Trans Link Systems

Aan de minister van Infrastructuur en Milieu
Mevrouw drs. M.H. Schultz van Haegen
Postbus 20901
2500 EX DEN HAAG

Amersfoort, 24 februari 2011

Betreft: Rapport 'Fraude met de OV-chipkaart'

Kenmerk: 0067-11/AH/TvD

Geachte mevrouw Schultz van Haegen,

Hierbij bied ik u, namens Trans Link Systems B.V. (TLS) en de OV-bedrijven zoals vertegenwoordigd in de regiegroep OV-chipkaart, het rapport 'Fraude met de OV-chipkaart' aan. Dit rapport is opgesteld in het kader van de motie van het lid Monasch, waarin hij de regering verzoekt om binnen een maand met een nadere rapportage te komen om de risico's van de recente kraakacties van de OV-chipkaart in kaart te brengen.

Dit rapport hebben wij ook aan PricewaterhouseCoopers gestuurd, aan wie u heeft gevraagd de rapportage van de vervoerders en TLS te valideren.

Ik vertrouw op een positieve beslissing voor de verdere invoering van de OV-chipkaart.

Met vriendelijke groet,

G.N. Neleman
Directeur
Trans Link Systems B.V.

Bijlage: Rapport 'Fraude met de OV-chipkaart'

Trans Link Systems B.V.
Stationsplein 151 - 157
3818 LE Amersfoort
The Netherlands

Tel.: +31 33 467 20 00
Fax: +31 33 467 20 99
E-mail: info@translink.nl
Website: www.translink.nl

BTW-nummer: NL810814341B01
KvK Gooi- en Femland: 30177126
Rabobank. 19.23.00.334

Rapportage Fraude met de OV-chipkaart

Auteur	Gerben Nelemans

Versie	1.2
Datum	23 februari 2010
Status	Definitief
Pagina's	26

INHOUDSOPGAVE

1. Achtergrond 4
1.1 De invoering van de OV-chipkaart 4
1.2 De OV-chipkaart gehackt 4
1.3 Onderzoeken door TNO en RHUL 5
1.4 Voorbereiding voor migratie 6
1.5 Fraudes in 2010 en 2011 6
2. Werking van het systeem 7
2.1 Vier niveau's 7
2.2 Transacties met de OV-chipkaart 9
2.3 Blokkeren van de OV-chipkaart 9
2.4 Beveiliging, een continu proces 10
2.5 De strafbaarheid 10
3. Huidige stand van zaken 12
3.1 Tijdslijn fraude januari 2011 12
3.2 Fraude ontwikkeling 13
3.3 Handleidingen en websites 14
3.4 Blokkeringlijst en aangifte 14
3.5 Geen financiële schade voor de reiziger 14
3.6 Tevredenheid van reizigers 15
4. Fraudescenario's 16
4.1 Impactbepaling bij vier actuele fraudescenario's 16
4.2 Criminele business case 18
4.3 Overige fraude scenario's 19
4.4 Wat is nieuw? 19
5. Maatregelen 20
5.1 Procedurele maatregelen 20
5.2 Systeemtechnische maatregelen 20
5.3 Invoeringsstrategie 21
5.4 Het migratieplan 22
5.5 Worst case scenario 22
6. NVB wel-uitzetten versus NVB niet-uitzetten 24
6.1 Geen verhoogd frauderisico 24
6.2 Fraude met papier 24
6.3 Dubbele kosten 25
6.4 Verwarrend voor de reiziger 26

1. Achtergrond

1.1 De invoering van de OV-chipkaart

De invoering van de OV-chipkaart in Nederland betekent de overgang van papieren vervoerbewijzen naar een elektronisch betaal- en reismiddel voor alle vormen van openbaar vervoer in Nederland. Eén kaart voor trein, tram, bus en metro: de OV-chipkaart. Er waren diverse redenen om de OV-chipkaart in te voeren ter vervanging van de papieren vervoerbewijzen. Een belangrijke reden is het reduceren van het zwartrijden in het openbaar vervoer en het terugdringen van fraude met de papieren vervoerbewijzen (zoals het vervalsen van strippenkaarten en abonnementen).

RET was het eerste OV-bedrijf dat de OV-chipkaart volledig ingevoerd heeft. Door de introductie van de OV-chipkaart is het percentage zwartrijders bij RET gedaald van 10-12% naar 3,3% in 2010. RET heeft als gevolg van de invoering van de OV-chipkaart daarmee een aanzienlijk lagere toegangsbewijsfraude gehad in 2010 dan in de jaren daarvoor, toen nog gereisd kon worden met papieren vervoerbewijzen.

GVB volgde RET vrij snel met de sluiting van het metrosysteem en daarna de afschaffing van de strippenkaart op bus en tram. In de strippenkaart periode was het veel makkelijker om zwart te rijden in de metro dan nu het geval is, omdat de toegang nu met poortjes is afgesloten die werken met de OV-chipkaart. GVB schat in dat het percentage zwartrijden in de metro is afgenomen van 14% naar 4%. Ook zag GVB in het papieren tijdperk veel misbruik met het papieren vervoerbewijs. Er werd gefraudeerd met strippenkaarten of deze werden nagemaakt. Hiervan werden er honderden per jaar in beslag genomen.

Naast bovenstaande biedt de OV-chipkaart vele andere voordelen: gemak voor de reiziger (één kaart voor al het openbaar vervoer), flexibiliteit voor tarieven en tariefsystemen (waaronder het betalen per afgelegde kilometer in plaats van het zonesysteem), een snellere en eerlijkere opbrengstenverdeling en een verhoging van de sociale veiligheid op en rond stationslocaties.

Het OV-chipkaart systeem maakt in de kaart gebruik van de Mifare Classic chip. Deze Mifare Classic chip is een van de meest gebruikte chips wereldwijd voor contactloze toepassingen. Niet alleen wordt de Mifare Classic gebruikt in diverse grote openbaar vervoer systemen (zoals de Oyster card in Londen waar de Mifare Classic nog steeds in gebruik is en de Charlie card in Boston) maar ook bij toegangsbeveiliging en diverse andere toepassingen. Dit was in 2002 ook de reden om deze chip te selecteren ('proven technology').

1.2 De OV-chipkaart gehackt

Eind 2007 is op een hackersconferentie in Berlijn voor het eerst aangetoond dat de gebruikte cryptografie in de Mifare Classic chip zwak is. In de daarop volgende maanden (in het begin van 2008) hebben diverse academici en andere hackers een reeks aan zwakheden van de Mifare Classic chip aangetoond. Hierdoor werd het mogelijk de Mifare Classic chip te kraken.

