

Statusrapport

Veiligheid betaalproduct

Pinpas

2006

De Nederlandsche Bank

Inhoudsopgave

1	Inleiding en conclusie	5
2	Kenmerken betaalproduct Pinpas	6
3	Fraude-ontwikkeling Pinpas	7
4	Status van genomen respectievelijk onderhanden zijnde maatregelen	7
4.1	Voorlichting consumenten	8
4.2	Verzending van bankpassen en Pinmailers	9
4.3	Fraudedetectie	10
4.4	Verplicht gebruik van Pincode bij buitenlandse betaalautomaten	10
4.5	Overstap van magneetstrip naar chip (EMV).....	11
4.6	Aanvullende eisen voor onbemande betaalautomaten	12
4.7	Richtlijnen voor plaatsing betaalautomaten	12
4.8	GEA beveiligingseisen / certificering	12
4.9	Deurlezers	12

1 INLEIDING EN CONCLUSIE

Inleiding

Naar aanleiding van een verzoek van de Minister van Financiën heeft de Nederlandsche Bank (DNB) een onderzoek uitgevoerd naar de veiligheid van de betaalproducten Pinpas en Incasso. De resultaten van dit onderzoek zijn weergegeven in het rapport “Veiligheid betaalproducten Pinpas en Incasso” dat in mei 2003 naar de Minister is verstuurd en gepubliceerd¹.

DNB concludeerde in dat rapport dat de betaalproducten op de Pinpas en het betaalproduct Incasso destijds voldoende veilig waren, maar gaf tevens aan in het kader van de oversight-taak de ontwikkelingen op dit gebied nauwgezet te blijven monitoren. Hiervoor zijn twee redenen aan te dragen. De eerste reden is de voortschrijdende techniek voor het uitvoeren van aanvallen en de ontwikkelingen op beveiligingsgebied. De tweede reden is de toegenomen belangstelling van steeds beter georganiseerde criminelen voor en hun gedegen kennis van de betaalproducten.

Doelstelling van dit statusrapport is het weergeven van de actuele status van de veiligheid van de Pinpas aan de hand van de beoordeling van onderhanden zijnde en genomen maatregelen en de cijfermatige ontwikkeling van fraude. Daarnaast worden aanbevelingen ter verdere verbetering van de veiligheid van de Pinpas gedaan. Voor dit statusrapport is informatie verkregen van de betrokken partijen, zoals de Nederlandse Vereniging van Banken, Currence Holding B.V. en Interpay Nederland B.V.

Conclusie

DNB trekt de conclusie dat de Nederlandse Pinpas nog steeds voldoende veilig is. De fraudecijfers tonen aan dat er een stijging van de fraude is in 2003, maar dat de fraude in 2004 en 2005 aanzienlijk afgenomen is. Voorts is het fraudebedrag gerelateerd aan de omzet nog steeds zeer klein. Daarnaast wijst onderzoek uit dat de meeste maatregelen die door ondermeer de banken zijn genomen om de fraude terug te dringen geïmplementeerd zijn en effect sorteren. Tevens zijn de destijds gedane aanbevelingen van DNB opgevolgd. Echter, criminelen zijn steeds beter georganiseerd en hebben de beschikking over uitstekende kennis en hoogwaardige technologische middelen. Ook is verplaatsing van fraude-incidenten van geldautomaten naar betaalautomaten waargenomen. Vandaar dat het noodzakelijk blijft de Pinpas nauwlettend te blijven monitoren, fraude-incidenten goed te onderzoeken en waar nodig aanvullende fraudemitigerende maatregelen te treffen. Met betrekking tot de invoering van EMV chiptechnologie verwacht DNB dat, indien de fraude significant toeneemt, de betrokken

¹ Beschikbaar op www.dnb.nl onder menukop kennisbank en daar onder overige documenten.

deelnemers aan het Nederlandse betalingsverkeer overgaan tot een versnelde invoering ervan, zodat skimmingfraude voor een langere periode ernstig bemoeilijkt wordt.

2 KENMERKEN BETAALPRODUCT PINPAS

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 van MasterCard international. 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 Pinpas²).

