiding PRS diensten te doen afnemen. Te denken valt bijvoorbeeld aan vormen van routing en ghost dialers. Desgevallend valt het betreffende gedrag als bedrog te kwalificeren. Er zijn echter gevallen waarin er geen bedrog is of de intentie om te bedriegen niet aan te tonen is. Een goed voorbeeld is het gebruik van autodiallers waarbij in een popup scherm wordt aangekondigd dat de verbinding verbroken wordt en een nieuwe, dure 0900-verbinding wordt opgezet, zodra de websurfer op de OK-button heeft geklikt. De eigenaar van de website die de autodialer bevat kan er honorabele redenen voor hebben om een nieuwe verbinding op te zetten. Het kan echter ook zijn dat de eigenaar erop gokt dat veel websurfers bij een popup scherm snel op de OK-button klikken zonder zich goed te vergewissen van de strekking van de boodschap op het popup scherm. De eigenaar buit zo het ongeduld of de slordigheid van websurfers uit. Zolang de eigenaar op het scherm aangeeft dat een dure nieuwe verbinding opgezet zal worden bij klikken op de OK-button, zal opzet op bedrog doorgaans niet te bewijzen zijn. Het systematisch uitbuiten van de ongeduldigheid van mensen en hen opzadelen met dure 0900-verbindingen die ze – althans dat nemen we aan – niet willen is uiteraard wel asociaal.

9.2.14 Achterdeuren

Een backdoor is een vorm van gemakkelijke, en dikwijls geheime toegang tot een programma dat door de programmeur of programmeurs zelf is ingebouwd. Hoewel het enkele inbouwen van een backdoor niet strafbaar is houdt het toch wel enkele risico's in voor de betreffende programmeur(s). Zoals al eerder gemeld maakt het de programmeur kwetsbaar voor afpersing (art. 317 en 318 Sr). Hij loopt echter nog meer risico's. Indien iemand schade aanricht in de computer nadat hij door de 'backdoor binnen is gekomen' zou de programmeur strafbaar kunnen zijn op basis van art. 350b Sr (culpose gegevensvernieling).

9.2.15 Valsheidsdelicten

> Art 225 Sr.
>
> Valsheid in geschrifte
>
> 1. Hij die een geschrift dat bestemd is om tot bewijs van enig feit te dienen, valselijk opmaakt of vervalst, met het oogmerk om het als echt en onvervalst te gebruiken of door anderen te doen gebruiken, wordt als schuldig aan valsheid in geschrift gestraft, met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie.
>
> 2. Met dezelfde straf wordt gestraft hij die opzettelijk gebruik maakt van het valse of vervalste geschrift als ware het echt en onvervalst dan wel opzettelijk zodanig geschrift aflevert of voorhanden heeft, terwijl hij weet of redelijkerwijs moet vermoeden dat dit geschrift bestemd is voor zodanig gebruik.

De toepasselijkheid van art. 225 Sr in de context van mobiele betaalsystemen hangt nauw samen met de vraag of computergegevens als geschrift aangemerkt kunnen worden en of dergelijke gegevens in de context waarin ze worden gebruikt een bewijsbestemming hebben. Zoals we al eerder hebben gezien beschouwt de Hoge Raad als een geschrift een bestand dat bestaat uit met enige duurzaamheid op een magneetschijf vastgelegde gegevens welke op tamelijk eenvoudige wijze leesbaar kunnen worden gemaakt.[107] Het is daarmee aan te nemen dat ook de gegevens van mobiele betaaltransacties als geschrift aangemerkt zullen kunnen worden.

Van een bewijsbestemming is sprake bij ieder geschrift waarin in het maatschappelijk verkeer betekenis voor het bewijs van enig feit pleegt te worden toegekend. [108] Bij authenticatiegegevens – welke gegevens bijvoorbeeld bij Mobile terminal cloning (telefonie) worden veranderd – is er zonder meer sprake van een bewijsbestemming. Juist de authenticatiegegevens hebben in het maatschappelijk verkeer betekenis als bewijs van de identiteit of de bevoegdheid van degene die met behulp van die gegevens een transactie authenticeert. Bij ander feiten ligt het wellicht moeilijker. Hebben bijvoorbeeld ook de tarieven zoals die in een systeem zijn vastgelegd bewijsbestemming? Privaatrechtelijk is wellicht te betogen dat deze gegevens niet als bewijs van de overeengekomen tarieven gelden. Privaatrechtelijk gaat het wellicht veeleer daarom welke tarieven naar de afnemer van de dienst zijn gecommuniceerd. Niettemin hebben de tarieven onzes inziens wel degelijk bewijsbestemming in strafrechtelijke zin. In de normale afwikkeling van transacties worden de in het systeem vastgelegde tarieven gebruikt om vast te stellen wat de verplichtingen van de afnemer van de dienst zijn. Weliswaar betreft het in geval van de vastlegging van tarieven in een systeem slechts een voorbereidend bestand dat een nodige voorwaarde is voor het opmaken van een factuur, maar de Hoge raad heeft in het arrest van 1991 reeds aangenomen dat ook een voorlopig bestand bewijsbestemming kan hebben. [109]

Valsheden met betrekking tot betaalpassen en waardekaarten zijn apart strafbaar gesteld in art. 232 Sr.

> Art. 232 Sr
>
> Valse betaalpas of waardekaart.
>
> 1. Hij die opzettelijk een betaalpas of waardekaart bedoeld voor het verrichten van betalingen langs geautomatiseerde weg, valselijk opmaakt of vervalst, met het oogmerk zichzelf of een ander te bevoordelen, wordt gestraft met gevangenisstraf van ten hoogste zes jaren of geldboete van de vijfde categorie.
>
> 2. Met dezelfde straf wordt gestraft hij die opzettelijk gebruik maakt van een valse of vervalste betaalpas of waardekaart als ware deze echt en onvervalst, dan wel opzettelijk zodanige betaalpas of waardekaart aflevert of voorhanden heeft, terwijl hij weet of redelijkerwijs moet vermoeden dat de betaalpas of waardekaart bestemd is voor zodanig gebruik.

De strafbaarstelling van fraude in art. 232 Sr is beperkt tot betaalpassen en waardekaarten. Deze begrippen lijken aan de uiterlijke verschijningsvorm van betaalinstrumenten te refereren. Dit kan de vraag oproepen of art. 232 Sr ook van toepassing is als de betaalfunctionaliteit

---

[107] Zie HR 15 januari 1991 NJ 1991, 668, m.nt. Corstens.

[108] HR 14 mei 1957 NJ 1957, 472, HR 29 april 1958 NJ 1959, 56 en HT+R 30 september 1980 NJ 1981 , 70.

[109] Zie HR 15 januari 1991 NJ 1991, 668, m.nt. Corstens.

gerealiseerd wordt door middel van een chip in een mobiel telefoontoestel.[110] De regering blijkt de begrippen betaalpas en waardekaart vooral functioneel te benaderen.[111] Onder een betaalpas wordt verstaan een voorwerp dat op naam van een bepaalde persoon is gesteld en is ingericht om uitsluitend door hem te kunnen worden gebruikt voor financiële transacties langs geautomatiseerde weg. Hierbij is te denken aan de bekende bankpasjes, al dan niet voor zien van een chip. Maar ook toekomstige technische vindingen moeten tot het begrip betaalpas worden gerekend voorzover zij in het maatschappelijk verkeer zijn bedoeld en worden gebruikt door bepaalde personen om financiële transacties te verrichten. Onder een waardekaart wordt verstaan een voorwerp waarvan langs geautomatiseerde weg een zeker geldsbedrag kan worden afgeschreven, evenwel zonder dat deze kaart aan een bepaalde persoon is gebonden. Gezien de functionele benadering die de regering kiest en expliciet insluiting van toekomstige ontwikkelingen lijkt ons verdedigbaar om ook een SIM-kaart die prepaid beltegoeden bevat als waardekaart aan te merken. Of echter een mobiel telefoontoestel als geheel als betaalpas of waardekaart is aan te merken is twijfelachtig. Daarvoor staat de uiterlijke verschijningsvorm van een mobiel toestel toch iets te ver af van wat gewoonlijk onder een betaalpas of waardekaart is te verstaan. Vervalsingen in een mobiel toestel (anders dan aan de SIM-kaart) zouden dan afgedaan moeten worden onder art. 225 Sr.

9.2.16 Witwas delicten

In paragraaf 6.2 zagen we dat een betaaldienst gebruikt kan worden om zwart geld wit te wassen. Een criminele organisatie koopt bijvoorbeeld grote hoeveelheden anonieme opwaardeerkaarten en gebruikt die vervolgens om (informatie)diensten af te nemen van de eigen betaaldienst. De inkomsten uit de betaaldienst zijn (ogenschijnlijk) legaal.

Voor 2001 kende het Nederlandse strafrecht geen specifieke bepaling voor witwaspraktijken. Destijds diende het OM terug te grijpen op de algemene helingbepalingen (art. 416 – 417bis Sr). Dat was mogelijk omdat heling ziet op een ruim scala aan gedragingen: het verwerven, voorhanden hebben, of overdragen van een goed of het vestigen of overdragen van een persoonlijk of zakelijk recht op een goed. De helingbepalingen kenden echter ook een aantal beperkingen. De belangrijkste beperking was dat degene die het gronddelict pleegt niet tevens als heler aangemerkt kan worden.[112] De dief kan bijvoorbeeld niet tevens als heler van het gestolen goed worden aangemerkt, ook al heeft hij het gestolen goed voorhanden. Degene die zijn eigen zwart geld witwast kon daarom niet aangepakt worden. Een andere beperking van de helingbepalingen was dat zij onvoldoende signaleerden dat witwassen een feit was dat de overheid serieus vervolgde.[113] Ook in de sfeer van de internationale rechtshulp kende de helingbepaling bepaalde beperkingen.

Vanwege de beperkingen die de helingbepalingen kenden is in 2001 het witwassen als een afzonderlijk delict strafbaar gesteld.

De centrale strafbaarstelling is in artikel 420bis Sr te vinden:

> 1. Als schuldig aan witwassen wordt gestraft met gevangenisstraf van ten hoogste vier jaren of geldboete van de vijfde categorie:

---

[110] Deze vraag is overigens van belang in verschillende rechtsgebieden en verschillende rechtsverhoudingen. De 'geld-terug' garantie uit Richtlijn 97/7/EG en Richtlijn 2002/65/EG heeft slechts betrekking op (fraude met) betaalkaarten. Bij de implementatie van eerstgenoemde richtlijn is het begrip 'betaalkaart' overgenomen (zie art. 7.1.9A.7 BW).

[111] Kamerstukken II 1989/90, 21551, nr. 3 (MvT) en kamerstukken II 1990/91, 21551, nr.6 (MvA).

[112] HR 7 februari 1978 NJ 1978, 661 en HR 31 maart 1987 NJ 1987, 796.

[113] Voor een uitgebreide bespreking van de achtergronden van de witwasbepalingen zie Schudelaro 2003, p. 112 e.v.

a. hij die van een voorwerp de werkelijke aard, de herkomst, de vindplaats, de vervreemding of de verplaatsing verbergt of verhult, dan wel verbergt of verhult wie de rechthebbende op een voorwerp is of het voorhanden heeft, terwijl hij weet dat het voorwerp – onmiddellijk of middellijk – afkomstig is uit enig misdrijf;

b. hij die een voorwerp verwerft, voorhanden heeft, overdraagt of omzet of van een voorwerp gebruik maakt, terwijl hij weet dat het voorwerp – onmiddellijk of middellijk – afkomstig is uit enig misdrijf.

2. Onder voorwerpen worden verstaan alle zaken en alle vermogensrechten.

Naast deze bepaling kent het Wetboek van Strafrecht nog enkele additionele strafbepalingen met betrekking tot witwassen: voor de recidivist is er het gekwalificeerde delict van art. 420ter Sr en ook de culpose witwasser heeft een eigen strafbepaling: art. 420quater Sr. Bij veroordeling voor een van de witwasdelicten kan ontzetting uit bepaalde rechten en ontzetting uit het beroep waarin het feit begaan is worden uitgesproken (art. 420quinquies Sr).

Zijn de genoemde bepalingen toepasbaar in de context van witwassen met mobiele betaalsystemen? De term voorwerp zou wellicht te beperkt in reikwijdte kunnen zijn: vallen er bijvoorbeeld ook vorderingen onder, of prepaid beltegoeden? Zoals uit het hierboven weergegeven tweede lid van art. 420bis Sr blijkt is de betekenis van het begrip voor toepassing van de witwasbepalingen nader bepaald.[114] Het omvat alle voor menselijke beheersing vatbare stoffelijke objecten («zaken») als alle vermogensrechten. Volgens de regering kan geld zowel onder de eerste categorie vallen, namelijk indien het de chartale vorm heeft, als onder de tweede (giraal geld).[115] Daarmee is aan te nemen dat de term voorwerp tevens een prepaid beltegoed of digital cash omvat.

9.2.17 Strafwaardig, maar niet strafbaar?

Zoals we hiervoor hebben gezien is het zich aanmelden voor diensten onder een valse naam (niet bestaande of de naam van een ander) een belangrijk instrument van fraudeurs. Men kan zich daarom de vraag stellen of in een strafbaarstelling zou moeten worden voorzien. Hierna worden de argumenten voor en tegen op een rijtje gezet.

Argumenten voor:

- Aanmelding onder valse naam is een voorportaal voor fraude met gebruikmaking van de valse naam.
- Strafbaarstelling maakt optreden mogelijk voordat daadwerkelijke fraude plaatsvindt. Door middel van verificatie tegen andere databanken kunnen bruikbare aanwijzingen voor het feit verkregen worden.
- De bewijspositie van het OM is gunstig.
- Legale anonieme alternatieven zijn beschikbaar voor degenen die hun echte naam niet willen prijsgeven: een prepaid toestel; het is overigens nog te bezien of er tezijnertijd ook anonieme mobiele betaalinstrumenten zullen bestaan.

Argumenten tegen:

- Er is sprake van gedrag dat op zich niet schadelijk is.

---

[114] Art. 420quater Sr over culpoos witwassen bevat een identieke bepaling.

[115] Zie Kamerstuken II 2000/2001, 27159, nr. 5, p. 1 (Nota naar aanleiding van het Verslag). De Memorie van Toelichting zegt er het volgende over: Het chartale geld, dat is omgezet in een boot, in een vordering uit lening, in een huis en vervolgens weer in een saldo bij een bank bijvoorbeeld, blijft een «voorwerp – middellijk of onmiddellijk – afkomstig uit enig misdrijf».