Manipulatie van gegevens op de chip in de OV-chipkaart was en is als gevolg van de kraak mogelijk. Reeds in 2008 zijn contacten geweest met politie en justitie over de strafbaarheid van het manipuleren van de OV-chipkaart en het proces van aangifte en vervolgen in het geval zich deze strafbare feiten voordoen.

1.3 Onderzoeken door TNO en RHUL

In 2008 zijn, in opdracht van respectievelijk TLS en het ministerie van Verkeer en Waterstaat, onderzoeken ingesteld naar de beveiligingszwakheden van de chip. Deze onderzoeken zijn uitgevoerd door TNO en Royal Holloway, University of London (RHUL). De contra-expertise van RHUL onderschreef een groot aantal van de conclusies van het TNO rapport, te weten:

- RHUL concludeert, in navolging van TNO, dat de huidige Mifare Classic chip nu als gekraakt moet worden beschouwd.
- Het feitelijke risico van een kraak treft niet de reiziger.
- De privacy is niet in het gedrang, omdat slechts de geboortedatum op de chip staat.

Als toevoeging op het TNO rapport concludeerde de contra-expertise het onderstaande:

- Er is een aantal aanvalsscenario's niet in het TNO rapport omschreven. Deze scenario's zijn pas na het TNO rapport door wetenschappers gepubliceerd. Hierdoor is het volgens RHUL lastig in te schatten wanneer de kaart precies vervangen moet worden. De periode van twee jaar, zoals genoemd in het TNO rapport, is dan ook lastig te verifiëren.
- In plaats van deze twee jaar dient er een gedetailleerd migratieplan te worden ontwikkeld, dat gereed moet zijn zodra de OV-chipkaart landelijk is uitgerold. Dit moment van 'gereed zijn' wordt de Migration Planning Milestone (MPM) genoemd.
- Na het bereiken van de MPM is bekend in hoeverre mogelijke fraude zich ook daadwerkelijk voordoet, of de voorgestelde korte termijnmaatregelen tegen fraude effectief zijn en wat een geschikt migratiepad voor de chip zou kunnen zijn. Definitieve besluitvorming over aanpak en tempo van eventuele migratie kan vervolgens worden genomen op basis van vooraf bepaalde stappen en 'triggers', waaronder de aard en omvang van daadwerkelijk misbruik.
- Er dient minimaal één algemene, herkenbare, en fysieke anti-fraude maatregel op de kaart te worden aangebracht.
- Er dient open naar het publiek gecommuniceerd te worden over de voortgang rondom de MPM.

Op basis van de contra-expertise zijn in 2008 door TLS en de OV-bedrijven de volgende besluiten genomen en vervolgstappen gezet:

- De OV-bedrijven en TLS nemen de aanbeveling van RHUL over om een MPM vast te stellen, in plaats van overhaast een andere chip te selecteren.
- Er worden gegevens verzameld voor misbruik van het systeem (fraude wordt gemeten en gerapporteerd).
- De OV-chipkaarten worden voorzien van een fysieke anti-fraude maatregel, te weten het aanbrengen van holografisch folie op de kaart.
- De effectiviteit en uitvoerbaarheid van de mogelijke korte termijn maatregelen worden door TLS en de OV-bedrijven beoordeeld. Enkele van deze maatregelen zijn vervolgens ingevoerd. De andere maatregelen zijn uitgewerkt, maar invoering hiervan was op dat moment niet noodzakelijk gezien de start van de MPM, de kosten van invoering en het fraudeniveau..

Bij de activiteiten die horen bij het opstellen van de MPM zijn ook externe onderzoeksinstellingen, wetenschappelijke instellingen en internationale zusterprojecten betrokken.

1.4 Voorbereiding voor migratie

De MPM en het bijbehorende Decision framework (dat omschrijft hoe de besluitvorming tot migratie plaatsvindt) zijn, nadat deze door TLS en de OV-bedrijven zijn opgesteld, door RHUL onderzocht. Op basis van de bevindingen van dit onderzoek is, mede om de doorlooptijd van migratie te verkorten, gestart met de voorbereidingen van migratie. De voorbereiding van migratie naar een nieuwe chip met een hoger beveiligingsniveau is met financiële ondersteuning van het ministerie en Fonds Eenmalige bijdrage NS (FENS) begin 2010 ook daadwerkelijk begonnen.

1.5 Fraudes in 2010 en 2011

In 2010 zijn slechts enkele gevallen van fraude door de detectieregels in de backoffice van TLS gesignaleerd. Na analyse is besloten de gedetecteerde, frauduleuze kaarten direct te blokkeren. In vrijwel alle gevallen bleek achteraf geen sprake van fraude maar was de oorzaak een foutieve instelling in en/of werking van het systeem. Bij één specifiek geval van fraude is besloten deze nader te volgen, waarna aangifte is gedaan bij het Openbaar Ministerie. Dit heeft geleid tot onderzoek, aanhouding en vervolging van een persoon uit Leiden.

In januari 2011 is in de backoffice van TLS fraude met in eerste instantie één anonieme kaart en later op een groeiend aantal kaarten geconstateerd. In verband met onderzoek is er niet geblokkeerd, maar zijn meer gegevens verzameld en geanalyseerd. Van deze vermoedelijke fraude is op 21 januari 2011 aangifte gedaan. Naderhand is bekend geworden dat deze fraude vermoedelijk is gepleegd door een aantal journalisten die anonieme OV-chipkaarten hebben gemanipuleerd en hierop hebben gereisd. Hierna volgde, net als in 2008, behoorlijke aandacht vanuit de media met als gevolg een politiek debat en een uitstel van de effectuering van het besluit om per 3 februari 2011 het Nationaal Vervoersbewijs (NVB) uit te zetten in de regio Haaglanden en provincie Zuid-Holland.

2. Werking van het systeem

In dit hoofdstuk is een korte beschrijving opgenomen van de werking van het OV-chipkaartsysteem. Hierbij wordt met name ingegaan op de wijze waarop transacties met OV-chipkaarten tot stand komen, hoe deze transacties worden geanalyseerd en hoe, in geval van fraude met een kaart, de blokkeringlijst in het systeem wordt verspreid.