De huidige Pinpas³ bevat ondermeer de volgende producten en functionaliteiten:

- het product PIN voor het verrichten van betalingen in Nederland;
- het product Maestro voor het verrichten van betalingen en geldopnames in het buitenland;
- de functionaliteit voor het opnemen van geld bij GEA's van de bank van de kaarthouder;
- de functionaliteit voor het opnemen van geld bij GEA's van een andere bank in Nederland (gastgebruik);

² De productnaam van de pinpas in Nederland is PIN, zoals opgenomen in het bijbehorende logo.

³ Ook het product Chipknip en bankspecifieke functionaliteit voor Internetbankieren is vaak op de Pinpas aanwezig.

3 FRAUDE-ONTWIKKELING PINPAS

De Pinpas met zijn verschillende bancaire producten is zeer succesvol. In Nederland worden jaarlijks met circa 20 miljoen Pinpassen ongeveer 1,3 miljard betaaltransacties verricht met een omzet van ongeveer 60 miljard Euro. Daarnaast worden met deze passen meer dan 500 miljoen geldopnames verricht.

Zoals uit de tabel is op te merken groeide de fraude van 2002 tot 2003 aanzienlijk. In 2004 zijn echter de meeste maatregelen ontwikkeld en is begonnen met de implementatie ervan. Dit leidde tot een opmerkelijke daling van de fraude van circa 12% in 2004 en zelfs met 24% in 2005.

Daarnaast kan uit de cijfers geconcludeerd worden dat het fraudebedrag gerelateerd aan de omzet nog steeds maar een zeer klein percentage is.

TABEL 1 CIJFERMATIGE ONTWIKKELING OMZET, VOLUME EN FRAUDE

Jaar	2002	2003	2004	2005
Omzet (Euro mln)	103.537	104.779	107.737	111.788
Volume (mln)	1.562	1.651	1.731	1.791
Totale fraude (Euro mln)	4,4	5,5	4,9	3,7
Percentage fraudegroei ten opzichte van het vorige jaar	-	25,1%	-11,8%	-24,0%
Fraude per transactie	€ 0,0028	€ 0,0034	€ 0,0028	€ 0,0021
Promillage totale fraude van de omzet	0,043‰	0,053‰	0,045‰	0,033‰

Het betreft hier de totalen van BEA en GEA transacties, cijfers van 2005 zijn onder voorbehoud

Met betrekking tot de typen fraude-incidenten is geconstateerd dat fraude in 2005 bij GEA's en onbemande betaalautomaten aanzienlijk afgenomen zijn. Wel is verplaatsing van fraude-incidenten van GEA's naar BEA's waargenomen en is geconstateerd dat de aanvallen een steeds professioneler karakter vertonen. Het gebruik van miniatuur camera's wordt niet geschuwd en zelfs de opzet van een ogenschijnlijk legale winkel, ingeschreven bij de kamer van koophandel, waar echte producten verkocht worden ten behoeve van het skimmen⁴ van bankpassen, heeft plaatsgevonden.

4 STATUS VAN GENOMEN RESPECTIEVELIJK ONDERHANDEN ZIJNDE MAATREGELLEN

In het eerste rapport "Veiligheid betaalproducten" is een aantal aanbevelingen en maatregelen naar voren gekomen ter verbetering van de veiligheid van de Pinpas. Dit hoofdstuk geeft de destijds gedane aanbevelingen en maatregelen weer en inventariseert bij elke de status en effectiviteit. Het betreft de volgende categorieën:

- Voorlichting consumenten;
- Verzending van bankpassen en Pinmailers;

- Fraudedetectie;
- Verplicht gebruik van Pincode bij buitenlandse betaalautomaten.
- Overstap van magneetstrip naar EMV;
- Aanvullende eisen onbemande betaalautomaten;
- Richtlijnen voor plaatsing betaalautomaten;
- GEA beveiligingseisen / certificering;
- Deurlezers;

Naast deze expliciet vermelde maatregelen is geconstateerd dat de Nederlandse banken constant bezig zijn met het beheersen van risico's in het betalingsverkeer. Voorbeelden hiervan zijn het periodiek uitvoeren van risico analyses en het houden van interbancaire overleg waar het onderwerp fraude aan de orde komt.

