Rapportage
Veiligheid Betaalproducten

Pinpas en Incasso

Mei 2003

De Nederlandsche Bank OBV/2003/00145

INHOUDSOPGAVE

1 SAMENVATTING

Naar aanleiding van een verzoek van de Minister van Financiën heeft de Nederlandsche Bank (de Bank) een onderzoek uitgevoerd naar de veiligheid van de betaalproducten die het meest in de belangstelling hebben gestaan in 2002, de pinpas en incasso. Samen maken deze twee producten 68% van het totale aantal transacties in het elektronisch retailbetalingsverkeer uit.

Het onderzoek is gericht op fraude-incidenten die zich met genoemde producten in 2002 hebben voorgedaan. De risico's die zich bij de betreffende fraudegevallen hebben gemanifesteerd zijn destijds bij de invoering van de producten grotendeels onderkend en daarvoor zijn maatregelen getroffen. In reactie op de incidenten heeft het bankwezen aanvullende maatregelen genomen. De Bank heeft de bevindingen en aanbevelingen uit het onderzoek voorgelegd aan de Nederlandse Vereniging van Banken. De reactie van de banken is in onderhavige rapportage verwerkt.

De Bank is van oordeel dat met betrekking tot het product pinpas de bestaande maatregelen aangevuld met recente acties door de banken vooralsnog toereikend zijn om de veiligheid daarvan in voldoende mate te garanderen. De Bank zal niettemin de ontwikkelingen op dit gebied nauwgezet blijven monitoren omdat de praktijk leert dat technologische ontwikkelingen het eenvoudiger maken om ongeautoriseerd magneetstripgegevens van pinpassen te kopiëren en de bijbehorende pincodes te achterhalen. Opgemerkt wordt dat het tot nu toe niet is gelukt de versleuteling van de pincode te kraken.

Ten aanzien van het betaalproduct incasso is de Bank in zijn algemeenheid van oordeel dat de bestaande maatregelen, aangevuld met recente acties door de banken, vooralsnog toereikend zijn om te waarborgen dat de schade door incasso fraudes zo beperkt mogelijk blijft. In de praktijk komt deze schade voor rekening van de banken. Verder is de Bank van oordeel dat met betrekking tot de beoordeling van incassanten en incasso-opdrachten de banken in opzet voldoende aanvullende maatregelen hebben geïnitieerd om het risico van onterechte incasso's zo klein mogelijk te houden. Teneinde een veilig betalingsverkeer in een e-business omgeving te bevorderen is de Bank van oordeel dat op korte termijn productvoorwaarden opgesteld moeten worden voor incasso op basis van Internetmachtigingen respectievelijk dat algemene richtlijnen voor toegang tot betaalrekeningen worden ontwikkeld en bekend gemaakt. Thans bestaan zulke voorwaarden en richtlijnen niet terwijl incidenteel toch incasso op basis van Internetmachtigingen plaatsvindt. Dit is een onwenselijke situatie en leidt tot onduidelijkheid in de markt. Inmiddels zijn voorstellen voor dergelijke productvoorwaarden interbancair onderhanden en zullen deze aan de Bank worden voorgelegd zodra ze gereed zijn.

De beoordeling door de Bank heeft als uitgangspunt dat 100% veiligheid in de praktijk niet haalbaar is en veiligheid een gezamenlijke verantwoordelijkheid is van alle betrokken partijen (banken, retailers en consumenten). Wel dient binnen de gegeven mogelijkheden en rekening houdend met efficiency een zo hoog mogelijke veiligheid te worden nagestreefd. Daarnaast is voor de beoordeling van de veiligheid van pinpas en incasso meegewogen de relatief geringe totaalomvang van de fraudes en de verdeling van het financiele risico tussen de banken, retailers en consumenten. De Bank is van mening dat de door haar gevolgde werkwijze bijdraagt aan het bevorderen van een betrouwbaar betalingsverkeer en zal ook andere betaalproducten onderzoeken op veiligheidsaspecten.

2 INLEIDING

In november 2002 heeft de Minister van Financiën de Nederlandsche Bank (de Bank) verzocht een rapportage op te stellen over de veiligheid van het betalingsverkeer (zie bijlage 1). Dit naar aanleiding van fraude incidenten met de betaalproducten pinpas en incasso die zich in de loop van 2002 hebben voorgedaan. Doel van het verzoek was na te gaan of de veiligheid van het betalingsverkeer verder zou kunnen worden verbeterd en, zo ja, een advies op te stellen over mogelijkheden tot verbetering van de veiligheid.

Om aan het verzoek te voldoen heeft de Bank een onderzoek verricht naar de veiligheid van de betaalproducten pinpas en incasso. Deze twee producten nemen samen ruim 68% van het totale aantal transacties in het elektronisch retailbetalingsverkeer voor hun rekening[1].

Het onderzoek heeft plaatsgevonden binnen het kader van de werkzaamheden die de Bank verricht op het gebied van oversight van het betalingsverkeer. In hoofdstuk 3 worden deze werkzaamheden kort beschreven en wordt in algemene zin ingegaan op de veiligheid van betaalproducten. In de hoofdstukken 4 en 5 wordt op hoofdlijnen ingegaan op de uitkomsten van het uitgevoerde onderzoek. Daarbij wordt allereerst het betreffende betaalproduct beschreven. Daarna wordt ingegaan op de aard en omvang van de onderzochte incidenten. Vervolgens is geanalyseerd welke maatregelen zijn, respectievelijk worden genomen om de geïdentificeerde risico's te mitigeren.
De bevindingen en aanbevelingen uit de onderzoeken zijn voorgelegd aan het bankwezen via de Nederlandse Vereniging van Banken en de reactie van de banken is verwerkt in de onderhavige rapportage.

1 Bron: DNB Kwartaalbericht maart 2003

3 VEILIGHEID BETAALPRODUCTEN

3.1 **Oversight op het betalingsverkeer**

Op basis van het EG-verdrag en de Bankwet is de Bank verantwoordelijk voor het bevorderen van de goede werking van het betalingsverkeer in Nederland. Dit omvat onder andere het uitoefenen van een specifieke vorm van toezicht op het betalingsverkeer, oversight[2] genaamd. In dat kader worden door de Bank op reguliere basis toetsingswerkzaamheden verricht op betaalsystemen, effectenafwikkelsystemen en betaalproducten. Voor de onderhavige studie is laatstgenoemde categorie relevant. De Bank volgt de ontwikkelingen op het gebied van betaalproducten, aangezien het niet goed functioneren van een betaalproduct kan leiden tot verstoringen in het financiële stelsel en het economische verkeer; ook zou het vertrouwen van het publiek in het Nederlandse betalingsverkeer kunnen worden geschaad. Ook in een aantal andere landen van de EMU vervullen centrale banken een rol in het oversight op betaalproducten.