2.1 Vier niveau's

Het OV-chipkaartsysteem bestaat uit vier niveaus, zoals in de figuur op de volgende pagina is te zien:

- **Level 1.** Dit is het niveau met alle apparatuur op reizigersniveau, zoals poortjes, kaartlezers, verkoopautomaten en controle-apparatuur. De OV-chipkaart wordt bij deze apparatuur gebruikt om in- en uit te checken of om saldo en producten op de kaart te laden.
- **Level 2.** Dit is het niveau van apparatuur op stations- of depotniveau en dient ter aansturing van de level 1 apparaten op een bepaalde locatie. Het verzorgt de communicatie, aansturing, configuratie en bewaking van de apparatuur die erop is aangesloten.
- **Level 3.** Dit is het centrale systeem van een OV-bedrijf, van waaruit de level 1 en level 2 apparatuur van het betreffende bedrijf wordt aangestuurd. Op hoofdlijnen heeft level 3 de volgende functies: bewaking en bediening van apparatuur in het veld, distributie van software en parameter instellingen naar apparatuur, routering van transacties, beveiliging van apparatuur en het verzorgen van de communicatie met de centrale backoffice van TLS.
- **Level 4.** Dit is het centrale systeem van TLS en de backoffice-omgeving achter de OV-chipkaart. In deze omgeving worden alle transacties met de OV-chipkaart verwerkt en geanalyseerd, wordt de blokkeringlijst samengesteld, worden alle gegevens van kaarthouders veilig opgeslagen (separaat van transacties), worden alle service-aanvragen voor OV-chipkaarten (zoals verlies/diefstal meldingen of adreswijzigingen) verwerkt en worden de OV-chipkaarten geproduceerd en geregistreerd.

Level 0: Kaarten

Persoonsgebonden OV-chipkaart	Anonieme OV-chipkaart	Wegwerpkaart (uniek per vervoerder)

Level 1: Apparatuur op reizigersniveau

Level 1 apparatuur bevat:
- Beveiligingsvoorzieningen voor lezen, schrijven en het creëren van transacties
- Zwarte lijst voor blokkeren
- Validatieregels voor kaart- en productgebruik
- Software om prijsberekeningen te doen
- Transacties
- Standenregisters

Level 2: Lokale systemen OV-bedrijf

Systeem bevat:
- Beveiligingsvoorzieningen voor doorgifte van transacties
- Apparaat besturingsgegevens
- Transactiebestanden
- Standenregisters

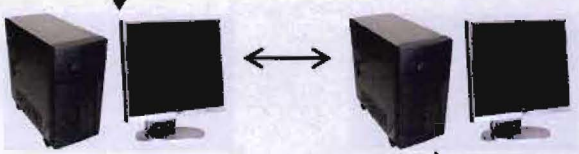
Level 3: Centraal systeem OV-bedrijf

Systeem bevat:
- Beveiligingsvoorzieningen voor doorgifte van transacties
- Apparaat besturingsgegevens
- Monitoring van apparatuur
- Configuratie van producten
- Rapportagefuncties
- Transactiebestanden
- Standenregisters

Systeem bevat:
- Relatie- en contactgegevens van kaarthouders (persoonsgebonden kaarten), conform Wbp

Level 4: Centraal verwerkingssysteem (TLS)

Systeem bevat:
- Beveiligingsvoorzieningen voor ontvangst van transacties
- Alle transactiebestanden
- Alle standenregisters
- Alle kaartgegevens
- Contractgegevens automatisch opladen (bankrekening)
- Validatieregels voor verwerking van transacties (de 3e beveiligingslaag)



www.ov-chipkaart.nl

0900-0980

2.2 Transacties met de OV-chipkaart

De OV-chipkaart werkt contactloos met de OV-chipkaartapparatuur. Iedere keer als de OV-chipkaart wordt aangeboden bij de apparatuur, zoals bij het inchecken, ontstaat, nadat diverse validaties op de kaart zijn uitgevoerd, een transactie in het systeem. Voor de kaarthouder heeft op dat moment de transactie (betaling) plaatsgevonden. De OV-chipkaart is leidend in het systeem. Dit betekent dat bijvoorbeeld de feitelijke waarde van de OV-chipkaart op de chip zelf is opgeslagen. De transacties worden door de apparatuur via de centrale systemen van de OV-bedrijven aangeboden aan de centrale backoffice van TLS. De backoffice 'volgt' als het ware de kaart en het gebruik van de kaart op basis van de transacties die in de backoffice worden aangeboden. De frequentie waarmee transacties aan de backoffice worden aangeboden, verschilt per type apparaat. Sommige apparaten, zoals poortjes, leveren de hele dag door hun transacties. Andere apparaten, zoals apparatuur in de bus, doen dit in de regel een beperkt aantal keer per dag, namelijk op het moment dat het voertuig op het depot is en verbinding kan maken met het level 2- of level 3-systeem van het OV-bedrijf. In uitzonderlijke gevallen komen de transacties ook een dag of paar dagen later binnen en in heel uitzonderlijke gevallen (bijvoorbeeld door sabotage of defecte apparatuur) komen transacties helemaal niet binnen in de backoffice. De kaarthouder merkt hier niets van, de betaling vindt plaats bij het aanbieden van de kaart. De transacties met een OV-chipkaart komen in willekeurige volgorde binnen in de backoffice. Hier worden alle transacties geanalyseerd en, nadat ze goed zijn bevonden, financieel verwerkt. Onderdeel van de analyse is dat de fraudedetectieregels worden toegepast op de transacties om frauduleuze handelingen met de OV-chipkaarten te kunnen detecteren. Deze fraudedetectieregels zijn in 2008 verfijnd en verbeterd naar aanleiding van de toen bekend geworden zwakheden met de chip in de OV-chipkaart en de diverse rapportages die hierover zijn geschreven. De analyse en verwerking van transacties zijn volledig geautomatiseerde processen. Momenteel worden dagelijks ongeveer 4,5 miljoen transacties op deze wijze verwerkt. Financiële verwerking betekent dat de opbrengsten worden uitgekeerd aan de betreffende OV-bedrijven. Dit gebeurt dagelijks.