4.1 Voorlichting consumenten

Voorlichting aan consumenten en bedrijven is een belangrijk middel voor het verhogen van het bewustzijn ten aanzien van het veilige gebruik van de Pinpas. Consumenten en bedrijven zijn hierdoor minder vatbaar voor fraude en kunnen fraudepogingen eerder herkennen en daarmee voorkomen.

Ten tijde van publicatie van het rapport “veiligheid betaalproducten” is reeds gestart met intensievere voorlichting van consumenten en bedrijven. Sindsdien voeren de banken en betrokken instellingen regelmatig campagnes uit voor het verbeteren van klantenbewustzijn en het veilige gebruik van de bankpas. Belangrijkste punt van de voorlichting is het erop wijzen van consumenten dat de Pincode nooit aan derden verstrekt mag worden en dat de bank er ook nooit om zal vragen. Bovendien wordt er bij de campagnes op gewezen dat consumenten melding van verdachte transacties en omstandigheden kunnen maken bij een landelijk meldpunt⁵.

Als onderbouwing van de communicatiestrategie richting consumenten en bedrijven is in opdracht van de Nederlandse banken en Interpay onderzoek gedaan naar onder andere de beveiligingsperceptie van de consumenten ten aanzien van de producten PIN en Chipknip.

Het effect dat voorlichting aan consumenten en bedrijven sorteert is moeilijk te kwantificeren. Geconstateerd is echter dat consumenten en bedrijven vaker gebruik maken van het landelijke meldpunt. Daarmee lijkt het bewustzijn van consumenten en bedrijven ten aanzien van het gebruik van de bankpas en Pincode vergroot te zijn.

⁴ Het ongeautoriseerd uitlezen van magneetstrip data ten behoeve van fraude.

4.2 Verzending van bankpassen en Pinmailers

In het verleden is gebleken dat het postale verzendingstraject van bankpassen en bijbehorende beveiligde enveloppen waarmee een Pincode verstuurd wordt (Pinmailers genaamd), een fraudegevoelig traject is. Bankpassen en Pinmailers zijn tijdens het verzendtraject gestolen en gekopieerd. In 2003 vond reeds intensief overleg plaats tussen de banken en TPG post en als gevolg hiervan hebben de banken in samenwerking met TPG post onder andere de hier beschreven maatregelen genomen. De eindverantwoordelijkheid over het verzendtraject van bankpassen ligt bij de banken.

De beveiliging van het transport van bankpassen met bijbehorende Pinmailer en bankpassen zonder Pinmailer (heraanvraag of Pinkeuze mogelijkheid) kan onderverdeeld worden in maatregelen te treffen door banken en door TPG post. De banken hanteren daarbij wel een enigszins verschillende systematiek. Sommige banken bieden klanten bijvoorbeeld Pinkeuze, zodat de Pincode niet opgestuurd hoeft te worden.

- De banken hebben onder andere de volgende maatregelen toegepast: Indien zowel bankpas als bijbehorende Pinmailer met Pincode verstuurd worden naar de klant dan gebeurt dit in gescheiden trajecten. Hierbij is het tijdstip en over het algemeen ook de verzendlocatie verschillend.
- Enkele banken geven klanten de mogelijkheid een Pincode te kiezen bij een bank kantoor op vertoon van legitimatie. De Pincode wordt dus niet verstuurd.
- Bijna alle grootbanken bieden klanten de keuze bij nieuwe passen deze ofwel thuis gestuurd te krijgen ofwel op te halen bij hun bankkantoor.
- Vervangingspassen worden over het algemeen geactiveerd bij een eerste transactie met de Pincode van de te vervangen pas.
- Sommige banken laten de bankpassen op het bankkantoor activeren met behulp van Pincode verificatie.

TPG post heeft onder andere de volgende maatregelen getroffen ter voorkoming van diefstal van bankpassen en Pinmailers:

- Vervanging van TPG brievenbussen door een veiliger variant.
- Route van verzending is aangepast en veiliger: sorteercentra zijn extra beveiligd met onder andere cameratoezicht, toegangscontrole d.m.v. pasjes, bewaking met beveiligingspersoneel en steekproefsgewijze uitgangcontrole.

⁵ Dit landelijk meldnummer - 030 283 65 55 – kan anoniem gebeld worden en melding van onveilige situaties rond pinnen bij betaalautomaten kan worden gemaakt.