- Er kunnen goede redenen bestaan voor het opgeven van een andere dan de eigen naam.
- Indien een aanvraagformulier is ondertekend met een valse handtekening is in het algemeen sprake van valsheid in geschrift, zodat voor deze gevallen reeds in strafbaarstelling is voorzien.
- Handhaving vergt verwerkingen van persoonsgegevens die hoewel rechtvaardigbaar toch de belangen van de betrokkenen kunnen schaden.
- Strafbaarstelling is eigenlijk alleen te verdedigen als er een fraude-intentie is. Het opnemen van een dergelijke intentie in de delictsomschrijving berooft de bepaling van veel van haar zin: zonder veel bewijsproblemen op kunnen treden tegen potentiële fraudeurs.
- Aanbieders van diensten kunnen al maatregelen nemen op basis van het civiele recht. Ze kunnen zich bijvoorbeeld contractueel het recht voorbehouden het contract te beëindigen, indien blijkt dat de klant zich niet onder de eigen naam heeft aangemeld.

In het algemeen wordt aan genomen dat slechts tot wetgeving overgegaan moet worden indien de noodzaak daartoe is komen vast te staan. Gezien het feit dat er reeds een strafbaarstelling is die in veel gevallen soelaas kan bieden en aanbieders van diensten in de contractuele sfeer maatregelen kunnen nemen, is een dergelijke noodzaak onzes inziens niet komen vast te staan, zodat wij een nieuwe strafbepaling hier niet geïndiceerd achten.

Een ander voorbeeld van gedrag dat wellicht niet strafbaar is, is het gebruik van andermans mobiel telefoontoestel voor het afnemen van betaaldiensten, bijvoorbeeld het opvragen van een betaald weerbericht. Dit gedrag lijkt diefstal, maar is het dat ook? De dader lijkt in de eerste plaats een dienst (het weerbericht) weg te nemen. In het licht van de delictsomschrijving van art. 310 Sr (diefstal) of art. 321 Sr (verduistering) betekent dit dat een dienst als een goed aangemerkt zou moeten worden en dat op zijn minst gezegd dubieus. Men zou ook nog kunnen denken dat het wegnemen van een informatiedienst het wegnemen van een hoeveelheid gegevens zou kunnen zijn, maar ook hier loopt men tegen het probleem aan dat gegevens geen goed zijn.[116] Er is wel eens geprobeerd het gebruik van andermans telefoon te bestraffen als diefstal van elektriciteit (elektriciteit is wel een goed[117]), maar ook dat is op niets uitgelopen.[118] De rechtbank oordeelde: "De stroom wordt niet afgeleverd aan gespreksvoerder of abonnee, maar door de PTT gebruikt voor het tot stand brengen van de gewenste verbinding. Er vindt derhalve geen toeëigening plaats van deze stroom door degene die het gesprek aanvraagt, evenmin als er sprake is van het zich toeëigenen van benzine wanneer men gebruik maakt van een taxi waarvoor men de ritprijs niet betaalt." Tenslotte zou men nog kunnen denken dat de dader het giraal geld of prepaid beltegoed wegneemt (art. 310 Sr) of zich toeeigent (art. 321 Sr) waarmee de informatiedienst betaald wordt. Giraal geld is wel een goed.[119] Een probleem hier zou kunnen zijn dat de verrekening voor de afgenomen dienst automatisch en op de achtergrond plaatsvindt. Wellicht biedt dit voor een verdachte perspectief om oogmerk (art. 310 Sr) dan wel opzet (art. 321 Sr) op toe-eigening van het giraal geld dan wel beltegoed te ontkennen. Overigens is dit probleem afwezig indien gebruik wordt gemaakt van een mobiel betaalsysteem in plaats van een mobiele informatiedienst. In dat geval drukt de dader bepaalde toetsen op het mobieltje in om daarmee een betaling (bijv. een overschrijving) te verrichten en dan is oogmerk of opzet op toe-eigening van het geld of tegoed natuurlijk veel moeilijker te ontkennen.

---

[116] HR 3 december 1996, NJ 1997, 574.

[117] HR 23 mei 1921, NJ 1921, 564, W 10728.

[118] Rb. Den Haag 6 november 1985, NJ 1987, 400.

[119] HR 11 mei 1982, NJ 1982 583.

Misschien dat het gedrag onder art. 326c Sr gebracht kan worden als men onder valse signalen tevens begrijpt signalen verstuurd door een onbevoegde. In de rechtspraak is onder valse sleutel ook wel verstaan het gebruik van een sleutel door een onbevoegde, zodat er een aanknopingspunt bestaat voor een dergelijke interpretatie. [120]

9.3 De status van de aanbieder van een mobiel betaalsysteem

Het afnemen van betaalde SMS (informatie)diensten heeft een grote vlucht genomen. Bij prepaid klanten wordt de vergoeding daarbij ten laste gebracht van het uitstaande beltegoed. De vraag dient zich daarmee op mobiele netwerkexploitanten daarmee al dan niet onder het EGI-regime vallen. Met andere woorden: is een prepaid beltegoed elektronisch geld zoals bedoeld in de EGI-richtlijn? Deze vraag maakt veel los bij marktpartijen.

Het EGI-regime stelt een aantal eisen aan partijen die er onder vallen. Zo geldt een zogenaamde terugbetaalplicht, worden eisen gesteld aan het aanvangskapitaal en het permanente vermogen, worden beperkingen gesteld aan de beleggingen die de EGI aanhoudt in verband met haar uitstaande (elektronisch geld)verplichtingen en worden eisen gesteld aan de bedrijfsvoering van de EGI. Daarnaast is nog een aantal regels dat voor kredietinstellingen gelden van toepassing verklaard op EGI's. Het gaat dan vooral om regels over het aanvragen, verlenen en intrekken van vergunningen, over vergunningsvoorwaarden en over de controle van integriteit van beleidsbepalers.

Partijen uit de financiële wereld, die zelf meestal onder een nog strenger regime dan EGI vallen, brengen naar voren dat GSM-operators grootschalig 0900 of andere premium rate services bieden waarmee derde partijen worden betaald voor hun dienstverlening. Het behoeft wat hun betreft geen discussie dat deze partijen zonder meer onder het regime zouden moeten vallen. Ze wijzen dan ook naar De Nederlandse Bank (DNB) om het EGI-toezicht op dergelijke aanbieders zo snel mogelijk in werking te laten treden.

De netwerkexploitanten, aan de andere kant, vinden dat het EGI-regime niet van toepassing is op hun activiteiten. Ze beargumenteren dat de mobiele operator betaalt voor de geleverde diensten, niet de eindgebruiker zelf. Deze betaling vindt plaats met chartaal of giraal geld. De dienstenaanbieder wordt dus niet betaald in beltegoeden. Anders gezegd: de exploitanten redeneren dat ze de betreffende toegevoegde-waardediensten inkopen van de aanbieders daarvan. Vervolgens wederverkopen ze wat ze nu als eigen diensten beschouwen aan hun eigen klanten, net zoals ze hun eigen telecommunicatiediensten verkopen. Omdat geen enkele derde het beltegoed als betaalmiddel accepteert zou het EGI-regime niet van toepassing zijn. Ze wijzen, bij monde van lobbyorganisatie GSM Europe, ook op de gevolgen voor de mobiele telecommunicatiesector als deze wel over het regime zou vallen. De consequenties voor operators zouden groot zijn, en de ontwikkeling van nieuwe diensten in de sector zou daarvan nadelige gevolgen ondervinden.

Op 15 april 2003 heeft DNB zich het voorlopige standpunt ingenomen dat prepaid beltegoed inderdaad niet aan te merken is als elektronische geld in de zin van de WTK 1992. Ze geeft daarbij echter expliciet aan dat het standpunt mogelijk wordt herzien in de toekomst, onder meer gezien de discussie die wordt gevoerd door de Europese Commissie en de toezichthouders in Europa.

Het algemene beeld dat ontstaat uit interviews met marktpartijen is dat de status qua niet tot in de eeuwigheid kan worden gehandhaafd. Meer duidelijk hierover is nodig, in Nederland en daarbuiten. Daarbij is de meest gehoorde mening dat op langere termijn, als het dienstenaanbod via mobiele telefoons een steeds meer divers karakter zal krijgen, de redenering van de mobiele operators niet meer houdbaar is. Bij ongewijzigde wetgeving zullen ze dan ófwel zich er bij moeten neerleggen dat ze vallen onder het EGI-regime, met alle

[120] HR 20 mei 1986, NJ 1987, 170.

consequenties van dien; ófwel de financiële transacties richting derden moeten onderbrengen bij een andere, onafhankelijke organisatie: een eigen beltegoed voor communicatie, en een beurs met een tegoed voor (informatie)diensten bij een externe partij. Overigens wint de laatste tijd ook het idee steun dat wellicht voorzien moet worden in een sui generis wettelijk regime voor telecommunicatieaanbieders. Het toepassen van het onverkorte EGI-regime zou wel heel zwaar drukken op telecommunicatieaanbieders voor iets dat maar een klein deel van hun totale activiteiten uitmaakt. Een bijkomend argument voor een apart wettelijk regime is bovendien dat telecommunicatieaanbieders pas achteraf kunnen beoordelen welk deel van een prepaid tegoed als elektronisch geld is aangewend.

De Europese Commissie die zelf van mening lijkt te zijn dat prepaid kaarten in mobiele telefoons wel elektronisch geld zijn als ze voor het afnemen van producten of diensten van derden gebruikt worden heeft onlangs een consultatieronde gehouden.[121] Uit de reacties van de partijen die van zich hebben laten horen, is echter geen eenduidig beeld naar voren gekomen.[122] De discussie rondom prepaid beltegoeden en het daarop toe te passen regime voor prudentieel toezicht is hiermee voorlopig niet afgesloten.

9.4 De bescherming van de consument

In deze paragraaf wordt onderzocht of de bestaande bepalingen ter bescherming van consumenten toereikend zijn voor mobiele betaalsystemen.

Voor consumenten zijn vooral twee kwesties van belang. Enerzijds dienen zij voldoende en juiste informatie te beschikken over de financiële diensten waarvan zij gebruik maken. Anderzijds hebben zij belang bij een goede regeling van de risicoverdeling voor het geval dat er onbevoegd gebruik gemaakt wordt van hun betaalinstrumenten.

In de financiële sector is al voorzien in een ruime mate van consumentenbescherming. In dit verband kunnen vooral de richtlijn 2002/65/EG (financiële diensten op afstand) en aanbeveling 97/489 genoemd worden.

Met betrekking tot genoemde kwesties is de consumentenbescherming in de telecommunicatie minder ver ontwikkeld. Richtlijn 97/7/EG (koop op afstand) is niet van toepassing op overeenkomsten die worden gesloten met telecommunicatie-exploitanten door het gebruik van publieke telefoon. De (publieke) informatievoorziening aan consumenten met betrekking tot 0900 nummers en PRS-diensten is voorwerp van zelfregulering. De zogenaamde 0900-code wordt beheerd door de Stichting Informatiediensten (Stic) en de Stichting Onafhankelijke Commissie Informatienummers (Stichting OCI).

Nadeel van zelfregulering is dat deze niet dekkend is. Zo bestrijkt de code bijvoorbeeld niet de informatie die met betrekking tot SMS-diensten zou moeten worden verstrekt. Het consumentenprogramma Radar maakte begin 2003 attent op misstanden rond SMS-diensten. Abonnees bleken vaak niet de beschikking te kunnen krijgen over de informatie die zij nodig hadden om SMS-abonnementen op te zeggen, waardoor zij vaak ongewild betaalde SMS-jes bleven ontvangen. Telco's zijn inmiddels bezig te bezien hoe zij deze situatie door middel van zelfregulering op kunnen lossen.[123]

Een andere vraag is of de specifieke regelingen die ter bescherming van consumenten voor de financiële sector gelden niet tevens voor telco's zouden moeten gelden. Een belangrijke vraag is of deze discussie gelijk op gaat met de vraag of telco's als EGI aangemerkt kunnen worden.

---

[121] Zie http://europa.eu.int/comm/internal_market/bank/e-money/index_en.htm.

[122] Zie http://forum.europa.eu.int/Public/irc/markt/markt_consultations/library?l=/financial_services/e-money_operators&vm=detailed&sb=Title.

[123] Zie http://www2.trosradar.nl/?url=PHP/news/3/6/dossier.

Telco's trekken het idee dat hun beltegoeden geen geld zijn uiteraard door naar deze discussie en stellen zich op het standpunt dat Aanbeveling 97/489 en de - in Nederland nog niet geïmplementeerde - richtlijn 2002/65/EG (financiële diensten op afstand) niet op hen van toepassing zijn.

Leveren beide genoemde regelingen echter aanknopingspunten om aan te nemen dat zij reeds nu van toepassing zouden kunnen zijn op telco's waar het gaat om hun beltegoeden?

Met betrekking tot Aanbeveling 97/489/EG is de central vraag of een beltegoed aangemerkt worden als een betaalinstrument met toegang op afstand of als een elektronisch geldinstrument in de zin van de Aanbeveling. Een "betaalinstrument met toegang op afstand" wordt gedefinieerd als een instrument waarmee een houder toegang kan krijgen tot geldmiddelen die zich op diens rekening bij een instelling bevinden, waarbij een betaling aan een begunstigde wordt toegestaan en waarvoor gewoonlijk een persoonlijk identiteitsnummer (pincode) en/of een ander soortgelijk bewijs van identiteit benodigd is. Hieronder zijn met name betaalkaarten (krediet-, debet-, uitgestelde debiterings- of bankkaarten) en toepassingen voor telefonisch en thuisbankieren begrepen. Bij een beltegoed is in het algemeen geen sprake van een rekening in traditionele zin. Een "elektronisch-geldinstrument" wordt gedefinieerd als een oplaadbaar betaalinstrument niet zijnde een betaalinstrument met toegang op afstand, bestaande in een kaart waarop waarde is opgeslagen of in een computergeheugen, waarop waarde-eenheden elektronisch worden opgeslagen hetgeen de houder ervan in staat stelt bepaalde transacties te verrichten, zoals het overmaken van gelden of het opnemen van contanten. Met name de eis dat geld overgemaakt of opgenomen moet kunnen worden levert (vooralsnog) een redelijk sterk argument op voor het standpunt dat een beltegoed niet als elektronisch geldinstrument aangemerkt kan worden.

Richtlijn 2002/65/EG definieert financiële diensten ruim. Onder financiële diensten wordt verstaan iedere dienst van bancaire aard of op het gebied van kredietverstrekking, verzekering, individuele pensioenen, beleggingen en betalingen. Iedere dienst op het gebied van betalingen laat ruimte om ook telco's onder de werking van deze richtlijn te brengen. De richtlijn is echter nog niet geïmplementeerd in Nederlandse wetgeving.