2.3 Blokkeren van de OV-chipkaart

OV-chipkaarten kunnen om verschillende redenen op de blokkeringlijst worden gezet. De belangrijkste reden is een melding van een kaarthouder dat een persoonsgebonden OV-chipkaart verloren of gestolen is. Maar het kan ook voorkomen dat uit de fraudedetectieregels een aanwijzing komt voor frauduleus gebruik van de OV-chipkaart. Ook in dat geval wordt de betreffende kaart op de blokkeringlijst gezet. De blokkeringlijst wordt samengesteld in de backoffice en vervolgens via de centrale systemen van de OV-bedrijven verspreid naar de apparatuur in het veld. Ook hier geldt dat er verschil in frequentie kan bestaan tussen apparatuur die vast op 'de wal' staat en apparatuur die zich in voertuigen bevindt. Hierdoor kan het voorkomen dat een bepaalde blokkeringlijst al wel in een poortje aanwezig is, maar nog niet in een kaartlezer in de bus.

Als een OV-chipkaart op de blokkeringlijst staat, wordt de kaart geblokkeerd bij het eerstvolgende gebruik van de kaart bij een apparaat. Dit betekent dat de kaart niet meer gebruikt kan worden. Kaarten die vanwege fraude op de blokkeringlijst zijn geplaatst, blijven hier permanent op staan. Hoewel de blokkade door het manipuleren van de OV-chipkaart ongedaan kan worden gemaakt, kan de kaart toch niet worden gebruikt, omdat deze permanent op de blokkeringlijst blijft staan. Een technische maatregel is in voorbereiding (zie maatregelen) om te voorkomen dat blokkades van een kaart ongedaan kunnen worden gemaakt.

2.4 Beveiliging, een continu proces

Beveiliging is een continu proces voor TLS en de OV-bedrijven. Als onderdeel hiervan worden het fraudedetectiesysteem en de fraudedetectiemaatregelen continu verbeterd als dit nodig is en aangepast als zich nieuwe fraudescenario's voordoen. OV-bedrijven en TLS werken hiervoor samen met beveiligingsexperts en hackers, maar hebben ook een aantal medewerkers met deze deskundigheid in dienst.

2.5 De strafbaarheid

In Nederland moet voor het gebruik van openbaar vervoer diensten door iedereen worden betaald. OV-bedrijven controleren hierop om zwart- en grijsrijden alsmede het gebruik van vervoerbewijzen waarmee is geknoeid. te beperken. Met politie en justitie zijn door de OV-bedrijven afspraken gemaakt over handhaving en vervolging. Ieder OV-bedrijf doet dit voor zichzelf waarbij er (zichtbare) verschillen zijn tussen de diverse modaliteiten van vervoer. Dit is zo in de papieren wereld en met de OV-chipkaart verandert er weinig aan het optreden van OV-bedrijven, politie en justitie tegen zwartrijden en kaartmisbruik. Net als bij de strippenkaart moet de reiziger een geldig vervoerbewijs hebben, dat gekocht is via de normale verkoopkanalen, dus waar niet mee geknoeid is. Net zoals de strippenkaart correct moet zijn afgestempeld om geldig te zijn als vervoerbewijs, moet de reiziger ook correct inchecken met de OV-chipkaart.

De volgende strafbare feiten voor manipulatie met de OV-chipkaart zijn geconstateerd:

- Het hacken van de OV-chipkaart
- Het manipuleren van het saldo
- Het 'thuis' inchecken
- Het in bezit hebben van voorwerpen (apparatuur of programma's) om OV-chipkaarten valselijk op te maken (te manipuleren)
- Het reizen met een gemanipuleerde OV-chipkaart (zowel saldo als product, zoals het studentenreisproduct)
- Het verkopen of verschaffen van gemanipuleerde kaarten

- ***Het hacken van de OV-chipkaart***

  Het hacken van de OV-chipkaart is strafbaar gesteld in artikel 138a Sr., computervredebreuk. De maximale straf voor het plegen van dit feit is een gevangenisstraf voor de duur van één jaar of een geldboete van maximaal € 18.500,-.

- ***Het manipuleren van het saldo en het thuis inchecken***

  Het manipuleren van het saldo, zowel door kopie van het image van het saldo als door manipulatie "in" de kaart en het creëren van een thuis check-in, is ook strafbaar gesteld in artikel 232 lid 1 Sr. Dit artikel stelt het opzettelijk valselijk opmaken van een waardekaart strafbaar. De maximale straf voor het plegen van dit feit is een gevangenisstraf voor de duur van zes jaren of een geldboete van maximaal € 74.000,-.

- ***Het in bezit hebben van voorwerpen (apparatuur of programma's) om OV-chipkaarten valselijk op te maken (te manipuleren)***

  Het voorhanden hebben van computerapparatuur en software met als doel het vervalsen van de OV-chipkaart (zoals strafbaar gesteld in artikel 232 Sr.) is strafbaar gesteld in artikel 234 Sr. De maximale straf voor het plegen van dit feit is een gevangenisstraf voor de duur van vier jaren of een geldboete van maximaal € 18.500,-.

- ***Het reizen met een gemanipuleerde OV-chipkaart en het verkopen of verschaffen van gemanipuleerde kaarten***

  Het reizen met een gemanipuleerde OV-chipkaart is strafbaar gesteld in artikel 232 lid 2 Sr. (opzettelijk gebruik maken van een vervalste waardekaart met het oogmerk zichzelf te bevoordelen). Het verkopen of aan anderen verstrekken van gemanipuleerde OV-chipkaarten is strafbaar gesteld in dit zelfde artikel. De maximale straf voor het plegen van dit feit is een gevangenisstraf voor de duur van zes jaren of een geldboete van maximaal € 74.000,-.

Verweer met betrekking tot artikel 232 lid2, het reizen met een vervalste OV-chipkaart

In de recente strafzaak tegen de fraudeur uit Leiden is door de verdediging het verweer gevoerd dat de verdachte naast zijn gemanipuleerde OV-chipkaart ook steeds heeft gereisd met een legale OV-chipkaart/regulier vervoerbewijs. De rechtbank overweegt hierover dat: "op basis van de inhoud van het dossier en het verhandelde ter terechtzitting niet kan worden vastgesteld dat verdachte het oogmerk heeft gehad om zichzelf te bevoordelen en om zelf opzettelijk de door hem vervalste OV-chipkaarten als echt en onvervalst te gebruiken. Verdachte heeft namelijk gesteld dat hij met de vervalste OV-chipkaarten slechts in- en uitcheckte en daarnaast een regulier vervoersbewijs gebruikte. In het dossier bevindt zich onvoldoende bewijs om te kunnen oordelen dat dit niet het geval is".

Zowel de officier van justitie als TLS delen dit oordeel niet. Door met de vervalste OV-chipkaart in- en uit te checken pleegt verdachte al het in artikel 232 strafbaar gestelde. Ons inziens zou dit verweer niet tot vrijspraak, maar slechts tot een strafmatiging kunnen leiden. De officier van justitie heeft dan ook besloten tegen deze uitspraak in hoger beroep te gaan.