3.2 **Gevolgde aanpak bij het oversight op de betaalproducten pinpas en incasso**

In het algemeen wordt bij het oversight op betaalproducten door de Bank het beginsel gehanteerd van een zo veel mogelijk ongestoorde en vrije marktwerking. Uitgangspunt daarbij is dat de betrokken marktpartijen in principe worden geacht steeds in staat te zullen zijn tot het ontwikkelen en het in continuïteit aanbieden van betrouwbare en veilige betaalproducten. In de praktijk hoeft dit echter niet altijd het geval te zijn. Indien de veiligheid en betrouwbaarheid van betaalproducten in het geding komen, bijvoorbeeld blijkend uit een toenemend aantal fraudegevallen, kan de Bank, met in achtneming van het beginsel van vrije marktwerking, aanbevelingen ter verbetering opstellen. Het bestaande wettelijke kader voorziet evenwel niet in de mogelijkheid voor de Bank om aanbevelingen dwingend te kunnen opleggen.

Het oversight op betaalproducten is enerzijds gericht op het volgen van relevante *nieuwe* ontwikkelingen die mogelijk een belangrijke invloed kunnen hebben op de goede werking van het betalingsverkeer (zoals bijvoorbeeld bij mobiel bankieren het geval is), anderzijds betreft dit het analyseren van de adequate werking van *bestaande betaalproducten*, voor zover deze van materieel belang kunnen zijn voor de goede werking van het betalingsverkeer. Bij het vaststellen van de prioriteit waarmee betaalproducten worden getoetst, wordt uitgegaan van een risico analyse. Daarnaast is het optreden van incidenten een factor die van invloed is op de te stellen prioriteiten. Opgemerkt mag worden dat in de Nederlandse praktijk zich hierbij doorgaans geen grote problemen voordoen. Wel heeft zich in 2002 een stijging van het aantal incidenten ten aanzien van de betaalproducten pinpas en incasso voorgedaan ten opzichte van 2001.

---

[2] Dit is de internationaal gebruikelijke term. Zie ook de brochure *Oversight op systemen in het betalings- en effectenverkeer*, 2002, De Nederlandsche Bank N.V., http://www.dnb.nl

3.3 **Gehanteerde definitie van veiligheid**

Bij het beoordelen of een betaalproduct veilig is dient te worden bedacht dat veiligheid maar tot op zekere hoogte objectiveerbaar is. Zoals hiervoor vermeld wordt de veiligheid van een product getoetst aan de hand van een risico analyse. Daarenboven is veiligheid een subjectief begrip, gerelateerd aan de perceptie van het publiek. Naarmate het vertrouwen van het publiek in betaalproducten groter is, mag worden gesteld dat de gepercipieerde veiligheid groter is. Daarnaast heeft elk betaalproduct zijn eigen veiligheidskenmerken die niet los kunnen worden gezien van de functionaliteit van het betreffende product. De relevante vraag is derhalve wanneer een product voldoende veilig[3] is. Deze vraag laat zich in de praktijk niet eenvoudig beantwoorden maar het is evident dat er voor alle betrokken partijen een op een risico analyse gebaseerde evenwichtige verhouding dient te zijn tussen de verantwoordelijkheden, restrisico´s en kosten. Een 100% veiligheidsniveau is in de praktijk evenwel niet haalbaar, in dat geval zouden de kosten van het desbetreffende product economisch gezien namelijk prohibitief kunnen worden danwel zouden de functionaliteit of het gebruiksgemak zodanig negatief worden beïnvloed dat het niet meer door het publiek geaccepteerd zou worden. Wel dient evenwel binnen de beschikbare mogelijkheden een zo hoog mogelijk veiligheidsniveau te worden nagestreefd.

De beveiligingsmaatregelen in en rondom betaalproducten bestaan uit technische en organisatorische maatregelen. Een goede werking van deze maatregelen is afhankelijk van een juiste toepassing ervan door zowel de banken als bedrijven (zoals toonbankinstellingen) en consumenten. Een goede veiligheid is dus een gezamenlijke verantwoordelijkheid van alle betrokken partijen omdat elke partij hieraan kan bijdragen. Bij een te laag veiligheidsniveau worden de risico's op fouten en fraude groter en daar gaan maatschappelijke kosten mee gepaard die (uiteindelijk) door alle partijen gedragen worden.

De banken hebben in hun reactie op de uitgevoerde onderzoeken (zie verderop) bevestigd dat zij een zo veilig en efficiënt mogelijk betalingsverkeer nastreven en dat zij ver gaan in het nemen van verantwoordelijkheid om bijvoorbeeld fraude te voorkomen en te bestrijden. Recent is het Maatschappelijk Overleg Betalingsverkeer (MOB) ingesteld waarin diverse maatschappelijke partijen zijn vertegenwoordigd zoals de banken, retailers en consumenten[4]. Het aspect veiligheid van het betalingsverkeer is in het MOB belegd in een aparte werkgroep, waardoor veiligheidsaspecten een breder draagvlak kunnen krijgen.

---

[3] Vanuit oversight perspectief betekent voldoende veilig dat minimaal aan een aantal beveiligingseisen wordt voldaan. Deze eisen kunnen variëren per betaalproduct.

[4] De Bank heeft met betrekking tot het MOB een faciliterende rol.

4 ONDERZOEK PINPAS

4.1 **Kenmerken betaalproduct pinpas**

4.1.1 *Productbeschrijving*

Een pinpas is een door de uitgevende instelling (bank) aan de houder verstrekte pas die tezamen met een persoonlijk identificatie nummer (pincode) geschikt is voor gebruik in geautomatiseerde systemen in het betalingsverkeer. Het verschaft de houder aldus langs elektronische weg direct toegang tot zijn betaalrekening. Met dit betaalproduct kan via geldautomaten (GEA´s) geld worden opgenomen van de eigen bankrekening en kunnen in winkels via betaalautomaten (BEA´s) aankopen worden betaald.