9.5 Zelfregulering en preventie

In de eerste paragraaf van dit hoofdstuk is gebleken dat de meeste vormen van – voorzienbaar - frauduleus gedrag met betrekking tot mobiele betaalsystemen al strafbaar zijn. Strafrechtelijk optreden tegen fraude is echter niet een oplossing voor alle problemen die door fraude worden veroorzaakt. Het strafrecht biedt bijvoorbeeld weinig mogelijkheden om maatregelen te nemen ter beperking van schade die optreedt als fraude zich ontvouwt. Het strafrecht geeft ook niet aan hoe partijen in een ingewikkelde waardeketen het best kunnen samenwerken bij een (vermoeden van) fraude. Ook het civiele recht en het bestuursrecht bieden geen pasklare oplossingen voor deze vragen. Er is daarom behoefte aan een nadere regulering of afstemming van gedrag die nauw aansluit op de concrete setting waarin partijen zich bevinden. Zelfregulering kan in die behoefte voorzien. Het Convenant tot het tegengaan van Oneigenlijk Gebruik van Informatienummers is een treffend voorbeeld van zelfregulering van partijen in een waardeketen. Een aantal vaste en mobiele netwerkaanbieders, platformaanbieders en KPN Carrier Services hebben in het Convenant vastgelegd hoe zij met vermoed oneigenlijk gebruik van informatienummers omgaan. Daartoe definieert het Convenant wat tussen partijen zal gelden als oneigenlijk gebruik en is een procedure overeengekomen voor het vaststellen van oneigenlijk gebruik in een concreet geval. Het convenant geeft aan hoe te handelen bij een geconstateerd vermoeden van oneigenlijk gebruik, schept onderlinge informatieplichten en bevat financiële afspraken (over opschorting van betalingen en terugbetalingsverplichtingen). Het Convenant bevat ook afspraken over de afsluiting en het niet-aankiesbaar maken van informatienummers en de plaatsing op een zwarte lijst van nummerexploitanten in geval van oneigenlijk gebruik. Het is goed voorstelbaar

dat er bij de uitrol van enige vorm van mobiel betalen behoefte zal bestaan aan zelfregulering die onderwerpen als de genoemde ter hand neemt. Dergelijke zelfregulering kan echter pas van de grond komen als er duidelijkheid is over de wijze waarop mobiel betalen straks vorm zal krijgen, met name omdat zelfregulering nauw aansluit op de concrete setting van partijen in een waardeketen. Vooralsnog is nog niet duidelijk welke van de vier onderscheiden varianten straks het dominante model zal worden, laat staan dat duidelijk is hoe de infrastructuur voor mobiel betalen straks in concreto uit zal zien.

De overheid heeft recentelijk het bovengenoemde Convenant omarmd. Een groot aantal (overheids)instanties gaat intensiever samenwerken met de partijen vertegenwoordigd in het Convenant, te weten: het Ministerie van Economische Zaken, het Openbaar Ministerie, de OPTA, de Bovenregionale Recherche Noord- en Oost- Nederland (BR NON), de Stichting Informatiedienstencode (Stic), de Nederlandse Vereniging van Informatiedienstaanbieders (NVI) en ICT Telecom, als vertegenwoordiger van de telecommunicatiesector.[124] Afgaande op dit voorbeeld, lijkt de rol van de overheid met betrekking tot zelfregulering er vooral een te zijn van het versterken van en voortbouwen op initiatieven die in de private sector zijn genomen. De vraag is of de overheid een proactievere, initiërende rol zou moeten spelen bij zelfregulering van mobiel betalen. Het Convenant richt zich op een gezamenlijk probleem van de partijen in de waardeketen. Dat levert een prikkel op voor partijen om tot zelfregulering te komen. Het is niet duidelijk of zich een soortgelijke situatie zal voordoen ten aanzien van mobiel betalen. Het is daarom aan de overheid om wat dit betreft de vinger aan de pols te houden, en te bezien of de belangen van zwakkere partijen (consumenten?) voldoende tot hun recht komen en zonodig stappen te zetten om tijdig tot regulering van pertinente belangen te komen.

Een ander vraag betreft het volgende: in hoeverre werpt het recht barrières op voor de sector bij het via zelfregulering bestrijden van fraude. In het bijzonder is uit het onderzoek een element naar voren gekomen: de vraag of privacyregels in de weg staan aan het aanleggen van zwarte lijsten van fraudeurs en het beschikbaar stellen van een dergelijke lijst binnen de waardeketen.

De gegevens van degenen die op een zwarte lijst staan kwalificeren als persoonsgegevens in de zin van de Wet bescherming persoonsgegevens. De WBP is daarmee van toepassing. Dat betekent persoonsgegevens in verband met zwarte lijsten op behoorlijke en zorgvuldige wijze en in overeenstemming met de WBP moeten worden verwerkt. Het College bescherming persoonsgegevens biedt een handreiking in de vorm van een checklist voor zwarte lijsten.[125] Deze checklist is gebaseerd op onderzoek dat reeds in 1995 is verricht.[126] De Europese artikel 29 Werkgroep heeft eveneens een werkdocument over zwarte lijsten opgesteld. [127] De beheerder van een zwarte lijst moet een protocol opstellen welk protocol eventueel op rechtmatigheid getoetst kan worden door het College Bescherming Persoonsgegeven, zoals gebeurd is met het Protocol Incidentenwaarschuwingssysteem financiële instellingen.[128] Indien een zwarte lijst behalve in Nederland ook in het buitenland gebruikt moet kunnen worden, wordt het bewerkelijker om aan voorwaarden rond het privacyrecht te voldoen, maar niet

---

[124] Zie http://www.ez.nl/content.jsp?objectid=11448.

[125] Zie http://www.cbpweb.nl/themadossiers/th_zwl_regels.stm?refer=true&theme=purple.

[126] A.F. Rommelse, Zwarte lijsten. Belangen en effecten van waarschuwingssystemen, Achtergrondstudies en Verkenningen 4, http://www.cbpweb.nl/downloads_av/AV04.pdf?refer=true&theme=green.

[127] Werkdocument over zwarte lijsten van de Groep Gegevensbescherming Artikel 29, 11118/02/NL/def.WP 65, beschikbaar op: http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp65_nl.pdf

[128] Zie http://www.cbpweb.nl/documenten/uit_z2002-0495.stm?refer=true&theme=green&refurl=http%3A//www.cbpweb.nl/themadossiers/th_zwl_publ.stm.

onmogelijk. Bij gebruik binnen de EU kunnen eventuele verschillen in implementatie van privacywetgeving voor frictie zorgen. Indien het nodig is persoonsgegevens door te geven naar derde landen, moeten die derde landen in beginsel over een adequaat niveau van bescherming van persoonsgegevens beschikken. Bij uitzondering kunnen echter ook gegevens doorgegeven worden naar landen die geen adequaat beschermingsniveau kennen (art. 77 WBP). Ook in internationale context werpt privacyrecht dus geen onoverbrugbare barrières op voor de aanleg van zwarte lijsten. Wel vergt de aanleg van zwarte lijsten veel van het organisatievermogen van de betrokken bedrijven. Een wat concreter probleem betreft het registreren van oprichters van frauderende rechtspersonen. Indien vastgesteld is dat een rechtspersoon fraudeert, komt niet steeds vast te staan of de natuurlijke personen achter deze rechtspersonen zelf ook gefraudeerd hebben. Dat maakt het moeilijk om hen op een zwarte lijst te plaatsen.

Ondertussen blijkt dat in de financiële sector al op ruime schaal gebruik gemaakt wordt van een zwarte lijst. Volgens de Nederlandse Vereniging van Banken staan ongeveer twintigduizend fraudeurs geregistreerd in de externe verwijzingsapplicatie, i.e. de zwarte lijst van de banken.[129]

9.6 Conclusie

In dit hoofdstuk zijn de volgende onderzoeksvragen behandeld: Is het bestaande wettelijke instrumentarium toereikend om deze (nieuwe) vormen van fraude adequaat te bestrijden? Zo niet, op welke terreinen bestaan lacunes? Hoe kunnen deze lacunes gedicht worden?

Bij de beantwoording van deze vragen is een viertal perspectieven gehanteerd, namelijk strafbaarstellingen, de status van de aanbieder van een mobiel betaalsysteem, consumentenbescherming en preventie en zelfregulering. De conclusies zijn gegroepeerd rond deze perspectieven.

Strafbaarstellingen

Mobiel betalen bevindt zich nog in een embryonaal stadium. Welke uitrolvariant straks dominant zal blijken is nog onduidelijk. Ook over de toekomstige fraudevormen bestaat nog onduidelijkheid. Bij de geraadpleegde experts leefde het gevoelen dat fraude in verband met mobiele betaalsystemen in het verlengde zal liggen van huidige bekende fraudevormen.

Ook bestaat het idee dat de bestaande strafbaarstellingen voldoende techniekonafhankelijk zijn geformuleerd om ook fraude met mobiele betaalsystemen te kunnen bestrijden. Een analyse van de in hoofdstuk 6 onderscheiden fraudevormen heeft dat beeld bevestigd. Er is nog onvoldoende noodzaak nu al in eventuele strafbaarstellingen te voorzien.

Een uitzondering is wellicht phishing dat strafbaar gesteld zou kunnen worden als een bijzondere vorm van bedrog. Het door enige vorm van misleiding verkrijgen van authenticatiegegevens is een belangrijke voorbereidingshandeling op eigenlijke fraude. Het is echter onzeker of zij gedekt wordt door de huidige bedrogbepalingen die sterk georiënteerd zijn op vermogenscriminaliteit. De strafbaarstelling van phishing zou overigens niet uniek zijn voor mobiele betaalsystemen, maar heeft het karakter van een algemene vorm van computercriminaliteit.

Een andere mogelijke nieuwe strafbaarstelling betreft het zich onder een valse naam aanmelden voor telecommunicatie- of financiële diensten. Ook dit is belangrijke voorbereidingshandeling op eigenlijke fraude. Niettemin is het twijfelachtig of hier de noodzaak bestaat om tot een nieuwe strafbaarstelling te komen. Enerzijds is dit feit al

[129] Zie de Volkskrant van 23 november 2004, p. 1: "Duizenden 'fraudeurs' op zwarte lijst".

strafbaar als valsheid in geschrift in die gevallen waarin de naam een bewijsbestemming heeft en dat zal vaak het geval zijn (bijvoorbeeld blijkend uit een handtekening). Anderzijds beperkt het de mogelijkheden van degene die om te honoreren redenen (bijvoorbeeld uit veiligheidsoverwegingen) hun eigen naam niet willen prijsgegeven.

Een ander gedrag dat wellicht een nieuwe strafbaarstelling rechtvaardigt is het wederrechtelijk gebruik van een (mobiele) telefoon voor het afnemen van betaaldiensten. Het is twijfelachtig of het gebruik van andermans telefoon zonder toestemming (bijv. om betaaldiensten af te nemen) nu reeds strafbaar is. Het lijkt geen diefstal te zijn omdat primair een dienst wordt afgenomen. Het is twijfelachtig of het afnemen van een dienst kan gelden als het wegnemen van een goed en alternatief of bewezen kan worden of de dief zich het geld waarmee die dienst betaald wordt opzettelijk toeeigent. Toepassing van bedrogbepalingen is twijfelachtig omdat er bij afwezigheid van een authenticatie geen misleiding van de dienstverlener hoeft plaats te vinden.

De status van de aanbieder van een mobiel betaalsysteem

Op dit moment worden prepaid beltegoeden nog niet aangemerkt als elektronisch geld in de zin van Richtlijn 2000/46/EG en de WTK 1992 (waarin genoemde richtlijn is geïmplementeerd). De betreffende telco's vallen dan ook niet onder het zogenaamde EGI-regime. De financiële sector ziet hierin een ongerechtvaardigde bevoordeling van de telco's. De telco's vrezen dat zij niet kunnen voldoen aan sommige eisen die aan EGI's gesteld worden, vooral aan de eisen van solvabiliteit en liquiditeit niet. Bovendien zou het uitvoerbaar maken van de terugbetaalverplichting grote investeringen vergen van de telco's. De sleutel tot deze discussie ligt in Europa. De Europese Commissie heeft onlangs een publieke consultatie over dit onderwerp afgesloten. De verwachting is dat het onontkoombaar is dat het uitgeven van prepaid beltegoeden onderworpen wordt aan op de financiële activiteiten toegespitste regels over bedrijfsvoering en aan regels over prudentieel toezicht.

Consumentenbescherming

Het idee bestaat dat met betrekking tot financiële dienstverlening al een voldoende uitgewerkt regelstelsel tot bescherming van de consument bestaat. Indien telecommunicatieaanbieders als EGI aangemerkt zullen worden ligt voor de hand dat behalve regelgeving over prudentieel toezicht, de WID en de Wet MOT, ook de betreffende regelgeving met betrekking tot consumentenbescherming bij financiële dienstverlening (Aanbeveling 97/489/EG en de toekomstige implementatie van Richtlijn 2002/65/EG) op hen van toepassing wordt. Onduidelijk is of deze regelgeving nu al op telecommunicatieaanbieders toegepast zou kunnen worden voor zover het hun omgang met prepaid beltegoeden betreft. Gezien de consumentenbelangen die op het spel staan zou dit wel gewenst zijn.

Preventie en zelfregulering

Marktpartijen beschouwen het aanleggen van zwarte lijsten als een belangrijk wapen in de strijd tegen fraude. Ze voelen zich echter belemmerd door privacyregelgeving bij het opzetten van desbetreffende databases, vooral indien die een internationaal karakter hebben. Uit het onderzoek blijkt dat privacywetgeving de aanleg van zwarte lijsten niet belemmert, maar wel bepaalde voorwaarden stelt aan het beheer en de samenstelling van de lijsten.

Het Convenant tot het tegengaan van Oneigenlijk Gebruik van Informatienummers is een voorbeeld van een geslaagde vorm van zelfregulering die voorziet in afstemming en samenwerking tussen de betrokken partijen in de telecommunicatiewaardeketen. Het maakt adequaat optreden tegen fraudeurs mogelijk. Het is aan de overheid om te bewaken dat de

belangen van zwakkere partijen bij mobiel betalen niet in gedrang komen indien bij mobiel betalen een dergelijke samenwerking binnen de keten niet van de grond zou blijken te komen.

10 Conclusie en discussie

10.1 Inleiding

In dit hoofdstuk laten we de belangrijkste conclusies uit de voorgaande hoofdstukken nog eens de revue passeren. Daarmee worden de onderzoeksvragen uit het eerste hoofdstuk eveneens beantwoord.