3. Huidige stand van zaken

3.1 Tijdslijn fraude januari 2011

In 2010 zijn slechts enkele gevallen van fraude (op diverse anonieme kaarten) door de fraudedetectieregels in de backoffice van TLS gesignaleerd. De gedetecteerde, frauduleuze kaarten zijn direct geblokkeerd. Bij één specifieke situatie is, mede omdat er sprake was van een patroon, besloten om deze kaarten niet direct te blokkeren. De kaarten zijn gedurende langere tijd gevolgd en er is aangifte gedaan bij de officier van justitie in Utrecht. Deze is hierop een onderzoek gestart, dat vervolgens heeft geleid tot de aanhouding van een persoon uit Leiden alsmede de veroordeling van deze persoon op een aantal strafbare feiten (veroordeling was tot 60 uur werkstraf en een gevangenisstraf van één maand voorwaardelijk). De persoon in kwestie heeft aangegeven dat het manipuleren van de kaarten is gedaan met hulpmiddelen, informatie en tools die op het internet aanwezig waren c.q. gekocht konden worden en eenvoudig konden worden gebruikt. Tevens heeft de zaak behoorlijke media aandacht gehad in die tijd. Toch heeft dit niet geleid tot een toename van fraudegevallen met de OV-chipkaart, hoewel de randvoorwaarden hier wel voor aanwezig waren.

Op 12 januari 2011 is door de fraudedetectieregels in de backoffice van TLS fraude met een anonieme OV-chipkaart gedetecteerd. Ook hier is besloten, vergelijkbaar met de situatie van Leiden, om niet direct tot blokkade van de kaart over te gaan, maar deze te volgen en zodoende een dossier op te bouwen. Al snel was vergelijkbare fraude waarneembaar op meerdere kaarten en leek er sprake van een patroon. Op 14 januari 2011 zijn de betrokken vervoerders (waar met de gefraudeerde kaarten werd gereisd) geïnformeerd en is hen verzocht om relevante camerabeelden veilig te stellen. Op 14 januari 2011 is ook de Officier van Justitie van deze situatie op de hoogte gesteld. In de daarop volgende dagen is een dossier opgebouwd van de betreffende kaarten. Op 21 januari is formeel aangifte gedaan van deze zaak.

Op 25 januari 2011 hebben journalisten van NOS, Webwereld en RTV Rijnmond bekend gemaakt dat zij enige tijd hebben gereisd op gemanipuleerde OV-chipkaarten. Hiervoor zou gebruik zijn gemaakt van een Windowsprogramma dat in combinatie met een aan te schaffen RFID reader (indicatie aanschafprijs € 30) het saldo op de OV-chipkaart kan manipuleren en ongeautoriseerd kan verhogen. Eveneens is een fraudescenario getoond, waarmee 'thuis' ingecheckt kan worden door een check-in op een bepaald station op de kaart te manipuleren. Vervolgens wordt niet in- en uitgecheckt bij de OV-chipkaartapparatuur en ziet de conducteur tijdens de rit met de controle-apparatuur een valide check-in op de kaart staan. Aangezien op dit moment de controle-apparatuur geen transacties afgeeft aan de backoffice en de kaart niet bij de gebruiksapparatuur wordt aangeboden (en er dus geen transactie ontstaat), blijft deze fraude momenteel onopgemerkt. Dit fraudescenario is niet van toepassing in situaties, waarbij aan boord van een voertuig moet worden ingecheckt en in situaties waarbij toegang door poortjes wordt verleend.

De software om laatstgenoemde fraudescenario uit te voeren, is op internet verschenen op 14 februari 2011, de software om het saldo te manipuleren was reeds eerder op internet te vinden. De zwakheden van de chip, waarvan de software gebruikmaakt, zijn dezelfde als die eind 2007 aan het licht zijn gebracht en waarvan ook de reeds sinds die tijd vindbare software op internet gebruikmaakt. Uitspraken zoals 'OV-chipkaart definitief gekraakt', die doen vermoeden dat de zwakheden groter zijn geworden of dat er meer zwakheden zijn gevonden,

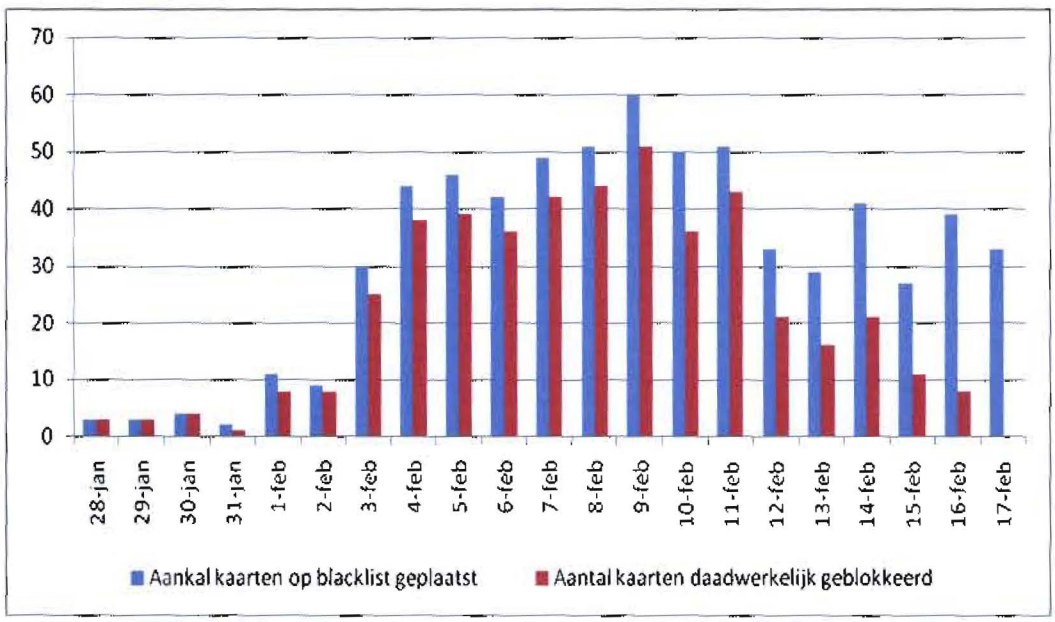
zijn daarmee onjuist. Het verschil is dat er Windows-software in omloop is gebracht, waardoor de toegankelijkheid tot de manipulatiemogelijkheden is vergroot.