De pinpas is geïntroduceerd in 1982 met aanvankelijk een beperkte werking, namelijk opname van geld in GEA´s bij de eigen bank van de pashouder. In 1985 werd gastgebruik (opname bij andere banken dan de eigen bank) mogelijk voor de bij de Bankgirocentrale aangesloten banken en in 1997 heeft ook de Postbank zich bij het gastgebruik aangesloten. In 1985 zijn proeven gestart met het betalen via de pinpas in betaalautomaten. In 1988/89 is het BEAnet ontstaan waarbij één (landelijke) interbancaire infrastructuur is ingevoerd.

In de jaren negentig is het mogelijk geworden de bankpas in het buitenland te gebruiken bij geld- en betaalautomaten, door aan te sluiten bij het internationale betaalsysteem Maestro. In tegenstelling tot het nationale betaalsysteem is het bij Maestro mogelijk bij bepaalde betaalautomaten te betalen zonder gebruik te maken van de pincode. Daarbij dient de houder van de pas de door de betaalautomaat verstrekte transactiebon te ondertekenen. Bij gebruik van geldautomaten in het buitenland is de pincode wel steeds verplicht (evenals bij gebruik van zowel geld- als betaalautomaten in het binnenland, conform de initiële opzet van de pinpas[5]).

4.1.2 *Aansprakelijkheid / financieel risico*

Conform de Voorwaarden Bankpas en de Voorwaarden Gebruik Geld- en Betaalautomaten is in geval van verlies, diefstal, misbruik of vervalsing van een pinpas de klant tot een bedrag van € 150 aansprakelijk voor de gevolgen van onbevoegd gebruik vanaf het moment van verlies of diefstal van de pas tot het moment van melding hiervan aan de bank. Deze aansprakelijkheid kan worden verhoogd tot het totale bedrag van de onbevoegde transacties indien de bank kan aantonen dat deze onbevoegde transacties hebben kunnen plaatsvinden doordat de klant zijn verplichtingen ten aanzien van het zorgvuldig omgaan met de pinpas en de pincode, niet heeft nageleefd. Conform afspraken tussen de Nederlandse Vereniging van Banken (NVB) en de Consumentenbond is de hiervoor genoemde aansprakelijkheid beperkt tot € 45 voor misbruik bij

[5] De productnaam van de pinpas in Nederland is PIN, zoals opgenomen in het bijbehorende logo.

bankpastransacties waarbij gebruik van de pincode niet vereist is (uitsluitend op bepaalde locaties in het buitenland).
Bij incidenten waarbij kan worden aangetoond dat de klant slachtoffer is geworden van een fraudezaak (doorgaans omdat meerdere meldingen betrekking hebben op het gebruik bij één bepaalde automaat, een zogenaamd common point of purchase) wordt de schade van de klant voor het totale bedrag door de bank vergoed.

4.2 **Incidenten in 2002**

4.2.1 *Soorten incidenten*

In het onderzoek zijn negen typen incidenten met de pinpas nader bezien. In alle gevallen ging het om fraudes door criminelen waarbij op verschillende manieren te werk werd gegaan:

- onderschepping van bankpassen die per post onderweg naar de rekeninghouders waren;
- gebruik van gestolen en geblokkeerde passen;
- verwisseling van pasjes bij kaartautomaten NS stations;
- kopiëren van pasjes in restaurants;
- kopiëren van pasjes bij betaalautomaten bij bemande tankstations;
- kopiëren van pasjes bij betaalautomaten bij onbemande benzinepompen;
- kopiëren van pasjes via mobiele betaalautomaten;
- kopiëren van pasjes bij geldautomaten;
- kopiëren van pasjes via deurlezers van ruimtes waarin zich geldautomaten bevinden.

Opgemerkt wordt dat van het totale aantal incidenten waarbij een pashouder schade claimt wegens (vermeend) misbruik van zijn pas, een deel van deze claims onterecht blijkt vanwege vergissingen of fraude door de pashouder zelf of door diens familieleden. In dit onderzoek zijn dergelijke incidenten buiten beschouwing gelaten.

4.2.2 *Omvang schade*

Het totaal aantal passen dat bij de negen onderzochte incidenten betrokken was, bedroeg bij benadering 800. De totale schade beliep circa 2 miljoen euro (variërend van 25.000 euro tot 1 miljoen euro per type incident). Hoewel deze schade in absolute zin niet onaanzienlijk is, dient te worden bedacht dat ten opzichte van het totale gebruik van de pinpas de schade relatief gering is. Er staan in Nederland circa 20 miljoen bankpassen uit waarmee in totaal via betaalautomaten in winkels ruim 50 miljard euro werd betaald in 2002 (via 1,07 miljard transacties). Daarnaast zijn met de pinpassen circa 500 miljoen opnames uit geldautomaten verricht ter waarde van 50 miljard euro.

4.3 **Manifestatie van risico's**

Bij de onderzochte incidenten hebben de volgende risico's (of combinaties daarvan) zich gemanifesteerd:

A. het stelen van originele passen;
B. het ongeautoriseerd lezen en kopiëren van magneetstripgegevens;
C. het op enigerlei wijze bekend worden van de pincode bij een ander dan de houder van de pas;
D. het omzeilen van de pincode (bij handtekening gebaseerde betalingen in het buitenland).

Uit de uitgevoerde analyse is naar voren gekomen dat deze risico's reeds in het verleden door de banken zijn onderkend[6] en dat destijds maatregelen zijn genomen. Bovendien wordt met betrekking tot risico C opgemerkt dat het tot nu toe niet is gelukt de versleuteling van de pincode te kraken. Het bemachtigen van de pincode vindt plaats door bijvoorbeeld over de schouders mee te kijken (shouldering), via miniatuurcamera´s af te kijken of via neptoetsenborden (pinpad overlays) te registreren. De bestaande maatregelen, tezamen met het specifieke risico (A t/m D) waarop de maatregel is gericht, zijn weergegeven in box 1.

4.4 **Maatregelen**

Om de veiligheid van (het gebruik van) de pinpas en pincode verder te vergroten, zijn in aanvulling op de in box 1 beschreven maatregelen door de banken de volgende maatregelen genomen respectievelijk onderhanden. Bij deze maatregelen is aangegeven op welke specifieke risico's uit de vorige paragraaf deze maatregelen gericht zijn.