De structuur van de conclusies sluit aan op de structuur van het rapport. In de volgende paragraaf staan de conclusies over de markt voor mobiel betalen (deel I). In dit deel staan de eerste drie onderzoeksvragen centraal (met nadruk op de eerste onderzoeksvraag). De derde paragraaf benoemt de conclusies uit deel II van het rapport (fraude bij mobiel betalen). In deze paragraaf van de conclusies komen onderzoeksvragen 4, 5 en 8 aan bod. In de vierde paragraaf staan de bevindingen uit het derde deel – het juridische kader – centraal. Daarmee worden onderzoeksvragen 6 en 7 beantwoord. In de laatste paragraaf komen nog enkele overige conclusies aan bod.

10.2 Conclusies over de markt voor mobiel betalen (deel I)

Mobiel betalen heeft enige omvang maar zal in de toekomst zich nog verder ontwikkelen. De markt voor mobiel betalen omvat veel verschillende verschijningsvormen. Gegeven de door ons gehanteerde definitie, wordt er nu in Nederland al op behoorlijke grote schaal mobiel betaalt. Alleen al de betalingen via 090x nummers bedroegen in 2002 naar schatting 350 tot 400 miljoen Euro. Daarnaast groeit de wat nieuwere markt van betalingen via premium rate SMS diensten snel (met name ringtones en logo's). Er zijn echter een aantal nieuwe, meer geavanceerde vormen van mobiel betalen op komst. Deze bieden onder meer een grotere functionaliteit in relatie tot de geleverde diensten of producten (in plaats van een statisch tarief gekoppeld aan de oproep van een bepaald nummer), bredere toepassingsmogelijkheden (waaronder local en remote betalingen) en andere afrekenmechanismen (zoals debetbetalingen).

De verwachtingen voor mobiel betalen in Nederland zijn gematigd. Veel partijen in de financiële sector stellen dat mobiel betalen geen overtuigende voordelen heeft boven de alternatieven. Daarnaast zijn de kosten aanzienlijk. De introductie is een complexe zaak en als er niet snel een grote schaal wordt bereikt, blijven de transactiekosten hoger dan die van andere betaalmiddelen. Alleen in de deelmarkt van betalingen van on-line content wordt mobiel betalen op de korte tot middellange termijn behoorlijke kansen toegedicht. Ook de wat slechtere economische vooruitzichten worden genoemd als een reden waarom de verwachtingen omtrent mobiel betalen naar beneden zijn bijgesteld.

Markt voor mobiel betalen toont verwachtschap met de markt voor internetbetalingen, maar er zijn ook belangrijke verschillen. Ten eerste heeft de (consumenten)vraag een duidelijk ander karakter: Internetbetalingen worden bijvoorbeeld regulier gebruikt voor relatief grote, internationale betalingen, bij mobiel betalen zal dat minder het geval zijn. Ten tweede zijn de eisen aan beveiliging anders en daarmee ook de veiligheidsrisico's. Dat heeft onder meer te maken met het feit dat mobiele telefoons gemakkelijk prooi van diefstal kunnen worden of door hun geringe afmetingen gemakkelijk verloren kunnen worden. Ook de technische beveiliging stelt andere eisen. Ten derde noopt mobiel betalen tot andere inrichting van het proces (en daarmee het gebruiksgemak). Een voor internetbetalingen acceptabele methode met TAN-lijsten of cryptocalculator is voor mobiel betalen niet goed denkbaar.

De ontwikkelingen bij mobiel betalen zijn nog omgeven door veel onzekerheden. Deze zijn primair niet van technische aard. De onzekerheden zijn eerder het gevolg van het ontbreken van een sluitende business case voor mobiel betalen.[130]

Juist in Nederland zal mobiel betalen last hebben de markt te veroveren. In Nederland is de (toonbank)betaalmarkt goed ontwikkeld. Het pinsysteem is breed ingevoerd en wordt alom als erg kosteneffectief beschouwd. Betalingen met chipcards beginnen - na een valse start - ook serieuze omvang te bereiken. Op de meeste deelmarkten voor mobiel betalen vormen deze bestaande systemen geduchte concurrenten, behalve bij de deelmarkt van on-line content.

--> Al met al zal de introductie van mobiel betalen naar verwachting niet op snelle wijze plaatsvinden

Door het dilemma nationaal/internationaal zal naar verwachting alleen de deelmarkt van online content betalingen zich snel ontwikkelen. De betalingsmarkt heeft een bij uitstek nationaal karakter. Meer geavanceerde implementaties van mobiel betalen - zoals authenticatie met een additionele chipcard in de mobiele telefoon - vragen echter om een grote (lees: internationale) schaal om op kosteneffectieve wijze ingevoerd te kunnen worden. Dat levert een dilemma op. De verwachting van de meeste marktpartijen is dat mobile betalen in eerste instantie vorm zal krijgen als nationale, wat minder geavanceerde implementaties.

De ontwikkeling van verschillende deelmarkten bij mobile betalen zal zich over de tijd uitspreiden. De markt voor mobiel betalen zal zich naar verwachting het eerst ontwikkelen als diensten voor het verrichten van microbetalingen ten behoeven van online content of online diensten. Pas wat later in de tijd zullen vervolgens (2) lokale microbetalingen, (3) remote macrobetalingen (ook internationaal) en (4) lokale macrobetalingen op de markt verschijnen.

Er zijn veel kleinere initiatieven maar ze zijn weinig kansrijk. Er ontwikkelen zich talloze initiatieven, die worden aangeboden door bestaande partijen maar ook door nieuwe toetreders tot de markt. Deze initiatieven, in Nederland en ook daarbuiten, vinden we zowel bij internetbetalingen als bij mobiel betalen. Veel initiatieven hebben echter moeite enige schaal te bereiken en soms verdwijnen ze niet lang na de introductie. Nieuwe toetreders staat dan het failliet in het vooruitzicht.

De (vele) internationale normalisatie-initiatieven worden door marktpartijen als weinig belangrijk beschouwd. Reeds enige jaren geleden zijn er talloze initiatieven genomen ter normalisatie van mobiele betaalsystemen. Bijna elk van deze initiatieven wordt gedomineerd door één bepaald type spelers: telecommunicatiebedrijven, banken of creditcard organisaties. Nederlandse marktpartijen geven echter aan relatief weinig van dergelijke initiatieven te verwachten; ze staan in hun ogen te ver van de realiteit en kunnen te weinig inspelen op de sterk uiteenlopende nationale context.

10.3 Conclusies over fraude bij mobiel betalen (deel II)

Bij de introductie van nieuwe diensten en systemen nemen vooral de risico's voor technische fraude sterk toe. Op dit moment is bij zowel telecommunicatiediensten als bij betaaldiensten de zogenaamde relatiefraude de grootste categorie. Bij de introductie van nieuwe mobiele betaaldiensten verwachten wij echter dat technische fraude de overhand krijgt, in ieder geval voor enige tijd. Met name nieuwe onderliggende technieken (GPRS, UMTS, intersystem roaming) creëren onzekerheid over de frauderisico's. Met name technische ontwikkelingen als het gebruik van IP-adressering brengen veel onzekerheden met zich mee.

---

[130] Dit geldt tenminste voor de case voor mobile betalen op zichzelf; voor mobiele netwerkexploitanten kan mobile betalen een enabler zijn om andere diensten te realiseren (zoals betaalde content).

Fraudevormen zijn slechts beperkt te voorspellen. Hoewel marktpartijen zich inspannen om ex-ante deze risico's in kaart te brengen en hun systemen afdoende tegen misbruik te beschermen, zijn lang niet alle technische en niet-technische risico's vooral te voorspellen. Aanbieders zijn dan ook in belangrijke mate aangewezen op een reactief fraudebeleid. Het is een gegeven dat deels achter de feiten zult blijven aanlopen.

Bestaande fraude-detectiesystemen zijn tot op zekere hoogte bruikbaar in de nieuwe wereld. De huidige systemen van zowel telecommunicatie-exploitanten als van financiële partijen kunnen onder meer door geavanceerde patroonherkenning fraude's aan het licht brengen. Veel van de huidige technieken zijn ook bruikbaar in de nieuwe context van mobiel betalen. Er bestaan echter ook veel vormen van fraude die niet goed door bestaande systemen kunnen worden opgespoord.

De inschattingen van de omvang van fraude bij mobiel betalen verschillen, alsook het belang van de bestrijding. Geïnterviewden hebben sterk uiteenlopende beelden bij de omvang en het belang van bestrijding. Het is natuurlijk mogelijk dat bedrijven om strategische of bedrijfstechnische redenen frauderisico's en fraudeomvang naar de buitenwereld liever bagatelliseren. Toch lijkt het er sterk op dat ook de werkelijke inschattingen uiteenlopen.

Nieuwe toetreders lopen een verhoogd risico op schade door fraude. De aandacht voor fraude en de effectiviteit van de bestrijding daarvan is noodgedwongen lager dan bij gevestigde spellers. Plegers van fraude zullen inspelen op deze zwakte en zich juist op deze partijen richten.

Fraude door criminele organisaties is een serieuze bedreiging. Vooral bij telecommunicatienetwerken zien we nu al diverse vormen van goed georganiseerde fraude, gepleegd door grote bendes met internationale vertakkingen. SIM-kaarten verdwijnen soms linea recta over de grens om daar in belhuizen te worden ingezet. Nieuwe technieken worden snel bestudeerd door criminelen die eventueel capabele cryptologen en technici inschakelen om beveiligde systemen te kraken. De hoge werkloosheid onder dergelijke specialisten in Oost-Europese landen is daarbij een serieus risico.

Met een complexer wordende waardeketen neemt de kans op fraude door bedrijven in de waardeketen toe. Reeds nu zijn er bij premium rate nummers talloze min of meer malafide partijen actief. Dat varieert van diensten die het klanten amper mogelijk maken om hun abonnement op te zeggen tot 0900-nummers die alleen maar – onbedoeld - aangeroepen worden door autodialers. Deze praktijken waren reeds de aanleiding tot een code voor zelfregulering in de sector. Deze ontwikkeling zal zich mogelijk voortzetten en versterken als de waarketen complexer wordt en als de diversiteit van diensten (en mogelijkheden daartoe) toeneemt.

Steeds meer wordt de mens de zwakke schakel. De technieken waarvan fraudeurs zich bedienen zijn steeds geavanceerder. Het wordt voor de eindgebruiker steeds lastiger de benodigde zorgvuldigheid in acht te nemen: een slim geschreven malafide applicatie is zelfs door de meest ervaren gebruiker niet meer te herkennen als zodanig, en malafide applicaties weten de gebruikersinterface echte betaaldiensten op een zo overtuigende wijze te imiteren dat het de gebruiker eigenlijk niet meer aan te rekenen valt dat deze zijn pincode heeft ingevoerd.

Uit gesprekken en de literatuur mag worden opgemaakt dat ook interne fraude een aanzienlijke omvang heeft. Het gaat daarbij om fraude door (of met behulp van) medewerkers. Sommige bedrijven rekenen fraude door dealers ook tot interne fraude. Gezien het karakter van deze studie gaan we echter niet dieper in op interne fraude.

10.4 Conclusies over wet- en regelgeving (deel III)

Strafbaarstellingen

Fraudevormen rond mobiel betalen zullen in het verlengde liggen van huidige bekende fraudevormen. Mobiel betalen bevindt zich nog in een embryonaal stadium. Welke uitrolvariant straks dominant zal blijken is nog onduidelijk. Ook over de toekomstige fraudevormen bestaat nog onduidelijkheid. Bij de geraadpleegde experts leefde het gevoelen dat fraude in verband met mobiele betaalsystemen in het verlengde zal liggen van huidige bekende fraudevormen.

De bestaande strafbaarstellingen dekken fraude bij mobiel betalen al voor een groot deel. Bij experts bestaat het idee dat de bestaande strafbaarstellingen voldoende techniekonafhankelijk zijn geformuleerd om ook fraude met mobiele betaalsystemen te kunnen bestrijden. Een analyse van de in hoofdstuk 6 onderscheiden fraudevormen heeft dat beeld bevestigd. Er is nog onvoldoende noodzaak nu al in eventuele strafbaarstellingen te voorzien.

Een aparte strafbaarstelling van phishing is het overwegen waard. Phishing zou strafbaar gesteld moeten worden als een bijzondere vorm van bedrog. Het door enige vorm van misleiding verkrijgen van authenticatiegegevens is een belangrijke voorbereidingshandeling op eigenlijke fraude. Het is echter onzeker of zij – als voorbereidingshandeling - gedekt wordt door de huidige bedrogbepalingen die sterk georiënteerd zijn op vermogenscriminaliteit (en niet zozeer op het verkrijgen van authenticatiegegevens). De strafbaarstelling van phishing zou overigens niet uniek zijn voor mobiele betaalsystemen, maar heeft het karakter van een algemene vorm van computercriminaliteit.

Aanmelding onder valse naam behoeft geen aparte strafbaarstelling. Een andere voorbereidingshandeling betreft het zich onder een valse naam aanmelden voor telecommunicatie- of financiële diensten. Niettemin is het twijfelachtig of hier de noodzaak bestaat om tot een nieuwe strafbaarstelling te komen. In de eerste plaats is dit feit al strafbaar als valsheid in geschrift in die gevallen waarin de naam een bewijsbestemming heeft en dat zal vaak het geval zijn (bijvoorbeeld blijkend uit een handtekening). Bovendien beperkt het de mogelijkheden van degene die om te honoreren redenen (bijvoorbeeld uit veiligheidsoverwegingen) hun eigen naam niet willen prijsgegeven.

De status van de aanbieder van een mobiel betaalsysteem

De huidige status quo – op telco's wordt geen enkel prudentieel toezicht gehouden - is instabiel. Op dit moment worden prepaid beltegoeden nog niet aangemerkt als elektronisch geld in de zin van Richtlijn 2000/46/EG en de WTK 1992 (waarin genoemde richtlijn is geïmplementeerd). De betreffende telco's vallen dan ook niet onder het zogenaamde EGI-regime. De financiële sector ziet hierin een ongerechtvaardigde bevoordeling van de telco's. De telco's vrezen dat zij niet kunnen voldoen aan sommige eisen die aan EGI's gesteld worden, vooral aan de eisen van solvabiliteit en liquiditeit niet. Bovendien zou het uitvoerbaar maken van de terugbetaalverplichting grote investeringen vergen van de telco's.

Een sui generis regime voor prudentieel toezicht op telco's komt steeds nadrukkelijker in beeld. De sleutel tot de discussie rond het prudentieel toezicht op telco's ligt in Europa. De Europese Commissie heeft onlangs een publieke consultatie over dit onderwerp afgesloten. De verwachting is dat het onontkoombaar is dat het uitgeven van prepaid beltegoeden onderworpen wordt aan op de financiële activiteiten toegespitste regels over bedrijfsvoering en aan regels over prudentieel toezicht.