- Sorteertraject is bijna volledig machinaal, waardoor het onderscheppen van post bemoeilijkt wordt.

Uit de fraudecijfers blijkt dat bovenstaande maatregelen ter bescherming van het verzendtraject van de Pinpassen effectief zijn. Fraude in het verzendingstraject is momenteel klein te noemen.

Recentelijk is de verhuis-, bewaar-, en doorzendservice van TPGpost in het nieuws verschenen. Deze service kan mogelijk misbruikt worden voor het verzenden van financiële gegevens of bankpassen naar een adres van een fraudeur. TPGpost heeft echter adequate maatregelen getroffen om misbruik van deze service te voorkomen. Deze maatregelen bestaan onder andere uit het verlengen van de ingangsdatum van de service na aanvraag en het uitvoeren van additionele controles.

4.3 Fraudedetectie

In 2003 is door de banken besloten fraudedetectie op betaaltransacties en geldopnametransacties bij een andere bank (gastgebruik) toe te passen en sinds medio 2003 beschikt Interpay over een fraudedetectie systeem. Het betreft hier dus geen geldopnametransacties met de Pinpas bij de bank van de kaarthouder zelf. Dit systeem is opgezet voor het detecteren van ongebruikelijke transactiepatronen en maakt gebruik van de transactie- en fraudegegevens, die door de Nederlandse banken worden aangeleverd. Niet alle banken leveren transacties voor het detectie systeem aan.

Het detectiesysteem is succesvol gebleken bij het herkennen van onder andere skimmingfraude en het achterhalen van de locatie waar skimming heeft plaatsgevonden. De informatie wordt gebruikt voor de juridische vervolging van criminelen.

4.4 Verplicht gebruik van Pincode bij buitenlandse betaalautomaten

In het buitenland is het op sommige locaties mogelijk de Pinpas te gebruiken voor betalingen zonder dat daarbij de Pincode geverifieerd wordt, maar op basis van een handtekening.

In de rapportage “veiligheid betaalproducten” is reeds aangegeven dat dit zeer onwenselijk is. DNB heeft namelijk als beleid dat de autorisatie van een debetkaarttransactie (i.c. de Pinpas) gebaseerd dient te zijn op de eigenschappen “kennis en bezit”. De banken geven invulling aan dit beleid door voor de eigenschap “kennis en bezit” de combinatie van Pincode (kennis) en Pinpas (bezit) te hanteren.

Thans is geconstateerd dat MasterCard, ondanks aandringen van de Nederlandse banken, deze vorm van betalingen met de Pinpas niet zal verbieden. Wel heeft MasterCard onlangs als gevolg van de invoering van EMV (zie paragraaf 4.5) de aansprakelijkheid van fraude verlegd naar de

winkelier, indien deze nog steeds gebruik maakt van een terminal zonder de mogelijkheid voor de invoer van een Pincode, met als doel het gebruik ervan te ontmoedigen.

Door deze verschuiving van de aansprakelijkheid is gebleken dat het aantal BEA's zonder de mogelijkheid van de invoer van een Pincode afneemt.

DNB is van mening dat het onwenselijk is dat de mogelijkheid blijft bestaan om een betaling met de Pinpas te verrichten zonder verificatie van de Pincode. Gezien het afnemende aantal BEA's in het buitenland waar op deze manier betaald kan worden, wordt het risico niet als hoog ingeschat. Aanvullende maatregelen, behalve het onder de aandacht blijven brengen van banken bij Mastercard van dit probleem, worden momenteel niet nodig geacht.

4.5 Overstap van magneetstrip naar chip (EMV⁶)

Het gebruik van chiptechnologie voor debetkaart betalingen zal het namaken van bankpassen ernstig bemoeilijken. Interbancair is afgesproken dat de EMV standaard voor de binnenlandse en buitenlandse debetkaart betalingen volledig ingevoerd gaat worden. Dit is tevens het geval in de meeste Eurolanden. Op termijn zal de EMV standaard ook voor de Single Euro Payment Area (SEPA) gelden. SEPA betekent dat betalingen in Euro op dezelfde manier en tegen dezelfde condities kunnen worden gedaan en ontvangen als in het huidige binnenlandse retail-betalingsverkeer. 'SEPA-betalingen' worden dan ook aangemerkt als 'euro-binnenland' betalingen. De ingangsdatum van SEPA is voorzien op 1 januari 2008.