<u>Voorlichting consumenten (C)</u>

In aanvulling op de normale voorlichting van de consumenten is met een herhaling van de campagne (en brochure) *Pinnen: hou het veilig* door de banken inmiddels intensiever de aandacht gevestigd op veilig gebruik van de pinpas. Deze brochure bevat nu ook een oproep aan de consument om verdachte omstandigheden bij een betaalautomaat te melden bij een landelijk meldnummer en dergelijke omstandigheden bij een geldautomaat te melden bij de betreffende bank.

<u>Verzending van de passen (A, D)</u>

Er vindt intensief overleg plaats met TPG Post om vast te stellen welke (extra) maatregelen genomen kunnen worden om diefstal van originele passen in het postale traject tegen te gaan.

---

6 Met betrekking tot de pinpas was tijdens de uitvoering van het onderzoek geen integrale interbancaire risicoanalyse beschikbaar. Ten behoeve van het onderzoek zijn de risico´s geïnventariseerd uit diverse documenten. Door de Raad van Advies van Interpay is inmiddels besloten een integrale Risicoanalyse Cards op te laten stellen.

Fraudedetectie / monitoring (A, B, C, D)

Door de banken is besloten om in het tweede kwartaal van 2003 fraudedetectie van (gastgebruik) transacties in te voeren. Deze maatregel beoogt tijdig te signaleren dat van een normaal patroon afwijkende transacties plaatsvinden. De consument kan dan door de banken pro-actief gewaarschuwd worden.

Box 1. Bestaande maatregelen mbt pinpas, betaal- en geldautomaten.

Voorlichting consumenten (C, D)

Eén van de belangrijkste maatregelen om misbruik van een pinpas te voorkomen, is de toepassing en geheimhouding van de pincode. In Nederland is het gebruik van de pinpas bij zowel geldautomaten als betaalautomaten niet mogelijk zonder pincode. De pashouder wordt er op gewezen dat hij zorgvuldig met de pincode dient om te gaan en deze niet aan derden mag verstrekken.

Verzending van de passen (A, D)

Voorbeelden van maatregelen van (individuele) instellingen tegen (de gevolgen van) diefstal van originele passen uit het postale traject zijn het versturen via Safe Mail of Brief met Legitimatie en het geheel of gedeeltelijk (voor buitenlandgebruik) geblokkeerd verzenden van passen.

Versleuteling pincodes (C)

De pincode wordt niet opgeslagen op de magneetstrip en om het aftappen van pincodes te voorkomen worden deze vanaf het moment van intoetsen versleuteld.

Handtekening indien gebruik zonder pincode mogelijk is (D)

Het gebruik van de pinpas bij buitenlandse betaalautomaten is vaak mogelijk zonder gebruik van de pincode. Daarbij dient, conform internationale afspraken, de houder van de pas de door de betaalautomaat verstrekte transactiebon te ondertekenen (signature-based transacties).

Certificering betaalautomaten (B)

Betaalautomaten dienen te voldoen aan interbancair opgestelde beveiligingseisen. Hierop worden de automaten getoetst en gecertificeerd. Deze certificering is met name gericht op de veiligheid van de pincode respectievelijk de in het pinpad aanwezige cryptografische sleutels. Eén van de eisen die aan betaalautomaten wordt gesteld is dat deze *tamper responsive* moeten zijn. Dat wil zeggen dat een automaat buiten werking treedt zodra er mee gemanipuleerd wordt.

Richtlijnen voor plaatsing betaalautomaten (B, C)

Richtlijnen met betrekking tot het plaatsen van betaalautomaten is een maatregel die er op gericht is dat het niet mogelijk is voor anderen om mee te kijken tijdens het intoetsen van de pincode. Een extra hulpmiddel tegen het afkijken is het verplichte privacy shield (beschermkapje) bij betaalautomaten. Daarnaast beoogt deze maatregel het risico tegen te gaan dat magneetstripgegevens bij het gebruik van de pinpas in betaalautomaten ongeautoriseerd kunnen worden gelezen. De plaatsing van betaalautomaten moet zodanig zijn dat de pashouder zijn pas niet hoeft af geven (of tenminste niet uit het oog hoeft te verliezen) zodat deze niet ongemerkt gekopieerd wordt.

Beveiligingseisen voor geldautomaten (B, C)

Evenals dat voor betaalautomaten het geval is, zijn beveiligingseisen opgesteld voor geldautomaten. Deze eisen, zoals fysieke eisen aan de verschillende onderdelen (pinpad, kaartlezer, geldvergaarbak, etc.) en eisen met betrekking tot pinmanagement, zijn er op gericht te waarborgen dat de pashouder zijn pinpas en de pincode kan gebruiken in een veilige automaat zonder het risico te lopen dat zijn pasgegevens gekopieerd worden of zijn pincode wordt bemachtigd.

Verplicht gebruik pincode bij betaalautomaten in het buitenland (D)

Op een vraag van de Bank of het gebruik van de pincode bij alle betaalautomaten in het buitenland verplicht is te stellen, is door de banken aangegeven dat dat niet éénzijdig mogelijk is. De Nederlandse banken hebben van meet af aan onderkend dat het toestaan van signature-based transacties mogelijk enigszins verhoogde financiële en reputatierisico's zou meebrengen en hebben zich in het internationale overleg – tevergeefs - verzet tegen het toestaan van deze

faciliteit. Het toestaan van signature-based transacties werd gezien als een belangrijke voorwaarde om kritische massa voor Maestro te realiseren. En dat werd ook als een belang voor de Nederlandse pashouder gezien omdat deze met Maestro in het buitenland elektronisch zou kunnen betalen en geld kan opnemen. Belangrijke overweging van de Nederlandse banken om zich niet van de internationale gemeenschap af te zonderen, was bovendien dat de snelle verbreiding van Maestro als voorwaarde werd gezien voor de wens om de Eurocheque en Girobetaalkaart uit te faseren en daarmee de inmiddels fors opgelopen chequefraude terug te brengen en uiteindelijk geheel uit te bannen.
De banken hebben toegezegd het standpunt van de Bank (gebruik pinpas altijd in combinatie met pincode) nogmaals ter kennis te brengen van Mastercard Europe in Brussel en er opnieuw op aan te dringen dat Maestro signature-based zo snel mogelijk volledig wordt vervangen door pin-based transacties. Aangegeven is dat de invloed van de Nederlandse banken in de internationale besluitvorming in deze beperkt is.