Consumentenbescherming

De EGI-discussie heeft ook consequenties voor de consumentenbescherming. Het idee bestaat dat met betrekking tot financiële dienstverlening al een voldoende uitgewerkt regelstelsel tot bescherming van de consument bestaat. Indien telecommunicatie-aanbieders als EGI aangemerkt zouden worden ligt voor de hand dat behalve regelgeving over prudentieel toezicht, de WID en de Wet MOT, ook de betreffende regelgeving met betrekking tot consumentenbescherming bij financiële dienstverlening (Aanbeveling 97/489/EG en de toekomstige implementatie van Richtlijn 2002/65/EG) op hen van toepassing wordt.

De consumentenbescherming bij beltegoeden is onduidelijk. Onduidelijk is of Aanbeveling 97/489/EG en de toekomstige implementatie van Richtlijn 2002/65/EG nu al op telecommunicatie-aanbieders toegepast zou kunnen worden voor zover het hun omgang met prepaid beltegoeden betreft. Gezien de consumentenbelangen die op het spel staan zou dit wel gewenst zijn.

Preventie en zelfregulering

Privacywetgeving blokkeert het gebruik van zwarte lijsten niet. Marktpartijen beschouwen het aanleggen van zwarte lijsten als een belangrijk wapen in de strijd tegen fraude. Ze voelen zich echter belemmerd door privacyregelgeving bij het opzetten van desbetreffende databases, vooral indien die een internationaal karakter hebben. Uit het onderzoek blijkt dat privacywetgeving de aanleg van zwarte lijsten niet belemmert, maar wel bepaalde voorwaarden stelt aan het beheer en de samenstelling van de lijsten. De beheerder van een zwarte lijst moet een protocol opstellen welk protocol eventueel op rechtmatigheid getoetst kan worden door het College Bescherming Persoonsgegeven, zoals gebeurd is met het Protocol Incidentenwaarschuwingssysteem financiële instellingen.[131]

Het is aan de overheid de belangen van zwakke partijen te bewaken bij (ontbreken van) zelfregulering bij mobiel betalen. Het Convenant tot het tegengaan van Oneigenlijk Gebruik van Informatienummers is een voorbeeld van een geslaagde vorm van zelfregulering die voorziet in afstemming en samenwerking tussen de betrokken partijen in de telecommunicatiewaardeketen. Het maakt adequaat optreden tegen fraudeurs mogelijk. Het is aan de overheid om te bewaken dat de belangen van zwakkere partijen bij mobiel betalen niet in gedrang komen indien bij mobiel betalen een dergelijke samenwerking binnen de keten niet van de grond zou blijken te komen.

10.5 Andere conclusies en observaties

Gebrek aan capaciteit bij het OM. Veel interviewpartners hebben gewezen op de relatief lage capaciteit die het Openbare Ministerie beschikbaar heeft voor het behandelen van fraudezaken. Als een gedupeerde partij zoals een netwerkexploitant besluit aangifte te doen van een fraudegeval wordt deze zaak dan ook vaak niet in behandeling genomen. Bovendien krijgen de voor deze studie relevante vormen van fraude een steeds complexer karakter; dat vraagt ook om zeer specialistische kennis, alsook mechanismen om snel van nieuwe kennis meester te maken.

---

[131] Zie http://www.cbpweb.nl/documenten/uit_z2002-0495.stm?refer=true&theme=green&refurl=http%3A//www.cbpweb.nl/themadossiers/th_zwl_publ.stm

Bijlage 1. Fraudevormen bij telecommunicatie

De onderstaande tabel sluit aan op paragraaf 5.3. De tabel geeft een – niet uitputtend – overzicht van vormen van fraude bij telecommunicatienetwerken. Daarbij wordt een onderscheid gemaakt tussen fraudevormen die specifiek bij vaste netwerken optreden, fraudevormen specifiek bij mobiele netwerken, en fraudevormen die bij beide typen netwerken worden geconstateerd.

De verzamelde fraudevormen sluiten elkaar niet onderling uit. Ze zijn tot een zekere hoogte ongelijksoortig, terwijl er ook fraudevormen zijn die onderling samenhangen.

Fraudevorm	*Korte omschrijving*	*Netwerk*[132]	*Schade bij*[133]
(Fixed) calling card fraud	Misbruik van belkaarten voor vaste netwerken (zoals de inmiddels niet meer aangeboden Scope card van KPN). Door afkijken van de ingetoetste code ('*shoulder surfing*'), door hacking of andere manieren worden de benodigde code bemachtigd.	V	e/n
Call selling fraud	Verkoop van telefoongesprekken met een hoog tarief (met name internationaal) zonder de intentie de ingekochte gesprekken te vergoeden. Bijvoorbeeld in belhuizen. Zo kan de exploitant van het belhuis na de eerste, forse telefoonrekening met de noorderzon vertrekken	V/m	n
Call transfer / call forwarding fraud	Door nummerdoorschakeling wordt een duur nummer (premium rate) aangeroepen. Kosten komen ten laste van partij die niet bewust is van deze doorschakeling	V/m	e
Dealer fraud	Vormen van misbruik en fraude door de wederverkoper. Voorbeelden zijn: - Klanten accepteren die de toelatingsprocedures niet zijn doorgekomen - Niet bestaande klanten activeren om commissies en bonussen op te strijken - Ten onrechte verzekerde toestellen als gestolen opgeven - Oude telefoons achterhouden bij vervanging of upgrading in plaats van ze terug te sturen naar de netwerkexploitant - Identificeren van klanten die niet willen upgraden (geen nieuw toestel) en daarna zonder medeweten van die klant op zijn of haar naam een toestel aanvragen.	v/m	n
Terminal insurance fraud	Ten onrechte beroep doen op de verzekering van een mobiele telefoon.	m	n
Spookabonnementen ('ghosting')	Door toegang tot support systems maakt een medewerker een account aan of modificeert een bestaand account; bijv. omzetten van een prepaid account naar een (onbetaald)	v/m	n

[132] Deze kolom geeft aan of deze fraudevorm (vooral) op vaste (v) of mobiele (m) netwerken voorkomt.

[133] Deze kolom geeft aan wie er primair schade leidt: de netwerkexploitant (n) of de eindgebruiker (e). Overigens kan het zijn dat door verzekeringen of coulance de schade die primair bij de eindgebruiker lag alsnog verschuiven naar de netwerkbeheerder.

	abonnement.		
Handset stock theft	Georganiseerde diefstal van grotere aantallen mobiele telefoons, met name tijdens het logistieke proces. De marktwaarde van dergelijke toestellen maken dit een reële bedreiging voor netwerkexploitanten. (Overigens is dit niet zonder meer een vorm van fraude)	m	n
Premium rate service fraud	Door het 'arrangeren' van oproepen naar deze duurdere servicenummers (zoals 0900-nummers) verkrijgt de service-aanbieder inkomsten.	v/m	e
Subscription fraud	Met een valse of vervalste legitimatie worden diensten afgenomen en niet betaald. Dit omvat ook het gebruik van katvangers die geen verhaal bieden als abonnees (mensen die op eigen naam een abonnement afnemen maar dat feitelijk direct overdoen aan een derde persoon – tegen betaling).	v/m	n
Voicemail hacking	Door inbreken of manipulatie in het voicemail systeem kunnen onbetaald gesprekken worden opgezet.	v/m	n
Voucher fraud	Het op manipulatieve wijze verkrijgen van het nummer dat op opwaardeerkaarten (vouchers) staat en waarmee aanspraak gemaakt kan worden op een beltegoed.	v/m	n
PABX-related fraud	Fraude door het hacken van bedrijfstelefooncentrales (PABX)	v/m	e
Teeing-in	Fraude doordat iemand fysiek toegang heeft verkregen tot de telefoonverbinding en daar (tijdelijk) een tweede toestel op heeft aangesloten.	v/m	e
Handset fraud	Aangekochte, gesubsidieerde prepaid mobiele telefoons ontdoen van de netwerkbeveiliging (sim-lock) en vervolgens verkopen tegen marktwaarde (overigens kan hierbij de vraag wordne gesteld of hier wel sprake is van fraude)	m	n
Marketing fraud	Fraude die gebruik maakt van (onbedoelde) mogelijkheden bij marketingacties	M	n
Prepaid fraud	Fraude door het manipuleren van het beltegoed bij prepaid-systemen. Vormen zijn: - Aflezen van codes op kraskaarten voordat die aan de uiteindelijke eindgebruiker worden verstrekt - Kraken van de algoritmen die de codes genereren voor kraskaarten of on-line opwaardeercodes - Het meelezen van opwaardeercodes bij de rechtmatige koper ('shoulder durfing') - Het muteren van de service class van prepaid gebruikers (door medewerkers van de exploitant of door hacking)	M	n/e
Roaming fraud	Het inzetten van een SIM-kaart in het buitenland voor dure diensten die vervolgens niet afgerekend worden. De SIM-kaart wordt verkregen door *subscription fraud* of door diefstal.	M	n
Text messaging fraud	Het door manipulatie gratis afnemen van betaalde content-diensten via SMS.	M	n
Mobile terminal cloning	Het bellen via een gekloonde mobiele telefoon/SIM kaart. Bij de oudere, analoge telefoons kwam deze vorm van fraude	m	n

	regelmatig voor. Bij GSM is dit lastiger. Hoewel het algoritme door experts niet als heel sterk meer wordt beschouwd[134], zijn alleen gevallen van cloning bekend waarbij de originele SIM nodig was (dus *niet* via het afluisteren van de radioverbinding).[135] Deze vorm kost veel moeite maar levert weinig op: de fraudeur is ook al in het bezit van de originele kaart, en het GSM-netwerken laten (indien correct ingesteld) geen identieke clonen toe.		
Hacking/cracking/ phreaking	Hacking betreft het toegang verkrijgen ('inbreken') door individuen in computersystemen. 'Hackers' doen dit normaliter voor de 'sport' of de 'lol', om te laten zien dat ze het systeem slimmer af zijn. 'Crackers' proberen door het vinden van een password of door het opheffen van de beveiliging software en systemen binnen te komen. Dit doen ze om er persoonlijk gewin uit te halen. 'Phreaking' is een specifieke categorie waarbij individueen er in slagen de werking van billingsystemen te beïnvloeden en zo gratis (internationale) gesprekken te voeren.	v/m	n/e
IMEI duplication	Het IMEI nummer is een uniek serienummer voor GSM-toestellen. Door dit nummer te veranderen kan alsnog gebeld worden met een toestel dat reeds op de zwarte lijst is geplaatst.[136] Het probleem is dat bij een aantal fabrikanten het nummer relatief gemakkelijk (softwarematig) veranderd kan worden. Criminelen gebruiken soms een zogenaamde 'IMEI thumbler', die een lijst van geldige IMEI codes kent en één ervan in het aangesloten toestel programmeert.	m	n
Social engineering	Een fraudeur doet zich voor als medewerker van de netwerkexploitant en weet bij medewerkers belangrijke gegevens zoals passwords van onderhouds- of configuratiesystemen los te krijgen.	v	n
Autodialers	Computerprogramma's die onbedoeld instellingen op een PC veranderen waardoor de gebruiker via het modem onbedoeld gaat bellen naar premium rate nummers met hoge tarieven. Deze programma's worden vaak in de vorm van virussen verspreid, of in een zodanige vorm gegoten dat de eindgebruiker niet echt door heeft wat de consequenties van de installatie ervan zijn. De fraudeur (en verspreider van de autodialer) is tevens exploitant van het genoemde premium rate nummer en verkrijgt zo inkomsten.	v	e

[134] Encryptie-experts stellen vaak dat de veiligheid van een systeem in de sleutels moet zitten, en het gebruikte algoritme daarbij gewoon in de openbaarheid gebracht moet kunnen worden. Dat is zelf wenselijk, aangezien de wetenschappelijke gemeenschap dan eventuele fouten of zwakheden kan opsporen en zo het algoritme kan verbeteren. Zo zijn veel bekende encryptie-algoritmen (zoals DES) door de makers openbaar gemaakt. De algoritmen bij GSM (A3, A5 en A8) worden echter door de makers geheim gehouden. (Elke netwerkbeheerder is overigens vrij een eigen algoritme te kiezen; in de praktijk nemen de meeste exploitanten echter het voorbeeldalgoritme klakkeloos over.) Encryptie-experts beschouwen de GSM-beveiling niet als uitzonderlijk sterk, maar vooralsnog voldoet het in het licht van haar rol en is het in ieder geval kosteneffectief.

[135] Zo is in 1998 het clonen van een SIM-kaart gedemonstreerd. Daarbij was overigens sprake van een netwerkexploitant die een wat korte sleutellengte hanteerde dan GSM toestaat (om te voldoen aan de in zijn land geldende regelgeving over maximale sleutellengten).

[136] Voor details, zie Bekkers & Smits (1999).

Internal fraud	Betreft fraude die (mede) door eigen medewerkers wordt gepleegd. Veel vormen van fraude zijn eenvoudiger te plegen indien er tot interne gegevens of systemen is verkregen. Het gaat bij interne fraude om fraudevormen die al hierboven zijn besproken, met name spookabonnementen, het muteren van de service class van prepaid abonnementen en handset stock theft.		
Misleidend advertenties	Klant wordt opgeroepen via belmachine om een 0900 nummer te bellen binnen 24 uur om zijn prijs binnen te halen. Ander voorbeeld: 'bel 090x voor gratis vakantie'.	v/m	e
Family fraud	Familiefraude: vader of moeder weten bijvoorbeeld van niets, maar de kinderen wel.	v/m	e

Bijlage 2. Fraudevormen bij betaaldiensten

Voor opmerkingen bij deze tabel zie paragraaf 7.3.