De banken geven aan dat de migratie naar EMV technologie uit twee majeure operaties bestaat, namelijk de vervanging van bankpassen van de consumenten enerzijds en BEA's van winkeliers anderzijds. Vanaf 2006 zullen de eerste bankpassen uitgerust worden met EMV chips en door middel van reguliere vervanging gemigreerd worden. De GEA's zullen in 2007 zijn aangepast met de EMV technologie. De verwachting is dat eind 2010 nagenoeg alle bankpassen vervangen zijn. Het schattingspercentage voor de vervanging van BEA's is 60% vervanging in 2010 en 90% in 2012. Met deze planning loopt Nederland achter ten opzichte van de andere Europese landen. Het risico bestaat dan dat de skimmingfraude zich op termijn verplaatst van het buitenland naar Nederland.

DNB is van mening dat het gebruik van EMV chipcard technologie voor de lange termijn een goede maatregel is bij de aanpak van skimmingfraude van bankpassen. Zij zal de fraudeontwikkeling nauwlettend monitoren. In het geval dat de fraude de komende tijd significant zou toenemen, dan beveelt DNB een versnelde invoering van EMV en een snelle uitfasering van de mogelijkheid van het doen van transacties op basis van de magneetstrip aan.

4.6 Aanvullende eisen voor onbemande betaalautomaten

Vanaf 1 maart 2003 zijn aanvullende eisen, die erop gericht zijn het afkijken van pincodes te bemoeilijken en het ongeautoriseerd uitlezen van magneetstripgegevens tegen te gaan, voor onbemande betaalautomaten van kracht geworden. Deze eisen, bestaande uit technische en procedurele maatregelen, zijn thans volledig geïmplementeerd. De aanvullende eisen sorteren effect en dringen de fraude bij onbemande betaalautomaten terug.

4.7 Richtlijnen voor plaatsing betaalautomaten

Gebleken is dat betaalautomaten in het verleden niet altijd volgens de richtlijnen geplaatst zijn. Vooral de hoogte van plaatsing week nog wel eens af van de norm, waardoor het risico van afkijken van de PINcode groter was.

Inmiddels zijn echter de meeste betaalautomaten getoetst aan de richtlijn en volgens de norm geplaatst. Hierdoor wordt het kunnen afschermen van de Pincode door de consument eenvoudiger en het afkijken van de Pincode bemoeilijkt.

4.8 GEA beveiligingseisen / certificering

Skimming van bankpassen bij GEA's was in 2002 een toenemende vorm van fraude. De banken hebben in reactie hierop in samenwerking met de terminalleveranciers ondermeer de zogenaamde voorzetmondjes ontwikkeld. Deze voorzetmondjes worden op de kaartlezer van de GEA geplaatst, zodat het plaatsen van een skimmingdevice bemoeilijkt wordt. De meeste GEA's zijn momenteel uitgerust met zo'n voorzetmondje. Gebleken is dat de plaatsing van de voorzetmondjes een uiterst effectieve maatregel is in het tegengaan van skimmingfraude. Daarnaast is door de banken een zelfcertificeringstraject ingericht waarbij GEA's door banken zelf getoetst dienen te worden aan de hand van door de Nederlandse banken opgestelde eisen. Momenteel worden deze zelfcertificeringen door de meeste banken uitgevoerd.

4.9 Deurlezers

Deurlezers voor het verlenen van toegang tot ruimtes waar GEA's geplaatst zijn, lijken op het eerste gezicht een veilige oplossing, maar vormen een extra risico. Zij kunnen namelijk misbruikt worden en zijn in het verleden ook misbruikt voor het skimmen van bankpassen. DNB heeft in het rapport "beveiliging betaalproducten" aanbevolen deze lezers te verwijderen. Ten tijde van het onderzoek voor onderhavig statusrapport is aangegeven dat nagenoeg alle deurlezers verwijderd zijn.

⁶ EMV staat voor Europay, MasterCard, VISA. Het is een standaard voor de uitwisseling van betaalgerelateerde data tussen de chip op de PINpas en de BEA of GEA.