Zolang met de Maestro functionaliteit in het buitenland nog signature-based transacties uitgevoerd kunnen worden, zou de klant kunnen kiezen voor een pinpas zonder Maestro functionaliteit. Daarmee maakt hij een bewuste keuze voor een beperkte functionaliteit. Op de aanbeveling van de Bank om de klanten intensiever voor te lichten over de risico's van het product Maestro en over de keuzemogelijkheden, is door de banken aangegeven dat het "onnodig" wijzen op de risico's van een product het imago van het product kan schaden, terwijl de klant veel profijt kan hebben van het product. Daarnaast wordt de schade altijd vergoed als de klant niets te verwijten valt (bijvoorbeeld bij skimming[7] en vervolgens gebruik met vervalste handtekening) en is diens eigen risico dus verwaarloosbaar. Vanuit de klant gezien levert het product Maestro dus geen extra risico op en geldt, zoals eerder aangegeven, bij misbruik op basis van een handtekening zelfs een lager eigen risico dan bij gebruik van een pincode. Daarnaast is aangegeven dat de pashouder bewijstechnisch niet in een nadeliger positie wordt gebracht bij een transactie zonder dan bij een transactie met pincode.
Overigens wordt door sommige banken wel specifiek ingegaan (bijvoorbeeld op hun website) op extra maatregelen om de fraude met betalingen zonder pincode tegen te gaan.

<u>Overstap van magneetstrip naar chip (B)</u>
Een mogelijke maatregel om de veiligheid van de pinpas te vergroten is de overstap van magneetstrip naar (EMV) chip. Of dit een adequate oplossing is tegen de huidige fraudetechnieken kan pas beoordeeld worden als deze maatregel verder is uitgewerkt en in kaart is gebracht wat de voor- en nadelen zijn (zowel voor de banken, de retailers als de consumenten). Naar het zich laat aanzien is echter in elk geval de migratie van magneetstrip naar chip geen

goedkope en geen korte termijnoplossing. Dit onderwerp wordt zowel in interbancair verband als in het Maatschappelijk Overleg Betalingsverkeer geadresseerd. Ook in Europees verband staat dit punt hoog op de agenda.

Aanvullende eisen voor onbemande betaalautomaten (B, C)

Interbancair zijn inmiddels aanvullende beveiligingseisen vastgesteld voor onbemande betaalautomaten (buitenpalen, met name bij benzinestations) die per 1 maart 2003 van kracht zijn geworden en verplicht zijn voor alle nieuwe automaten. Voor de bestaande automaten is een tijdpad afgesproken om deze te vervangen. Totdat dit is gebeurd, is met de branche afgesproken dat pomphouders intensieve controles op deze apparaten uitvoeren.

Richtlijnen voor plaatsing betaalautomaten (B, C)

Inmiddels is de controle op naleving van deze richtlijnen voor plaatsing betaalautomaten aangescherpt. Verder worden de consumenten er middels de brochure “Pinnen: hou het veilig” op gewezen goed op de omgeving te letten en is zeer recent een centraal meldpunt bij Interpay ingericht waar verdachte situaties rond betaalautomaten gemeld kunnen worden.

GEA beveiligingseisen / certificering (B, C)

Naar aanleiding van een aanbeveling van de Bank hebben de banken aangegeven dat het *tamper responsive* maken van geldautomaten (buiten werking treden na manipulatie) technisch erg moeilijk is omdat bij de meeste fraudezaken sprake is van externe manipulatie van de automaat (skimmingapparatuur die over de pasgleuf wordt geplaatst). Door goede voorlichting aan de consument kan hier hoogstens een zekere mate van *tamper evident* worden bereikt, dat wil zeggen dat de consument kan zien dat er gemanipuleerd is. Sommige typen geldautomaten zijn wel tamper responsive voor de meer eenvoudige fraudevormen zoals de Libanese lus[8] en sommige banken plaatsen voorzetmonden om het plaatsen van skimmingapparatuur te bemoeilijken. De leveranciers van geldautomaten en de banken blijven gezamenlijk zoeken naar mogelijkheden om de geldautomaten zo veilig mogelijk te maken. Inmiddels is een taskforce bezig om, evenals dat voor de betaalautomaten gebeurt, ook een interbancaire GEA certificering uit te werken voor geldautomaten.

Deurlezers (B)

Sommige geldautomaten zijn geplaatst in een ruimte die voorzien is van een deur die geopend kan worden door de bankpas van de rekeninghouder door een lezer te halen. Gebleken is dat deze

---

[7] Skimming is het “afromen” van pinpasgegevens door deze te lezen (bijvoorbeeld via een gemanipuleerde of compleet valse geld- of betaalautomaat of via een separate magneetstriplezer) om deze gegevens vervolgens te kopiëren op een nieuwe pas.

[8] Deze techniek bestaat uit het plaatsen van een vals mondstuk op de kaartlezer waarbij de pinpas in een fysieke lus achter dit mondstuk terecht komt en de consument de pas niet meer terug krijgt na invoering. Vervolgens wordt de consument door een zogenaamde behulpzame voorbijganger geadviseerd nogmaals de pincode in te toetsen waarna de

lezers gemanipuleerd kunnen worden en dat via deze weg pasgegevens ongeautoriseerd kunnen worden gelezen. Interbancair is afgesproken dat dergelijke deurlezers moeten worden verwijderd en om de geldautomaten en omgeving dagelijks te controleren op onregelmatigheden.

4.5 **Oordeel**

De Bank is van oordeel dat met betrekking tot het product pinpas de bestaande maatregelen (zie box 1) aangevuld met recente acties door de banken (zie paragraaf 4.4) vooralsnog toereikend zijn om de veiligheid daarvan in voldoende mate te garanderen. Voor deze oordeelsvorming is meegewogen de relatief geringe totaalomvang van de fraudes en het feit dat de schade door de banken wordt gedragen (verantwoordelijkheidsverdeling). De Bank zal niettemin de ontwikkelingen op dit gebied nauwgezet blijven monitoren omdat de praktijk leert dat technologische ontwikkelingen, zoals steeds kleinere miniatuurcamera´s en handzamer skimmingapparatuur, het eenvoudiger maken om ongeautoriseerd magneetstripgegevens van pinpassen te kopiëren en de bijbehorende pincodes te achterhalen. Opgemerkt wordt dat het tot nu toe niet is gelukt de versleuteling van de pincode te kraken.

voorbijganger of zijn handlanger door afkijken de pincode kan achterhalen. De consument krijgt zijn pasje niet terug en zodra deze is vertrokken kan de fraudeur de pas bemachtigen en gebruiken met de afgekeken pincode.