Fraudevorm	*Korte omschrijving*
Verloren/gestolen kaart	Een verloren of gestolen kaart wordt gebruik om betalingen mee te verrichten.
Vervalsing ('counterfeit')	Een nagemaakte kaart wordt gebruik om betalingen mee te verrichten.
Fraudulous application	Een kaart wordt onder valse identiteit aangevraagd en vervolgens gebruikt.
Account take-over	Een bestaande, bonafide account wordt zonder de klant dat weet 'overgenomen' door een fraudeur en misbruikt.
Merchant bust-outs	Een nieuwe onderneming meldt zich aan als organisatie die betalingen accepteert. Na het al dan niet onterecht innen van betalingen verdwijnt de fraudeur (merchant) met de noorderzon
Card-holder bust-outs	Een klant opent een rekening. Na de betaalkaart/creditcard in korte tijd intensief te hebben gebruikt verdwijnt de fraudeur (klant) met de noorderzon
Money-laundry	Een criminele organisatie opent een dienst (bijvoorbeeld het leveren van content). Vervolgens gebruikt hij zwart geld om deze dienst bij zichzelf te kopen. Bij anonieme kaarten is dan niet traceerbaar. Het 'ontvangen' geld is daarmee witgewast. Met name kansspelen zijn hier berucht: een groot verlies van de 'klant' is een grote winst voor de exploitant. Als 'klant' en exploitant dezelfde zijn is het geld witgewassen.
Gecompromitteerde account data	Ergens in de keten zijn gegevens van kaarthouders (kaartnummers, vervaldata) gelekt naar een derde partij. Dat kan zijn door afluisteren van een communicatiekanaal (o.a. 'wire tapping'), door inbraak in gegevensbestanden bij de betalingsontvanger, door een tijdelijk afgegeven kaart aan een kelner, etc. Deze data kan vervolgens worden gebruikt om 'card not present' betalingen te verrichten. In feite kan het lek bij elke partij in de waardeketen voorkomen die beschikt over gevoelige data. Bij card-not-present creditcard transacties bijvoorbeeld zijn er dat nogal wat. Vooral nieuwe toetreders, waaronder payment service providers, hebben in eerste instantie hun aandacht meer gevestigd op het succesvol uitrollen van een dienst dan op veiligheidsbeleid en veiligheidsmaatregelen. Ook hebben ze vaak een kennisachterstand op fraudegebied ten opzichte van de langer gevestigde partijen. Juist in dergelijke situaties kunnen risico's ontstaan.
Identity theft	Een individu wordt als target uitgekozen en de fraudeur gaat over lagere tijd allerlei persoonlijke informatie van dat individu verzamelen, inclusief abonnementen, hypotheek, verzekeringen (' snuffelen in de vuilnisbak'). Met deze informatie kan de fraudeur vervolgens langzaamaan de identiteit van die klant aannemen en onder zijn naam diensten afnemen of betalingstransacties verrichten. Deze vorm van fraude is daarmee een verbijzondering van de hierboven besproken, meer algemene categorie 'vervalsing'.
Cross-border fraude	Dit is geen fraudevorm op zichzelf, maar het toepassen van hierboven besproken vormen van fraude over de grens. Omdat er bij de verwerking van (betalings)gegevens uit het buitenland vaak enige vertraging ontstaat is wordt de fraude pas later opgemerkt en is het lastiger de fraudeur te vinden en aan te pakken.
Shoulder-surfing	De pincode of andere belangrijke gegevens achterhalen door mee te kijken tijdens een transactie bij een betaalautomaat.

Phishing	Phishing (een samenstelling van Password Harvesting Fishing) betreft het aan eindgebruikers ontfutselen van belangrijke gegevens als passwords en pincodes. Het gaat dus om vormen van misleiding. Dit gebeurt door een malafide partij die zich voordoet als een bank, operator of andere dienstverlener waar de klant een relatie mee heeft. Vroeger werd deze vorm door beveiligingsexperts afgedaan als de categorie 'stommiteiten van de eindgebruiker'. Tegenwoordig maken de fraudeurs echter gebruik van zodanig geavanceerde methoden dat zelfs een zeer oplettende klant niet door heeft wat er zich afspeelt.[137] De Anti-Phishing Working Group (zie www.antiphishing.org) geeft aan dat het aantal sterk toeneemt waarbij de gebruikte methodes steeds geavanceerder zijn.
Malafide merchant	Een winkel (of een medewerker daarvan) plaatst een kaartlezer vóór de feitelijke pinautomaat. Door tevens de pincode af te kijken (*shoulder surfing* of een slim opgestelde 'beveiligingscamera' vergaren ze voldoende gegevens om vervolgens een betaalkaart te klonen en succesvol te gebruiken.
Onterechte chargeback, of storneren of andere vorm van intrekking van de betaling	Sommige betaalsystemen, zoals 'card not present' creditcard betalingen en machtigingen, staan het klanten toe om de betaling terug te draaien. Deze mogelijkheid wordt geboden uit het perspectief van consumentenbescherming, omdat het systemen betreft waar het (voor de bank) niet altijd direct duidelijk is of de klant inderdaad de betalingstoestemming heeft verleend. Consumenten kunnen deze mogelijkheid ook misbruiken door een betaling te annuleren voor een transactie waarmee ze wel degelijk hebben ingestemd.
Interne fraude	Fraude door medewerkers, die bijvoorbeeld overboekingen aanmaken zonder daartoe geautoriseerd te zijn.

[137] Zo weten fraudeurs door het gebruik van veiligheidslekken in browsers en operating systems de gebruiker tijdens een reguliere sessie om te leiden naar eigen webpagina's (of formulieren door te sturen naar eigen webpagina's) terwijl de gebruiker nog steeds netjes de bankpagina's met de juiste URL bleef zien. Voor details, zie C'T, 'Uit vissen: Diefstal van wachtwoorden op internet wordt steeds geraffineerder', oktober 2004.

Bijlage 3. Mogelijke vormen van fraude bij mobiele betaaldiensten

Voor opmerkingen bij deze lijst zie paragraaf 7.3.

RE1	**Verloren/gestolen toestel/ongeautoriseerd gebruik** Het gebruik van een verloren of gestolen toestel voor betaaltransacties, Zoals ook nu al verloren/telefoons of verloren/gestolen creditcards misbruikt worden. Het risico hangt af van de gebruikte beveiliging. Bij onbeveiligde toegang naar bijv. premium rate nummers, premium rate SMS en contentdiensten of andere onbeveiligde betaaltransacties is er een risico. Bij transacties beschermt met pincode of wachtwoord alleen risico als de gebruiker daar onzorgvuldig mee omging (of als het systeem technische tekortkomingen zou kennen). Drager van het risico zal meestal de eindgebruiker zijn (originele houder telefoon en rekening). Bij wallet (zonder autoload) is risico beperkt tot de omvang van het nog uitstaande tegoed. Bij direct debit kan risico groter zijn. Risicoverdeling kan ook afhankelijk zijn van algemene voorwaarden en eventuele verzekeringen tegen deze situatie.
RE2	**Abonnementsfraude (telefonie); frauduleuze aanmelding (bankwereld)** Door het gebruik van valse of vervalste legitimatie worden diensten afgenomen maar niet betaald. Voorbeelden zijn: (1) gebruik van vals paspoort of andere identiteitspapieren, (2) aanvragen met overleggen van geldige identiteitspapieren maar die direct daarna doorverkopen (of onder dwang afgeven) aan fraudeurs, (3) online bestellen met valse adressen en (4) zakelijke abonnementen met vervalste KvK- papieren.
RE3	**Account take-over / identiteitsdiefstal** Een bestaande, bonafide account wordt zonder de klant dat weet 'overgenomen' door een fraudeur en misbruikt. Bij *identity theft* wordt een individu als doelwit uitgekozen en de fraudeur gaat over lagere tijd allerlei persoonlijke informatie van dat individu verzamelen, inclusief abonnementen, hypotheek, verzekeringen (' snuffelen in de vuilnisbak'). Met deze informatie kan de fraudeur vervolgens langzaamaan de identiteit van die klant aannemen en onder zijn naam diensten afnemen of betalingstransacties verrichten. Deze vorm van fraude is daarmee een verbijzondering van de hierboven besproken, meer algemene categorie 'vervalsing'.
RW1	**Merchant bust-outs** Een nieuwe onderneming meldt zich aan als organisatie die mobiele betalingen accepteert. Na het al dan niet onterecht innen van betalingen verdwijnt de fraudeur (merchant) met de noorderzon.
RW2	**Interne fraude** Fraude door personeel, zoals diefstal apparatuur of spookabonnementen.
RW3	**Witwassen (money-laundry)** Een criminele organisatie opent een dienst (bijvoorbeeld het leveren van content). Vervolgens gebruikt hij zwart geld om deze dienst bij zichzelf te kopen. Bij anonieme betaaltransacties (bijv. anoniem gekochte opwaardeerkaart op en anoniem aangeschafte prepaid telefoon) is dat niet traceerbaar. Het 'ontvangen' geld is daarmee witgewassen. Met name kansspelen zijn hier berucht: een groot verlies van de 'klant' is een grote winst voor de exploitant. Als 'klant' en exploitant dezelfde zijn is het geld witgewassen.
RW4	**Homepage masking (bijv. in i-Mode)** Dit is het aanbieden van een (web)locatie die eruitziet als een bonafide locatie van een bekende dienstaanbieder, zodat bezoekers betaling sturen aan een verkeerde rekening.
RW5	**Naamnummerkaping, naamnummerfraude**

	Het eerste fenomeen is vergelijkbaar met domeinnaamkaping (‘0900-Philips‘) om een domeinnaam voor veel geld te verkopen. Fraude is in dit geval buitengewoon lastig aan te tonen. Er zijn verschillende relaties tussen nummers aan namen. Daarnaast kan er anders dan bij domeinnamen sprake zijn van toeval. Belangrijkste criterium moet het gebruik van naamnummers zijn in advertenties etc. Zogenaamde naamnummerfraude (‘0900-Phillips’) is vergelijkbaar met typo squatting e.d. (www.phillips.com)
RW6	**Consumentenmisleiding** Klant wordt opgeroepen via belmachine om een 0900 nummer te bellen binnen 24 uur om zijn prijs binnen te halen. Ander voorbeeld: 'bel 090x voor gratis vakantie'.
RW7	**Foute afrekeningen en salamifraude** Bijvoorbeeld aan klant melden 0,8 euro te rekenen en feitelijk 1,1 euro rekenen. Zeker bij walletbetalingen is dit voor de klant zeer lastig te constateren. Salamifraude betreft afroming tot ver achter de komma.
TE1	**Teeing-in** Fraude doordat iemand fysiek toegang heeft verkregen tot de telefoonverbinding, de uitgewisselde gegevens meeluistert of zelf verkeer (transacties) genereert.
TE2	**Text messaging fraud** Het door manipulatie gratis afnemen van betaalde content-diensten via SMS of content-platforms.
TE3	**Mobile terminal cloning (telefonie); Vervalsing/‘counterfeit’ (bankwereld)** Het gebruik van gekloonde telefoons/authenticatiemodules (SIM etc.). Bij de oudere, analoge telefoons kwam deze vorm van fraude regelmatig voor, door de betere beveiliging bij GSM lijkt dit vooralsnog geen probleem te zijn. Onderdelen van de het stelsel van beveiligingen bij GSM zijn in het verleden gecompromitteerd. Experts uit de telecommunicatiewereld nemen doorgaans aan dat het systeem als geheel nog steeds afdoende bescherming biedt. Andere experts hebben echter wel hun twijfels of we er zeker van mogen zijn dat deze beveiliging ook het komende decennium sterk genoeg zal blijken. Daarbij speelt ook mee dat veel betaaldiensten hogere eisen stellen aan de sterkte van de authenticatie dan dat bij telefoniediensten het geval is.
TE4	**Gecompromitteerde account data** Ergens in de keten zijn gegevens van kaarthouders (kaartnummers, vervaldata) gelekt naar een derde partij. Dat kan zijn door afluisteren van een communicatiekanaal (o.a. ‘wire tapping’), door inbraak in gegevensbestanden bij de betalingsontvanger, door een tijdelijk afgegeven kaart aan een kelner, etc. Deze data kan vervolgens worden gebruikt om ‘card not present’ betalingen te verrichten. Ook het ‘hengelen van post’ (waaronder brieven waarin inloggegevens, pincodes of wachtwoorden voorkomen) vallen binnen deze categorie. In feite kan het lek bij elke partij in de waardeketen voorkomen die beschikt over gevoelige data. Bij *card-not-present* creditcard transacties bijvoorbeeld zijn er dat nogal wat. Met name nieuwe toetreders, waaronder payment service providers, hebben in eerste instantie hun aandacht meer gevestigd op het succesvol uitrollen van een dienst dan op veiligheidsbeleid en veiligheidsmaatregelen. Ook hebben ze vaak een kennisachterstand op fraudegebied ten opzichte van de langer gevestigde partijen. Juist in dergelijke situaties kunnen risico’s ontstaan.
TE5	**Phishing** Phishing (een samenstelling van Password Harvesting Fishing) betreft het aan eindgebruikers ontfutselen van belangrijke gegevens als passwords en pincodes. Het gaat dus om vormen van misleiding. Dit gebeurt door een malafide partij die zich voordoet als een bank, operator of andere dienstverlener waar de klant een relatie mee heeft. Vroeger werd deze vorm door beveiligingsexperts afgedaan als de categorie ‘stommiteiten van de eindgebruiker’. Tegenwoordig maken de fraudeurs echter gebruik van zodanig geavanceerde methoden dat zelfs een zeer oplettende klant niet door heeft wat er zich