3.2 Fraude ontwikkeling

De onthullingen van de journalisten alsmede de aandacht vanuit de politiek in het daarop volgende debat met de Minister hebben in de media gezorgd voor een aanzienlijke aandacht voor de fraude met de OV-chipkaart. Deze verhoogde aandacht heeft ertoe geleid dat meer mensen op het idee zijn gebracht om één en ander zelf uit te proberen. Uit onderstaande grafiek staan de dagaantallen kaarten die in de backoffice op frauduleuze handelingen worden gedetecteerd. Hier is een groei te zien tot ongeveer 50 kaarten per dag. Opgemerkt wordt dat hierin nog niet de cijfers zitten van de OV-chipkaarten waarop een 'thuis check-in' wordt gemanipuleerd, aangezien dit nog niet meetbaar en detecteerbaar is.

Deze cijfers moeten worden gezien in het volgende perspectief:

- 9,5 miljoen gedistribueerde OV-chipkaarten in Nederland
- 100 miljoen transacties met OV-chipkaarten in januari 2011
- 1,8 miljoen unieke OV-chipkaarten per week in gebruik
- 4,5 miljoen transacties per dag



Het is zeer lastig c.q. vrijwel onmogelijk om op basis van de actuele gegevens een voorspelling te doen over de fraude ontwikkeling vanaf hier. Een feit is dat de aandacht in media en politiek heeft geleid tot een stijging in het aantal fraudegevallen.

De verwachting is dat met het verminderen van deze aandacht ook het aantal fraudegevallen daalt. Door nieuwe media-aandacht kan dit aantal echter weer tijdelijk toenemen.

TLS en de OV-bedrijven stellen dat daarbij sprake is van een beheerste en gecontroleerde situatie. De frauduleuze kaarten worden gedetecteerd en vervolgens op de blokkeringlijst geplaatst. Bij het eerstvolgende gebruik van de kaart wordt deze geblokkeerd.

3.3 Handleidingen en websites

Op het internet verschijnen diverse handleidingen en software programma's om de OV-chipkaart te kunnen manipuleren. Dit is strafbaar. TLS en de OV-bedrijven nemen hier dan ook maatregelen tegen. Continu worden publicaties op internet gevolgd en beoordeeld op strafbaarheid. Indien mogelijk wordt contact opgenomen met desbetreffende organisatie of websitebeheerder met het verzoek om publicaties en software te verwijderen of aan te passen.

3.4 Blokkeringlijst en aangifte

De frauduleuze OV-chipkaarten worden gedetecteerd in de backoffice van TLS. Deze controles worden op meerdere momenten per dag uitgevoerd op basis van de transacties die in de backoffice binnengekomen zijn. Ook in de weekenden vinden deze controles plaats. Frauduleuze kaarten worden direct na detectie op de blokkeringlijst geplaatst. Deze lijst wordt éénmaal per dag in het systeem verspreid. Kaarten die op de blokkeringlijst staan, worden bij het eervolgende gebruik geblokkeerd en kunnen daarna niet meer worden gebruikt. Aangezien deze blokkeringsinformatie wordt teruggegeven aan de backoffice is waarneembaar dat na enkele dagen een significant deel van de frauduleuze kaarten daadwerkelijk is geblokkeerd. De overige kaarten worden kennelijk na de manipulatie en eenmalig gebruik niet meer gebruikt.

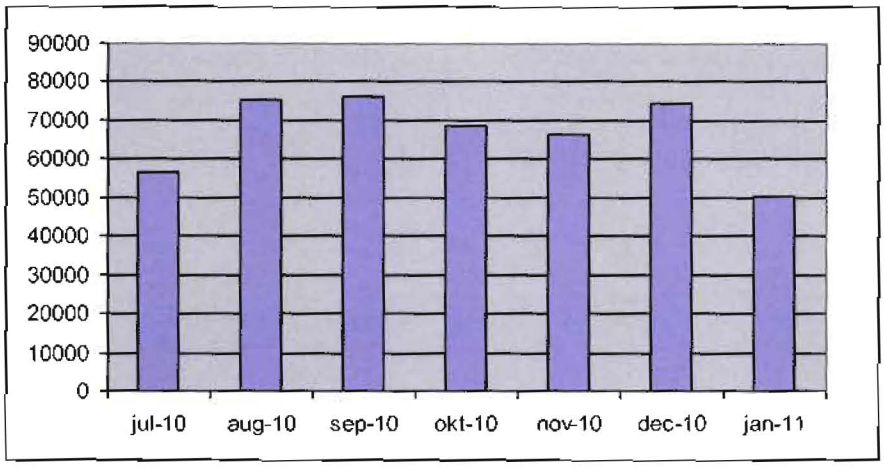
Van alle fraudegevallen waarbij op eenvoudige wijze de relatie kan worden gelegd met de identiteit van een persoon, wordt direct aangifte gedaan bij het Openbaar Ministerie. Met het OM wordt nauw overlegd, ook over de gevallen waarbij minder makkelijk deze relatie is te leggen.

3.5 Geen financiële schade voor de reiziger

Door het manipuleren van een OV-chipkaart, bijvoorbeeld door het saldo van een kaart te verhogen, lopen andere reizigers die een OV-chipkaart gebruiken en hiermee voor hun reis betalen, geen risico. Het risico ligt bij TLS en de OV-bedrijven. Er wordt immers 'vals geld' gecreëerd en vervolgens wordt dit geld gebruikt om te betalen voor een reis. Er is geen enkele logica vanuit de gedachte van een fraudeur (die uit is op financieel gewin) om het saldo van andere kaarten dan die van hem/haarzelf te manipuleren. Het is daarmee bijna ondenkbaar dat een reiziger financiële schade ondervindt door fraude. Als deze situatie zich toch voordoet, dan wordt de schade van de gedupeerde reiziger vergoed.

De reizigers hebben in januari 2011 hun OV-chipkaarten 100 miljoen keer gebruikt. In 2010 was dit in totaal voor het hele jaar ruim 900 miljoen keer. Het gebruik van de kaart is daarmee in januari gestegen en zeker niet (drastisch) gedaald. Bij de landelijke klantenservice OV-chipkaart zijn nagenoeg geen vragen van bezorgde reizigers binnengekomen naar aanleiding van alle aandacht voor de beveiliging van de kaart. Ditzelfde geldt voor de klantenservice afdelingen van de OV-bedrijven of bij de balies van OV-bedrijven.