5 ONDERZOEK INCASSO

5.1 **Kenmerken betaalproduct incasso**

5.1.1 *Productbeschrijving*

In 1960 is het automatisch incasso in Nederland geïntroduceerd. Sinds 1972 bieden vrijwel alle banken het interbancaire girale betaalproduct incasso in het retailbetalingsverkeer aan. Incasso is een betaalproduct waarmee de begunstigde een bedrag van de rekening van debiteuren (consument of bedrijf/instelling) naar zijn rekening laat overschrijven. De begunstigde neemt hiertoe het initiatief. Alleen bedrijven en instellingen kunnen als begunstigde een incassocontract met hun bank sluiten. De debiteur[9] dient vooraf expliciet toestemming te geven voor een incasso, door middel van een ondertekend machtigingsformulier[10]. De incassant dient zelf van iedere debiteur een dergelijke machtiging te verkrijgen en te administreren.

De incassanten leveren de incasso-opdracht bij hun bank of rechtstreeks bij Interpay aan op fysieke media zoals tape of cartridge of door gebruik te maken van datacommunicatie. De verwerking van aangeleverde incasso-opdrachten vindt plaats bij Interpay. De Postbank verzorgt zelf de verwerking van incasso-opdrachten binnen het eigen rekeningendomein en levert alleen de interbancaire incasso´s ter verwerking bij Interpay aan.

Er zijn verschillende soorten incasso´s. De meest bekende en gebruikte zijn de *automatische* incasso (of ook wel doorlopende machtiging), speciaal ontwikkeld voor betalingen met een repeterend karakter en de *éénmalige* incasso. De éénmalige incasso wordt ook gebruikt als alternatief betaalproduct bij toonbankbetalingen indien door een storing het gebruik van online betaalproducten (zoals de pinpas) niet mogelijk is.

Een belangrijke overweging voor de incassant voor het veelvuldig gebruik van dit betaalproduct is de efficiënte verwerking (en daarmee de lage maatschappelijke kosten) van massale periodieke betalingen en de snelle creditering van zijn rekening. Voor de consument is dit betaalproduct aantrekkelijk omdat het geen actie vraagt na de verstrekking van een machtiging en de consument in een aantal gevallen het efficiencyvoordeel van dit betaalproduct (deels) krijgt doorberekend.

5.1.2 *Aansprakelijkheid / financieel risico*

Het product automatische incasso is voor een groot deel gebaseerd op de vertrouwensrelatie tussen de incassant en zijn bank. Het is namelijk de incassant die de betreffende betaalopdrachten

9 Een debiteur kan zowel een consument zijn als een bedrijf of instelling.

10 Dit is tot op de heden de belangrijkste incassovariant. Sinds 1 juli 2002 bestaat ook de telefonische machtiging waarbij het vereiste van de schriftelijke machtiging is vervangen door strikte contract- en procedureafspraken met (bepaalde) incassanten.

genereert ten behoeve van zijn eigen rekening, terwijl het de bank van de incassant is die, in geval de debiteur de betaling betwist, de debiteur schadeloos stelt.

Het product incasso is voor de debiteur veilig omdat deze geen direct financieel risico loopt. Bij een onterechte transactie via een incasso-opdracht wordt de transactie na verzoek daartoe van de debiteur altijd teruggedraaid indien het verzoek binnen de gestelde termijn van 1 jaar (gerekend vanaf de datum van overboeking) is gedaan. De debiteur loopt wel een (beperkt) indirect financieel risico aangezien de liquiditeitspositie op korte termijn kan worden aangetast. Dit is het geval indien door een frauduleuze transactie een rekening ten onrechte wordt gedebiteerd en een volgende terechte betaaltransactie geen doorgang zou kunnen vinden vanwege een saldotekort of een overschrijding van de kredietlimiet.

5.1.3 *Omvang schade*

In het kader van de uitgevoerde onderzoek zijn gegevens over schadegevallen met incasso's opgevraagd bij een aantal banken. Daaruit komt naar voren dat er in 2002 een aantal gevallen van misbruik van incassocontracten van enige omvang is geweest. Bij de bevraagde banken zijn in totaal zo'n 20 gevallen bekend met een totaal potentieel schadebedrag voor deze banken van zo'n 15 miljoen euro. Begrepen is voorts dat de feitelijke schade aanzienlijk geringer is. Dit komt doordat de banken van de incassant, na ontdekking van misbruik, correctieve acties hebben ondernomen om de financiële schade te beperken, onder andere door het terugboeken van frauduleuze transacties en het blokkeren van rekeningen die gebruikt zijn voor het collecteren hiervan. De feitelijke schade vermindert hierdoor doorgaans met meer dan 90%. Uit de ontvangen cijfers van de bevraagde banken blijkt voorts dat in 2002 de feitelijke schade per bank maximaal 0,002 promille van het bedrag bedraagt dat jaarlijks met een incasso door die bank wordt overgeboekt. Inmiddels zijn er ruim 120.000 incassocontracten. In 2002 zijn ongeveer 990 miljoen transacties verricht met een waarde van 186 miljard euro.

5.2 **Incidenten in 2002**

In het kader van het uitgevoerde onderzoek zijn twee verschillende typen incidenten met incasso´s nader onderzocht.

<u>Misbruik bestaand contract</u>

Eén type incident betrof misbruik van een bestaand incassocontract door het inzenden van valse incasso opdrachten. Bij het onderzochte voorbeeld bleken incasso opdrachten te zijn verzonden zonder dat de rekeninghouder (geïncasseerde) hiervoor toestemming had gegeven. Door gebruik te maken van zijn bestaand incassocontract zijn door de betreffende fraudeur van bestaande rekeningen bedragen geïncasseerd zonder dat voor deze rekeningen incassomachtigingen waren verstrekt.

Onduidelijkheid en misbruik van Internetmachtigingen

Een andere groep van incidenten betrof klachten bij het gebruik van éénmalige machtigingen bij betalingen via Internet. De klacht was dat het bij aankopen op een website onvoldoende duidelijk is voor een klant dat, nadat zij een bankrekeningnummer en een accordering van een bedrag op Internet hebben ingevoerd, de verkopende partij een éénmalige incasso uitvoert. Daarnaast zijn er in enkele gevallen klachten dat een hoger bedrag geïncasseerd is dan waarvoor toestemming zou zijn gegeven, of dat ten onrechte meerdere malen afboekingen zijn uitgevoerd. Over specifieke gegevens ten aanzien van aantallen transacties die het zou betreffen en de potentiële fraude omvang beschikt de Bank niet.