[138] Zo weten fraudeurs door het gebruik van veiligheidslekken in browsers en operating systems de gebruiker tijdens een reguliere sessie om te leiden naar eigen webpagina’s (of formulieren door te sturen

	afspeelt.[138] De Anti-Phishing Working Group (zie www.antiphishing.org) geeft aan dat het aantal sterk toeneemt waarbij de gebruikte methodes steeds geavanceerder zijn.
TE6	**Malicious software ('Pacman-fraude', phone hacking, virusses, trojan horses)** Moderne mobiele telefoons hebben vaak een open platform/besturingssysteem waarvoor derde partijen applicaties kunnen schrijven. Een malafide partij kan hiervoor programmatuur schrijven met de bedoeling ongeautoriseerde betaaltransacties te verrichten of om bepaalde gegevens - zoals een pincode - te verzamelen ('malicious software'). Een dergelijk applicatie kan proberen gegevens aan de bonafide betaalapplicatie te ontfutselen of kan pogen verstuurde of ontvangen gegevens af te luisteren. Ook kan het programma zich op het scherm voordoen alsof het de echte betaalapplicatie is en zo onbedoeld de pincode in handen krijgen. Het kan hier ook om een virus gaan. (Noot: soms is deze categorie een verbijzondering van het hierboven beschreven *Phising,* namelijk wanneer malicious software wordt gebruikt om bepaalde gegevens los te krijgen van de eindgebruiker door misleiding).
TE7	**Remote phone hacking** Betreft het op afstand toegang verkrijgen tot het mobiele toestel en het inzien/wijzingen van gegevens of programmatuur. Hierbij wordt gebruik gemaakt van een draadloze verbinding zoals de reguliere radioverbinding, Bluetooth of WiFi. Zo hebben onlangs een groep Bluetooth-specialisten door het gebruik van high-gain antennes op een afstand van 1,7 km (!) contact kunnen leggen met mobiele telefoons. Vervolgens konden ze door gebruik te maken van diverse veiligheidslekken in bekende telefoontypes wijzigingen aanbrengen in gegevens (adresboeken, agenda's, visitekaartjes). Veel bekende GSM-telefoons hebben aanzienlijke veiligheidsgaten, die soms ook het ongeautoriseerd bellen (ook naar betaalnummers) mogelijk maken.[139]
TE8	**Denial-of-Service (DoS) attacks** Aanvallen met als doel om systemen plat te leggen, onder meer met behulp van strategieën als IP spoofing, smurf, SYN flood en buffer overflow (zie paragraaf 5.4).
TE9	**Sessieovername** Op diverse manieren kan een fraudeur proberen een bestaande (betaal)sesie over te nemen, waaronder het zogenaamde TCP Hijack. Maakt in de regel gebruik van het feit dat bij bepaalde evenementen (zoals handover of bepaalde routeringssituaties) geen nieuwe autorisatie vereist is. Niet goed afgesloten sessies kunnen door hackers worden opgespoord en verder gebruikt voor het sluiten van transacties.
TE10	**Aanval op systeemelementen en netwerkinterne processen** Door beveiligingsgaten in netwerkelementen als bijvoorbeeld de SGSN of GGSN. Met name roaming-interfaces zijn kwetsbaar door het ontbreken van security-aspecten in de norm.
TE11	**Misbruik bij reverse billing** Misbruik van systemen waarbij de eindgebruiker de ontvangen berichten betaald, bijvoorbeeld door het sturen van dubbele berichten.
TW1	**Fraude met inconsistente tariefstructuren** Bij inconsistente tariefstructuren, onder meer mogelijk bij betaalde content, kunnen exploitanten mogelijk geld verdienen door hun eigen dienst aan te roepen. Bij de huidige systemen kan het zo zijn dat een zeer korte aanroep (één seconde) naar een premium rate (0900)-nummer de exploitant van dat nummer meer inkomsten oplevert dan het de bellende partij kost. Een malafide gebruiker kan zo geld verdienen door zelf (geautomatiseerd) grote aantallen van dergelijke gesprekken per dag plaats te laten vinden. Omvang van het risico hangt onder meer af van de mate waarin dergelijke inconsistenties voorkomen. Verder hangt het af van de effectiviteit van fraudedetectie en van de maximale vergoedingen bij de betaalnummers.

naar eigen webpagina's) terwijl de gebruiker nog steeds netjes de bankpagina's met de juiste URL bleef zien. Voor details, zie C'T, 'Uit vissen: Diefstal van wachtwoorden op internet wordt steeds geraffineerder', oktober 2004.

[139] De aanval met als doel om onder meer adresboeken, agenda's en visitekaartjes te modificeren staat bekend onder de naam BlueSnarf. Voor een uitgebreidere beschrijving zie C'T, 'Aanval op Bluetooth-gsm met richtantenne', oktober 2004.

	Drager van het risico is in de regel de aanbieder van de betaaldienst (in geval van premium rate services dus de telecommunicatieaanbieder).
TW2	**Premium rate service fraud** Door het 'arrangeren' van afname van betaalde (content)diensten verkrijgt de service-aanbieder inkomsten. Dat arrangeren kan onder meer gebruik maken van ongeautoriseerde routing (o.a. doorverbinddiensten), en ghost dialers. Ook kan er sprake zijn van misleiding van klanten, het opwerpen van belemmeringen om abonnementen op premium SMS berichten op te heffen Fraude met premium rate nummers heeft inmiddels grote vormen aangenomen. In april 2004 besloot het Ministerie van Economische Zaken en het Openbaar Ministerie voor het aanpakken hiervan nauw samen te gaan werken de OPTA, de Bovenregionale Recherche Noord- en Oost- Nederland (BR NON), de Stichting Informatiedienstencode (Stic), de Nederlandse Vereniging van Informatiedienstaanbieders (NVI) en ICT Telecom.[140]
TW3	**Achterdeuren (back-doors)** De ontwikkelaar van (één van de) technische systemen heeft een ongedocumenteerde toegangsmogelijkheid tot het systeem ingebouwd. Deze kan worden gebruik om, zonder toestemming of medeweten van de bank of organisatie die deze systemen gebruikt, (betalings)gegevens op te halen of te muteren. Dergelijke back-doors kunnen zijn ingebouwd door een individu, een groep van individuen of door de (malafide) leverancier zelf, met als doel er later misbruik van te maken. Het kan echter ook dat een back-doors op persoonlijk initiatief door de softwareschrijver ingebouwd, bijvoorbeeld voor onderhouds- of controlewerkzaamheden, zonder de directe intentie om er misbruik van te maken of fraude te plegen. Deze persoon kan echter wel het slachtoffer van afpersing worden. Alleen al het feit dat hij geen (niet overeengekomen) back-door in had mogen bouwen brengt de softwareontwikkelaar in een chantabele positie. Back-doors blijken een probleem te zijn in verschillende sectoren. Zo is eerder geclaimed dat door de Nederlandse overheid in Israël aangeschafte systemen voor legaal aftappen onbedoeld van backdoors waren voorzien.[141]
RW4	**Autodialers** Computerprogramma's die onbedoeld instellingen op een mobiele telefoon veranderen waardoor de gebruiker onbedoeld premium rate services of betaalnummers/betaaldiensten afneemt. Deze programma's worden vaak in de vorm van virussen verspreid, of in een zodanige vorm gegoten dat de eindgebruiker niet echt door heeft wat de consequenties van de installatie ervan zijn. De fraudeur (en verspreider van de autodialer) is tevens exploitant van het genoemde premium rate nummer en verkrijgt zo inkomsten.

[140] Persbericht EZ, *Misbruik telefonische betaalnummers aan banden*, 19 april 2004.

[141] Paul Wouters, Patrick Smits, Dutch tapping room not kosher, c't Magazine, januari 2003.

Bijlage 4. Geïnterviewde personen en vragenlijst

Peter Loo / Bart Heinink	Orange
Hans Keijzer	Vodafone
Leonard Franken	ABN AMRO
Roland Uittenbogaard	DNB
Walter Hansen	Mastercard
Willem van de Berg	Maas International
Erwin Gerritsen / Richard van Erk	Interpay
Duco de Lange / André van Oudheusden	Neteconomy
Jeroen Schouten	KPN
Peter Potgieser	Interpay
Simon Lelieveldt / Edwin McGriffith	NVB
Willem de Jager	Rabobank

Vragenlijst bij het onderzoek 'Hoe criminelen de draad kwijtraken: Criminaliteitsgevoeligheidsanalyse mobiele telecommunicatie'

A. Introductie

1. Introductie van de gesprekspartners, korte schets van de activiteiten van het bedrijf / de organisatie

B. Wat zijn de belangrijkste nieuwe ontwikkelingen bij mobiele netwerken?

1. Belangrijkste *diensten*ontwikkelingen (met name gericht op consumenten)
    - Betalen (voor fysieke of elektronische goederen; lokaal of op afstand)
    - Toegevoegde-waardediensten, waaronder locatiegebonden diensten
    - Andere diensten
2. Belangrijkste *techniek*ontwikkelingen
3. Wat wordt verwacht van deze ontwikkelingen voor wat betreft consumentenadoptie van mobiel betalen? Welke penetratie zal worden gehaald? Vanaf wanneer?

C. Hoe worden deze ontwikkelingen vormgegeven?

1. Is uw bedrijf of organisatie actief bij de ontwikkeling van één van de hierboven bedoelde diensten? In welke status bevindt deze ontwikkeling zich? Wie zijn eventuele partners? Welk type marktpartijen spelen een minder belangrijke rol? Welke

brancheorganisaties of belangenorganisaties zijn relevant? Indien u zelf niet direct betrokken bent bij een project, maar wel kennis heeft over een project (bijvoorbeeld bij een andere organisatie) kunt u dat als uitgangspunt nemen.

2. Kunt u deze eigen ontwikkeling schetsen in het model van de waardeketen (bijgevoegd)?
3. Wat zijn de essentiële eigenschappen bij het project (vraag C-1)? (partijen, werkwijze, betalingsbeginselen (debit, credit, local, remote etc.)
4. Hoe ligt de precieze rol van de betrokken partijen (en vooral operators) bij de dat project? Zullen de telecommunicatieaanbieders zich transformeren tot een ander type dienstverlener?
5. Welke partij draagt de grootste risico's in relatie tot betalingstransacties? Betalen andere partijen een vergoeding voor dit risico?
6. Hoe verlopen de informatiestromen bij het systeem? Wie beheert welke informatie? Welke data wordt uitgewisseld (persoons- en klantgegevens, verkeersgegevens, authenticatiegegevens, locatiegegevens, transactiegegevens)?
7. Onder welk regelgevingregime vallen de verschillende deelnemers in het project (zoals de *financiële instelling*, of de *elektronische geldinstelling*)?
8. Wat is de eventuele relatie tot standaardisatietrajecten (zoals Mobile Payment Forum, Simpay, Mobey Forum, Mobile electronic Transactions (MeT) en PayCircle)? Wat zijn de verwachtingen bij deze trajecten?
9. Hoe ligt de relatie nationaal/internationaal? Is vanwege schaal een grote, grensoverschrijdende geharmoniseerde markt nodig (één enkel systeem) of zullen landen zoals nu nog gebruikelijk verschillende nationale invullingen aan hun betalingssystemen geven?
10. Welke andere initiatieven voor het ontwikkelen van vergelijkbare diensten zijn u bekend?

D. Wat is de huidige situatie met betrekking tot fraude bij reguliere mobiele telecommunicatiediensten? (niet m.b.t. mobiel betalen of toegevoegde-waardediensten)?

1. Hoe ernstig zijn de effecten? Wat zijn de trends? Hoe (effectief) worden de effecten bestreden?

E. Tot welke vormen van nieuwe fraude of criminaliteit zouden nieuwe technologische ontwikkelingen kunnen leiden?

1. Binnen diverse categorieën:
    - Fraude, bad dept of crimineel handelen bij de consument;
    - Crimineel handelen door (malafide) partijen in de waardeketen;
    - Fraude / crimineel handelen door derde partijen (niet de klant of een partij in de keten) (o.m. inbreken in het systeem of hacken);
    - Illegale handelingen binnen organisaties (door medewerkers).

F. Wat doen of voorzien partijen om risico's voor fraude en criminaliteit bij nieuwe ontwikkelingen te voorkomen?

1. Welke aanpak of procedures kunnen partijen inzetten om fraude/criminaliteit te voorkomen of te bestrijden?

2. In hoeverre bieden (parallelle) nieuwe technische ontwikkelingen ook *oplossingen* voor de bestrijding of preventie van de onderzochte vormen van criminaliteit

G. Wat is de status van het overheidsbeleid en het wettelijke instrumentarium?

1. Hoe kan het overheidsbeleid (nationaal, Europees) op dit gebied gekenschetst worden?
2. Is er wet- of regelgeving die als obstakel wordt gezien voor de voorspoedige ontwikkeling van mobiel betalen en andere nieuwe mobiele diensten?
3. Welke wetten en regels zijn nodig om nieuwe vormen van criminaliteit effectief te voorkomen en bestrijden? Op welk terrein bestaan eventuele lacunes in de wetgeving, vanuit de optiek van marktpartijen of vanuit de optiek van de overheid? Hoe kunnen deze gedicht worden? Kan buitenlandse wetgeving hierbij als voorbeeld dienen?

Slot

Tijdens een workshop zullen met name juridische elementen verder uitgediept worden. Is uw organisatie eventueel bereid deel te nemen aan die workshop, en welke persoon zou zich daar het beste voor lenen?

Bijlage 5. Deelnemers expertbijeenkomst

S. van den Broek	Ministerie van Financiën
M. Boots	Ministerie van Financiën
Dr. ir. L. Franken	ABN AMRO
B. Heinink	Orange
dr. mr. E.J. Koops	Universiteit van Tilburg
S. Lelieveldt	Nederlandse Vereniging van Banken
J. Schouten	KPN
R. Uittenbogaard	DNB
H. Zwijnenberg BSc	Ministerie van Economische Zaken

Wil Dessart	WODC
Rogier Rijpkema	Ministerie van Justitie
Rudi Bekkers	Dialogic
Frank Bongers	Dialogic
Maurice Schellekens	Universiteit van Tilburg
Jeroen Segers	Dialogic
Tiny van der Ven	Meetingminds

Bijlage 6. Overzicht initiatieven bij (mobiel) betalen

Mobiele telefonie gebaseerde initiatieven	
Digipay	NL
i-mode	NL
mobile2pay	NL
Moxmo	NL
Postbank mobiel bankieren	NL
vodafone v-live!	NL
M-Banxafe	Belgium
Mobile Payments Association	Czech Republic
m-Pay	Vodafone
Mobilhandel	Visa Norge and Telenor Mobil
Mobile Payment Services Association (MPSA) initiative	Orange, Telefonica, T-Mobile and Vodafone
Mobipay	Spain
Nokia	Dual chip
Nokia	RFID
Paybox	Germany

Internet initiatieven	
ABN amro e-wallet	NL
Bibit	NL
GlobalCollect van TPG	NL
Rabo Direct / Rabo internet machtiging / Minitix	NL
Secion	NL
Switchpoint modem/telefoon/mobile/ticket	NL KPN
Teletik Safepay	NL
Triple Deal	NL
TWYP ('The Way You Pay')	NL
Wallie	NL
Way2Pay	NL
wwwbon	NL
American Express Blue LockIT	American Express
Banxafe	Co-operation of Belgian Banks
1-Click	Amazon.com
Click&buy	FirstGate Internet US/Germany
Cybercash GmbH / Montrada	Dresdner Bank&Commerzbank
3D Secure and Verified by Visa	Visa
Digicash	
EMV	Europay/Mastercard/Visa
eps e-payment standard	four leading Austrian banks
MasterCard Secure Payment Architecture (SPA)	
Net900	German consultancy firm In Medias Res
Ogone	Belgian payment service provider
Paysafecard	four German and Austrian investment companie
SplashPlastic	UK
w-Ha	France Telecom

Specifieke oplossingen voor mobiel en internet betalen in het verkeer en vervoer	
MobilePay	NL
Noordned mobile ticketing	NL
Park-line mobiel betalen	NL
Translink	NL

Lijst met afkortingen

CDR	Call Detail Records; de informatie die bij elke communicatie in een (mobiel) netwerk wordt opgeslagen ten behoeve van de billing
CLI	Calling Line Identification; techniek achter de nummerweergave bij telefonie
DES	Data Encryption Standard; veelgebruikte encryptie algoritme. De sleutellengte is beperkt en hierom is DES te kraken; tegenwoordig wordt vaak drie DES algoritmes achter elkaar geschakeld (‘triple DES’)
ECBS	European Committee for Banking Standards
GGSN	Gateway GPRS Support Node; belangrijk netwerkelementen in een GPRS of UMTS network
GTP	GPRS Tunneling Protocol. Methode om gegevens te versturen in een GPRSA of UMTS netwerk
IMSI	International Mobile Subscriber Number; uniek, gestandaardiseerd nummer voor elke GSM kaart
MeT	Mobile electronic Transactions; forum dat een methode voor mobiel betalen ontwikkelt
MNO	Mobile Network Operator; exploitant van een mobile netwerk
MPF	Mobile Payment Forum forum dat een methode voor mobiel betalen ontwikkelt
MVNO	Mobile Virtual Network Operator; aanbieder van mobiele netwerkdiensten die de onderliggende capaciteit (deels) inkoopt bij een ander netwerk
PIN	Persoonlijk Identificatie Nummer
POS	Point of Sale; meestal doelend op een betaalterminal in een winkel o.i.d.
PRS	Premium Rate Service
SGSN	Serving GPRS Support Node; belangrijk netwerkelementen in een GPRS of UMTS network
SIM	Subscriber Idendity Module; unieke kaart behorend bij een mobile abonnement die in een mobiel toestel geplaatst wordt
SSL	Secure Socket Layer; methode om veilig (encrypted) gegevens via het internet te versturen
WiFi	Wireless Fidelity; populaire naam voor draadloze netwerken vorlgens de IEEE 802.11 familie van standaarden (officieel: certificaat dat de WiFi Alliance afgeeft aan producten die voldoen aan hun teststandaard)
WIM	Wireless Identification Module; als een SIM maar dan voor betaaltransacties
WODC	Wetenschappelijk Onderzoek- en Documentatiecentrum; Ministerie van Justitie

Geraadpleegde literatuur

Amersfoort P. van, L. Smit en M. Rietveld (2002) Criminaliteit in de Virtuele Ruimte. DSP groep en TNO/FEL in: Politie & Wetenschap. Politiekunde, nr. 1; 2002.