De grote media-aandacht in 2011 rondom het kraken van de OV-chipkaart heeft niet geleid tot een noemenswaardige toename van het aantal contactmomenten met klantenservice bij NS. In onderstaande figuur is het aantal contactmomenten opgenomen met reizigers. In de periode juli 2010 tot en met 11 februari 2011 zijn 14 contactmomenten geweest over fraude, waarvan 6 na de media-aandacht op 25 januari 2011. De 14 contactmomenten vonden plaats op een totaal van bijna 500.000 contactmomenten.



3.6 Tevredenheid van reizigers

In 2010 heeft Blauw Research een onderzoek gedaan bij NS naar de klanttevredenheid over het Reizen op Saldo bij NS. 76% van de reizigers vindt dat Reizen op Saldo (RoS) meer gemak biedt dan papieren kaartjes.

RET heeft een 7,3 gemeten voor klanttevredenheid bij hun laatste onderzoek.

4. Fraudescenario's

In 2008 zijn door TLS fraudescenario's opgesteld naar aanleiding van de zwakheden in de chip van de OV-chipkaart en de daaruit volgende mogelijkheden tot manipulatie van de kaart. Deze scenario's worden periodiek van een update voorzien. Dit is ook recent gebeurd naar aanleiding van alle aandacht voor fraude in de afgelopen weken. Ook worden regelmatig fraudetesten uitgevoerd met eigen gemanipuleerde kaarten om systemen, processen en procedures te testen. De fraudescenario's zijn op gedetailleerd niveau onderscheiden en inclusief detectiemogelijkheden beschreven.

4.1 Impactbepaling bij vier actuele fraudescenario's

Hieronder zijn vier actuele fraudescenario's nader uitgewerkt, waarbij aangegeven wordt wat de impact is. Opgemerkt wordt dat de aantallen zijn gebaseerd op verwachtingen, inschattingen en de beperkte trend in het aantal fraudegevallen dat voorhanden is.

1. **Ophogen van saldo en ermee reizen.**

   Bij dit scenario worden door de fraudeur de kaartsleutels gekraakt, wordt het image met kaartgegeven apart gezet, wordt de beurswaarde verhoogd en wordt het image met aangepast beurswaarde weer op de kaart geplaatst. Dit scenario is reëel en wordt op dit moment toegepast door fraudeurs. Er zijn meerdere detectiemogelijkheden, waardoor een saldoaanpassing in de backoffice goed kan worden gedetecteerd. Hierbij moeten we in ogenschouw nemen dat de fraudeurs steeds meer bekend zijn met de OV-chipkaart-toepassing en dat varianten kunnen worden uitgeprobeerd. Continue bewaking is daarom noodzakelijk en ingericht.

   Voor de business case is het belangrijk dat de reiziger voordeel kan halen uit het gebruik van een gefraudeerde kaart. Dus dat de baten hoger zijn dan de kosten. De kosten in deze business case bestaan uit de directe kosten van aanschaf materiaal en eventueel software. Verder zijn er indirecte kosten in termen van 'transactiekosten' voor de fraudeur, ofwel de inspanning die een fraudeur moet plegen om de fraude uit te voeren. Tot slot is er de 'pakkans maal sanctie' die wordt meegenomen. Bij een hoge pakkans en sanctie is de business case minder aantrekkelijk. De baten in de business case zijn in dit geval het gratis vervoer.

   Onze aannamen voor de kosten voor een fraudeur zijn als volgt: aanschaf kaart € 7,50, afschrijving NFC reader, € 2. Daarnaast moet de fraudeur een inspanning plegen; er moet software worden verkregen en geïnstalleerd, er moet een aantal handelingen worden verricht op een computer, er is tijdsbesteding nodig voor het verkrijgen van een nieuwe kaart als de oude wordt geblokkeerd. Uitgaande van een monetaire prijs[1] van één uur van circa €10 en een tijdsbesteding van circa 10 minuten per fraudehandeling komt dit op circa €1,50 aan administratieve lasten. Totale kosten van een gefraudeerde kaart is dus circa € 11,-. Op basis van bekende fraude in het OV-domein kan de fraudebereidheid worden afgeleid – exclusief 'pakkans maal sanctie'. Deze wordt door ons ingeschat op 15 tot 20%, gerelateerd aan de cijfers over zwartrijden.

   De pakkans schatten wij in als relatief laag, maar de boete voor frauderen met een OV-chipkaart is hoog, zie paragraaf 2.5. Door de relatief hoge boete voor misbruik van de

[1] Indicator administratieve lasten burgers, SEO in opdracht van ACTAL, 2006

chipkaart, schatten wij in dat de fraudebereidheid wordt beperkt tot 2 à 3%. Iedere dag worden momenteel ruim 15.000 reizen (op saldo) gemaakt met een minimale waarde van € 7,50. De gemiddelde waarde van deze reizen is € 11,08. Zoals de business case laat zien zijn deze reizen interessant voor een fraudeur. 3% fraude houdt in dat er bij 450 reizen gefraudeerd wordt. De impact hiervan is ca € 5.000,- per dag of € 150.000,- per maand. Bij gemiddeld twee reisbewegingen per dag horen circa 200 gefraudeerde kaarten.

2. Ophogen van saldo en het verzilveren daarvan aan een balie van een OV-bedrijf of via de backoffice.

Dit scenario is vergelijkbaar met scenario 1. Verschil is echter dat de fraudeur niet gaat reizen, maar dat de fraudeur tracht het illegaal opgehoogde saldo bij een balie in contanten te laten uitkeren.

Dit scenario is reëel en kan worden toegepast door fraudeurs. De afgesproken maximale restitutie per kaart is € 30. Bij gemiddeld 100 gefraudeerde kaarten is het maximale schadebedrag per dag € 3.000. Per maand is dit € 90.000.

Sinds twee weken is een proces ingericht dat bij restitutie een restitutieformulier moet worden ingevuld en de kaarthouder zich bij uitbetaling moet legitimeren. Daarnaast zijn de meeste balies uitgerust met camera's. Hierdoor verwachten we op dit moment dat deze restitutiefraude marginaal is. Bij de balies van NS is op dit moment geen patroon zichtbaar dat, na het publiceren van de software, het aantal restituties is toegenomen. Dit onderbouwt onze aanname dat restitutiefraude daadwerkelijk marginaal is.