5.3 **Manifestatie van risico's**

Onterechte / frauduleuze incasso-opdrachten

Zowel bij het type incident van misbruik van een bestaand contract als bij de Internetmachtigingen heeft zich een risico gemanifesteerd dat reeds in het verleden door de banken is onderkend in een interbancaire risico analyse. Het gaat hierbij om het risico dat onterechte (frauduleuze) incasso-opdrachten worden uitgevoerd door incassanten. Dit kan bijvoorbeeld door fictieve incasso opdrachten te genereren, door incasso's te genereren voor een hoger bedrag dan de machtiging van de debiteur aangeeft danwel door vaker incasso-opdrachten aan te maken dan de betreffende machtiging van de debiteur aangeeft. Voor dit risico hebben de banken in het verleden reeds maatregelen opgesteld (zie box 2).

Box 2. Bestaande maatregelen mbt incasso´s.

Beoordeling incassant.

Een belangrijke maatregel van banken om het risico van misbruik van een bestaand contract te mitigeren, is het beoordelen van de betrouwbaarheid van de incassant en van de financiële positie van de incassant voordat een contract wordt afgesloten.

Schriftelijke machtigingen.

Een maatregel met betrekking tot de rechtmatigheid van een incasso transactie is de verplichting voor de incassant om een schriftelijke machtiging van de betreffende debiteur te hebben.

Controle door debiteur / storneringsprocedure.

Een maatregel om onterechte incasso-opdrachten te ontdekken en te corrigeren is de controle door de debiteur op de juistheid van zijn afboekingen en de melding binnen een jaar aan zijn bank met het verzoek om een stornering (terugstorting) indien een naar zijn mening onterechte incasso heeft plaatsgevonden.

Onbewust afgeven machtiging

Bij de groep van incidenten betreffende de onduidelijkheid bij Internetmachtigingen heeft zich een nieuw risico voorgedaan, namelijk dat een consument een machtiging afgeeft zonder dat hij zich daarvan bewust is. Dit wordt mede veroorzaakt doordat gebruik wordt gemaakt van machtigingen via het Internet terwijl de randvoorwaarden hiervoor nog niet zijn uitgewerkt. Door de banken is aangegeven dat zij steeds nadrukkelijk hebben gecommuniceerd dat interbancair slechts twee machtigingsvarianten zijn geaccordeerd, namelijk de schriftelijke en de telefonische, zodat een incassant die via Internet machtigingen werft, bij betwisting in beginsel altijd zelf het financiële risico loopt. Immers een "Internetmachtiging" wordt door de banken niet als bewijs geaccepteerd wanneer de debiteur de transactie betwist.

5.4 **Maatregelen**

In aanvulling op de in box 2 beschreven bestaande maatregelen zijn door de banken de volgende aanvullende maatregelen genomen respectievelijk in uitwerking.

Beoordeling incassant.

Voor het beoordelen van de betrouwbaarheid van de incassant en van zijn financiële positie zijn aangescherpte interbancaire richtlijnen voor acceptatiecriteria voor incassocontracten opgesteld. Deze richtlijnen zijn recent door de NVB als dringende aanbeveling gecommuniceerd naar alle banken. Daarnaast worden momenteel interbancaire richtlijnen opgesteld voor het periodiek screenen van incassanten met lopende incassocontracten.
Recent is een interbancair sanctiebeleid afgesproken met betrekking tot het niet nakomen van de verplichtingen door de incassant.

Schriftelijke machtigingen.

De maatregel dat de incassant verplicht is om voor iedere incasso een schriftelijke machtiging van de betreffende debiteur te hebben werkt niet preventief, omdat binnen de huidige afspraken en werkwijzen met betrekking tot incasso de banken en Interpay geen zicht hebben op het aanwezig zijn van machtigingen (bij de incassant) en geen controle kunnen uitvoeren op het aanwezig zijn van (geldige) machtigingen voordat zij de incasso opdrachten ter verwerking bij Interpay aanbieden respectievelijk verwerken.
Om te voorkomen dat incasso-opdrachten worden geaccepteerd waaraan geen schriftelijke machtiging ten grondslag liggen waar dat wel contractueel is voorgeschreven, zouden banken vooraf moeten controleren of machtigingen inderdaad schriftelijk zijn afgegeven. Inherent aan de opzet van het betaalproduct incasso en aan de productvoorwaarden is echter dat dit pas achteraf kan worden vastgesteld indien een transactie door een debiteur wordt betwist. Indien dit vooraf zou moeten plaatsvinden, dient een compleet centraal machtigingenbestand te worden opgezet en

onderhouden waartegen elke transactie vóór verwerking preventief wordt getoetst. De banken hebben aangegeven dat een dergelijke maatregel[11] kostbaar is en alleen op lange termijn ingevoerd zou kunnen worden als dit doelmatig zou blijken te zijn op grond van een kosten/batenanalyse.

Controle door debiteur / storneringsprocedure.

Ten aanzien van de controle door de debiteur op de afboekingen van zijn rekening constateert de Bank dat de effectiviteit van deze controle enerzijds verzwakt is doordat banken minder vaak bankafschriften verzenden, anderzijds dat de mogelijkheden om frequenter te controleren toegenomen zijn door telebankieren en internetbankieren. De Bank is van mening dat debiteuren regelmatig gewezen dienen te worden op hun verantwoordelijkheid om deze controle uit te voeren.

De banken onderzoeken in het tweede kwartaal van 2003 op welke wijze de procedure "Melding Onterechte Incasso" gebruikersvriendelijker gemaakt kan worden. Bovendien wordt met de Stichting Ombudsman besproken op welke wijze een centrale klachtenprocedure over het gedrag van incassanten zou kunnen worden opgezet.

Plausibiliteit opdrachten

Vanaf november 2003 zal een deel van de incassoposten dagelijks door Interpay worden geanalyseerd op patroonsafwijkingen. Verder worden momenteel onderzoeken uitgevoerd, gericht op maatregelen voor de langere termijn, waaronder een online realtime detectiesysteem bij Interpay voor incasso. Bij deze onderzoeken wordt de mogelijkheid van een centrale interbancaire "zwarte lijst" meegenomen.