Asscher L.F. en A.H. Ekker (eds) (2002). Verkeersgegevens, een juridische en technische inventarisatie, Amsterdam: Cramwinkel.

Beinat E. (2001). Privacy and Location-based Services: Stating the Policies Clearly, Geoinformatics. September 2001.

Bekkers, R.N.A. & J.M. Smits (1999). GSM in detail: Techniek en realisatie van GSM, DCS 1800 en PCS 1900 [GSM in detail: Technology and implementation of GSM, DCS 1800, and PCS 1900]. Deventer, the Netherlands: Kluwer.

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

Buren R. van, S. Hille en R. van de Wetering (2002). Next Generation Scenario: Elektronisch betalen in Nederland. Telematica Instituut: Enschede.

Cools M. (2001). Billing in het 3G-tijdperk, in: ConneXie nr.5, 2001. p.58 ev.

Cools M. (2001). Telecommunicatiefraude - wie bepaalt wie betaalt? TNO-FEL-98-C131, Delft.

DNB (2003). Altijd en overal online betalen? Ontwikkelingen op het vlak van mobiel en internetbetalen. Kwartaalbericht September 2003.

Dommering E.J., N.A.N.M. van Eijk, J.A.M. Nijhof en M.L. Verberne (1999). Handboek Telecommunicatierecht. Inleiding tot het recht en de techniek van de telecommunicatie, Den haag: SDU.

ECB (2004). Electronic Payment Systems Observatory (ePSO). http://www.e-pso.info/.

European Central Bank (2003). electronification of Payments in Europe, ECB Monthly Bulletin mei 2003. p. 62 ev.

European Working Party on Information Technology Crime, Interpol (2001). Expert Statement. Overview of vital traffic data necessary for investigations, november 2001.

Europese Unie (2000). Richtlijn 2000/46/EG van het Europese Parlement en de Raad van 18 september 2000 betreffende de toegang tot, de uitoefening van en het bedrijfseconomische toezicht op de werkzaamheden van instellingen voor elektronisch geld.

Europol (2002). Expert meeting on cyber crime: Data retention. Europol verkeersgegevens wensenlijst. april 2002.

Evans D.S. & R. Schmalensee (2000). Paying with Plastic: The digital revolution in buying and borrowing. ISBN 0262550377. Massachusetts: The MIT Press.

G8 (2002). Principles on the Availability of Data Essential to Protecting Public Safety. Verklaring over een bewaarplicht. mei 2002.

G8 Government-private sector high-level meeting on high-tech crime (2001) Potential Consequences for Data Retention of Various Business Models Characterizing Internet Service Providers. Tokyo. May, 22-24, 2001.

Gururajan R. (2002). New Financial Transaction Security Concerns in Mobile Commerce, in: Information & Security. Volume 8, Number 1, 2002.

Heffernan S. (1996). Modern Banking in Theory and Practice. ISBN: 0-471-96209-0. Wiley.

Hes R. (2002). Verkeersgegevens in nieuwe generatie telecommunicatiesystemen. In L.F. Asscher en A.H. Ekker (eds) (2002). Verkeersgegevens, een juridische en technische inventarisatie, Amsterdam: Cramwinkel.

Hooper M. (2001). Billing the 3G extravaganca, in: Telecommunications International, September 2001, p.77.

Huitema G.B. (2002) Van de nota een deugd maken, verrekening van telecommunicatie- en informatiediensten vanuit klantperspectief. Oratie uitgesproken ter aanvaarding van de functie hoogleraar aan de Rijksuniversiteit Groningen. 26 november 2002: Academiegebouw Groningen.

Infodrome (2000). Vragen voor de overheid in het informatietijdperk.

Instituut voor Informatierecht (2002). Workshop 'Verkeersgegevens', een juridische en technische inventarisatie. IVER. 6 september 2002.

Jong F.W. de (2004) Thema elektronische transacties - Digitaal factureren, in: IT-Monitor : ontwikkelingen, achtergronden en trends op het gebied van bestuurlijke informatiekunde, automatisering en informatica (2004) nr.4 p.8-9 (2 refs.).

Kelly P. (2004) InDepth: Service Assurance Market Outlook 2004-2007. New investments in service assurance will be targeted at the service layer. in: OSS Observer, July 2004: Illinois.

Klaauw-Koops F.A.M. Van der & J.E.J. Prins (2002), Internationale privacyregulering: belangen, problemen en mogelijkheden, in: J.E.J. prins en J.M.A. Berkvens, Privacyregulering in theorie en praktijk, Deventer: Kluwer, p. 497 – 501.

Koops B.J. (1999). The Crypto Controversy: A Key Conflict in the Information Society. Den Haag: Kluwer Law International. 301 p. ISBN 90 411 1143 3.

Lahteenmaki J. (2003). Cellular network optimisation based on mobile location. IST project report. VTT Information Technology. Technical Research Centre of Finland. IST-2000-25382-CELLO.

Lelieveldt, S. (2003). "De telecommunicatiesector als 'nieuwe' aanbieder", *Bank- en Effectenbedrijf*, december, pp. 19-21.

Luiijf H.A.M. & M.H.A. Klaver (2000) Bitbreuk; De kwetsbaarheid van de ICT-infrastructuur en de gevolgen voor de informatiemaatschappij. Geschreven voor de workshop Kwetsbaarheid Informatienetwerken. Infodrome: Amsterdam.

Lynch D.C. & Lundquist, L. (1996). Digital Money: The New Era of Internet Commerce. New York: John Wiley and Sons.

M.L van Lankeren (2003). Call selling Fraude. Landelijk Expertisecentrum Telecommunicatiefraude.

Maatschappelijk Overleg Betalingsverkeer (2004). Betalen kost geld: Rapport kostenonderzoek toonbankbetaalproducten.

Mac-Gillavr E. (2000) Meewerken aan strafvordering door banken en internet service providers. Onderzoek uitgevoerd door de vakgroep Strafrecht en Criminologie van de Rijksuniversiteit Groningen in opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum van het ministerie van Justitie (WODC).

Martens A., B. Meelhuysen, P. Nieuwenhuis en B. Nieuwenhuis (2003). Betalen via nieuwe media. Onderzoek uitgevoerd door LogicaCMG & Hypercube in opdracht van het Ministerie van Economische Zaken: Den Haag/Utrecht.

Ministerie van Verkeer en Waterstaat (2003). Plaatsbepaling in mobiele communicatienetwerken. Zie: http://www.radionavigatie.nl.

Niemeijer E., J. Nijboer e.a. (1999). Informatisering van de samenleving en criminaliteit. Themanummer Tijdschrift voor criminologie, jaargang 1999/4.

Norman S. (2002). M-commerce, Technologies, Services and Business Model. Institute for eCommerce. Carnegie Mellon University.

Nwaike A. (2001). Telecommunications Billing, Revenue leakage and fraud risks.

Phillips A. (1987). The Role of Standardization in Shared Bank Card Systems in: H. L. Gabel, Product Standardization and Competitive Strategy, pp. 263-73, Amsterdam: Elsevier.

Rommelse F., Zwarte lijsten. Belangen en effecten van waarschuwingssystemen, Achtergrondstudies en Verkenningen 4, http://www.cbpweb.nl/downloads_av/AV04.pdf?refer=true&theme=green.

Schudelaro T. (2003). Electronic Payment Systems and Money Laundering. Risks and Countermeasures in the Post-Internet Hype Era, Nijmegen: Wolf legal Publishers.

Stiegelis M., J. Nube & B. Wijn (2002) M-payments. Overzicht van succesfactoren van M-payment in de Nederlandse markt.

Stol W.Ph., R.J. van Treeck, A.E.B.M. van der Ven (1999). Criminaliteit in Cyberspace. Een praktijkonderzoek naar aard, ernst en aanpak in Nederland. Studie door In-pact Onderzoeksteam in opdracht van het WODC. Elsevier bedrijfsinformatie B.V.

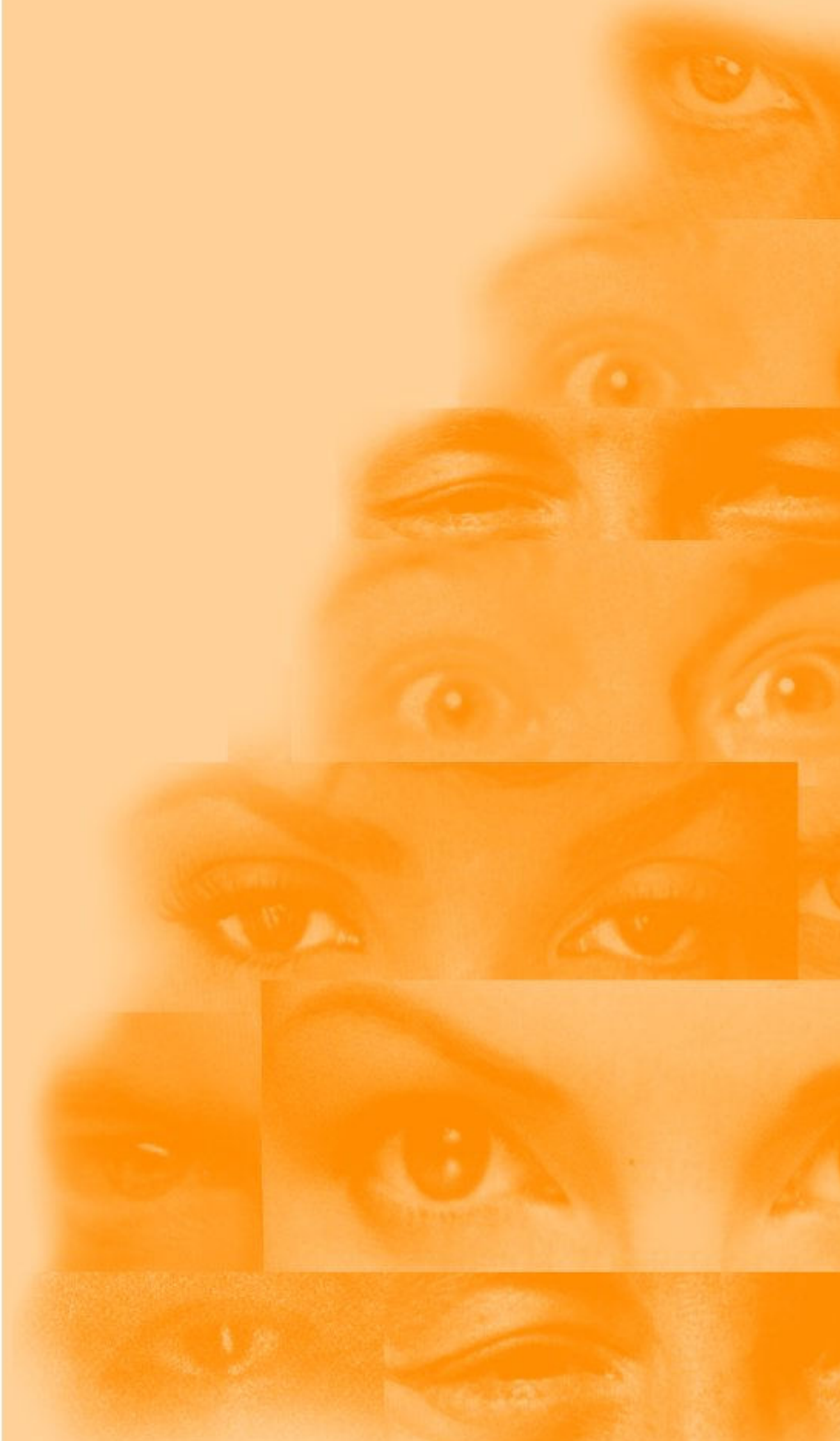
Stratix (2003). Bewaren Verkeersgegevens door Telecommunicatieaanbieders. Studie in opdracht van het WODC. Schilhil: Auteur.

Telematica Instituut (2002). Next Generation Scenario; TIbetaal: Electronisch betalen in Nederland. Den haag: EZ.

TNO (2000). De invloed van Application Service Provision op het telecommunicatiebeleidsveld, TNO rapport gemaakt in opdracht van het Ministerie van Verkeer en Waterstaat, Directoraat-generaal Telecommunicatie en Post.

Van Traa-team (2003). "Verkeerd verbonden? Belhuizen in Amsterdam". Amsterdam: Gemeente Amsterdam, Directie Openbare Orde en Veiligheid.

Werkgroep regelgeving aanpak telecommunicatie en –misbruik. Ministerie van Justitie. http://www.minjust.nl/b_organ/npc/informat/sitc_wg_regelgeving.htm.



Wilhelminapark 20
3581 ND Utrecht
Tel +31 30 2150580
Fax +31 30 2150595
info@dialogic.nl
www.dialogic.nl