Europese incasso

In het kader van de realisatie van de Single Euro Payment Area (SEPA) wordt door de Europese banken gewerkt aan een Europees incassosysteem (pan-european direct debit system). Het ligt in de bedoeling dat dit nieuwe systeem tezijnertijd alle binnenlandse incassosystemen in de landen in de Eurozone zal vervangen. Dat betekent dat de Nederlandse banken het nemen van maatregelen voor de thans geldende Nederlandse systemen nu al in dat perspectief beoordelen. De centrale banken in het Eurosysteem zullen zich tezijnertijd buigen over de beveiligingseisen voor een dergelijk Europees incassosysteem.

Internetmachtigingen

Rondom de internetmachtigingen zijn nog geen interbancaire maatregelen afgesproken. Inmiddels zijn wel voorstellen gedaan om te onderzoeken op welke wijze machtigingen via een e-business internetomgeving van voldoende waarborgen kunnen worden voorzien om deze op een

[11] Deze potentiële maatregel was reeds door de banken en Interpay opgenomen in de interbancaire risico analyse.

gelijksoortige wijze als controlemogelijkheid te accepteren als een schriftelijke machtiging. Mogelijke oplossingen daarvoor zijn elektronische handtekeningen en bevestigingen via beveiligde verbindingen of het opstellen van richtlijnen waarin centraal staat op welke wijze en onder welke omstandigheden toegang tot een betaalrekening kan worden verkregen. De concrete uitwerkingen zullen met de Bank worden besproken.

5.5 **Oordeel**

Incasso is een veel gebruikt en efficient betaalproduct. Omdat het voor een groot deel gebaseerd is op de vertrouwensrelatie tussen de incassant en zijn bank, is het belangrijk dat het imago met betrekking tot de veiligheid van dit product bij de consument goed blijft. Duidelijk is dat in de markt ook een sterke behoefte bestaat om dit product ook via andere kanalen te kunnen gebruiken zoals bijvoorbeeld via het Internet.

Veiligheid incasso

Ten aanzien van de schriftelijke machtigingen is de Bank van mening dat de banken een verantwoordelijkheid hebben om vast te stellen dat hun incassanten beschikken over schriftelijke machtigingen van de debiteuren van deze incassanten. De Bank kan zich vinden in het besluit van de banken dat een andere systeemopzet voor de incasso, waarbij de boeking van incasso-opdrachten zou worden voorafgegaan door toetsing aan een centrale database met machtigingen, ten koste zou gaan van de maatschappelijke efficientie en te kostbaar is om op korte termijn in te voeren. De Bank gaat er daarbij wel van uit dat periodiek geëvalueerd wordt of de kosten/batenanalyse voor betrokken partijen zodanig wijzigt dat de maatregel alsnog ingevoerd dient te worden. Bij de uitwerking van het Europees incasso product is een machtigingendatabase om transacties vooraf te verifiëren een maatregel die overwogen dient te worden. De European Payments Council heeft in het kader van deze pan-Europese incasso een task force belast met het uitwerken van dergelijke aspecten.

Met betrekking tot de beoordeling van incassanten en incasso-opdrachten is de Bank van mening dat de banken in opzet voldoende aanvullende maatregelen hebben geïnitieerd om het risico op onterechte incasso´s zo klein mogelijk te houden. Of deze maatregelen voldoende effect sorteren zal tezijnertijd beoordeeld moeten worden.

De Bank is van mening dat de bestaande maatregelen, aangevuld met recente acties door de banken, vooralsnog toereikend zijn om te waarborgen dat de schade door incasso fraudes voor consumenten en banken zo beperkt mogelijk blijft.

Incasso via Internet

Teneinde een veilig betalingsverkeer in een e-business omgeving te bevorderen is de Bank van oordeel dat op korte termijn productvoorwaarden opgesteld moeten worden voor incasso op basis van Internetmachtigingen respectievelijk dat algemene richtlijnen voor toegang tot betaalrekeningen worden ontwikkeld en bekend gemaakt. Thans bestaan zulke voorwaarden en richtlijnen niet terwijl incidenteel toch incasso op basis van Internetmachtigingen plaatsvindt. Dit is een onwenselijke situatie en leidt tot onduidelijkheid in de markt. Inmiddels zijn voorstellen voor dergelijke productvoorwaarden interbancair onderhanden en zullen deze aan de Bank worden voorgelegd zodra ze gereed zijn.

Bijlage 1. Brief Minister van Financiën

ministerie van Financiën

Directie Financiële Markten

Dr. A.H.E.M. Wellink
De Nederlandsche Bank NV
Postbus 98
1000 AB Amsterdam

Datum	Uw brief (Kenmerk)	Ons kenmerk	Inlichtingen
- 6 NOV. 2002		FM 2002-1492 M	Mr.dr.drs J.F.Koers T 070-3428993 F 070-3427984 E j.f.koers@minfin.nl

Onderwerp
Verzoek tot rapportage over de veiligheid van het betalingsverkeer

Naar aanleiding van recente incidenten rond bijvoorbeeld automatische incasso's, pinbetalingen en internetbankieren wil ik u verzoeken op korte termijn een rapportage op te stellen over de veiligheid van het betalingsverkeer. Daarbij verwijs ik ook naar mijn brief aan de Tweede Kamer van 25 oktober jongstleden over de vermeende veiligheidsrisico's van incasso-machtigingen, waarvan u een kopie vindt bijgevoegd. Op ambtelijk niveau is hierover met uw medewerkers reeds contact geweest.

Doel van mijn verzoek is na te gaan in hoeverre de veiligheid van het betalingsverkeer verder kan worden verbeterd. Mochten uit dit onderzoek of uit het reguliere toezicht knelpunten naar voren komen, dan verzoek ik u te adviseren over mogelijkheden om te bewerkstelligen dat de gewenste veiligheid alsnog kan worden bereikt. Ik zou het op prijs stellen als in uw reactie ook de bevindingen van het bankwezen en de Consumentenbond worden betrokken.

Graag zou ik uw bevindingen melden in een aan de Tweede Kamer toegezegde rapportage over de veiligheid van het betalingsverkeer. Deze zal nog dit jaar naar de Tweede Kamer worden gezonden.

De minister van Financiën,

Postbus 20201
2500 EE Den Haag

Bezoekadres
Korte Voorhout 7 Den Haag

www.minfin.nl