3. Het 'thuis' inchecken

Bij dit scenario worden door de fraudeur de kaartsleutels gekraakt, wordt het image met kaartgegeven apart gezet, wordt een check-in transactie gemanipuleerd en wordt het image met de nagemaakte check-in weer op de kaart geplaatst. Bij controle van een kaart blijkt de kaart een 'geldige' check-in te bevatten en laat de controleur de betreffende reiziger passeren.

Dit scenario wordt op dit moment naar verwachting nog vrijwel niet toegepast, omdat de noodzakelijk software op internet pas sinds kort beschikbaar is en nog niet optimaal werkt.

De business case van 'thuis inchecken' is vergelijkbaar met de business case van het verhogen van het saldo op de kaart. Dit fraudescenario vooral wordt toegepast bij het reizen met de trein. Dit komt doordat veel bus- en tramlijnen een gesloten instapregime kennen (inchecken onder toezicht van bestuurder of conducteur) en doordat bij een metroreis in de meeste gevallen gebruik wordt gemaakt van een gesloten poort. Daarnaast zijn voor een check-in in de bus of tram meer gegevens nodig (zoals een voertuignummer) die niet triviaal zijn en waarop door de controleur op het voertuig kan worden gecontroleerd.

In dit scenario zijn de kosten voor een fraudeur, voor zolang er geen transactie aan boord van de trein plaatsvindt, lager. Immers, de kaart wordt vooralsnog niet geblokkeerd. Dit betekent dat vooralsnog de kosten voor een nieuwe kaart en de administratieve lasten die hierbij horen, nog niet in de business case kunnen worden meegenomen. Ook schatten wij in dat op dit moment de pakkans in de trein zeer laag is. Wel moet de software nog breed beschikbaar komen en zal de maatregel om een transactie aan boord aan te maken binnen

afzienbare tijd worden gerealiseerd. Om deze reden gaan wij uit van een scenario met maatregel en een scenario zonder maatregel.

Zonder maatregel 'transactie aanmaken aan boord': de impact is significant hoger dan scenario 1. Wij gaan uit van een fraudebereidheid die stijgt van 2-3% naar ongeveer 10%. Omgerekend komt dit neer op ca € 15.000,- per dag of € 500.000,- per maand. Wij gaan uit van circa 750 kaarten per maand. Met maatregel 'transactie aanmaken aan boord': de business case en impact zijn gelijk aan scenario 1 ongeveer € 150.000,- per maand. Hierbij zijn ook ongeveer 200 kaarten in het geding.

4. **Productmanipulatie**
   Op blogs wordt melding gemaakt van productmanipulaties. Dit betreft het illegaal kopiëren van een product op een anonieme kaart. Ook wordt melding gemaakt van fraude met het studentenreisproduct waarbij week-reisrecht gewisseld wordt met weekeind-reisrecht. Deze vorm van fraude is herkenbaar in de backoffice van TLS. In principe staan deze producten op een persoonlijke OV-chipkaart, waardoor opsporing eenvoudiger is. De business case van productmanipulatie is vergelijkbaar met de business case van het verhogen van het saldo op de kaart.

   De business case en impact zijn gelijk aan scenario 1,ongeveer 150.000,- per maand. Hierbij zijn ongeveer 200 kaarten in het geding.

De fraudebereidheid bij reizigers is een gegeven, waardoor de impact van de drie genoemde effectieve fraudescenario's niet zonder meer bij elkaar mogen worden opgeteld. Gezien de grote onzekerheid in de schatting stellen wij dat de impact van de fraude totaal ingeschat mag worden op 200 tot 500 kaarten met een financiële impact van € 200.000,- tot 400.000,- per maand. Totdat controle aan boord mogelijk is wordt rekening gehouden met 750 gefraudeerde kaarten en impact van ongeveer € 750.000,- per maand.

Uitgaande van het feit dat twee tot drie dagen met een gefraudeerde kaart kan worden gereisd alvorens deze wordt geblokkeerd, kunnen we aannemen dat er dagelijks 100 tot 250 nieuwe gefraudeerde kaarten in omloop worden gebracht. Op basis van de gemiddeld 50 gefraudeerde kaarten per dag die wij op dit moment zien, lijkt de impact een reële inschatting.

4.2 Criminel,e business case

De hierboven beschreven scenario's zijn gebaseerd op individueel gebruik. Op dit moment leent alleen de verkoop van kaarten met illegaal verhoogd saldo of productfraude zich voor het illegale circuit. Bij 'thuis inchecken' moet steeds voorafgaand aan een reisbeweging de stationscode en het reistijdstip aangepast worden. Dit soort services on-line aanbieden is te risicovol ten opzichte van het potentieel gewin. Ook restitutie aan de balie is niet interessant. Een crimineel moet steeds met risico van ontdekking een restitutie bij een balie aanvragen. Het gewin hierbij is circa € 20 per keer. Voor grote bedragen moet de crimineel zich te vaak bekendmaken.

Bij illegale ophoging is het gemiddelde gewin per kaart circa € 40 (twee dagen reizen à € 22,- per dag). De maximale verkoop per dag wordt ingeschat op 50-100 kaarten. Daarbij heeft de crimineel een dagomzet van € 2.000 en € 4.000. Bij de verkoop van 50-100 kaarten per dag loopt de fraudeur aanzienlijk risico op ontdekking. De strafmaat op verhandelen van gefraudeerde kaarten is erg hoog. Dit kan oplopen tot zes jaren celstraf en € 74.000 boete. De pakkans is aanzienlijk en het gewin is beperkt.

Productfraude wordt door check-in en check-uit gegevens snel gedetecteerd, zodat slechts enkele dagen gereisd kan worden met een verkregen gemanipuleerde kaart. De situatie voor

een crimineel is dan gelijk aan de situatie met illegale ophoging van de kaart. Er moeten teveel kaarten worden verkocht om een interessante dagopbrengst te genereren. Bij verkoop van een grote hoeveelheid kaarten is de pakkans aanzienlijk.

Geconcludeerd kan worden dat gezien de beperkte omzet en de hoge strafmaat het niet realistisch is dat criminele organisaties zich gaan richten op handel in gefraudeerde OV-chipkaarten.

4.3 Overige fraude scenario's

De fraudescenario's die sinds 2008 bekend zijn, worden periodiek geactualiseerd. Dit is ook recent gebeurd. Naast de voornoemde actuele scenario's zijn ook andere mogelijke fraudescenario's uitgewerkt. Hierbij valt onder andere te denken aan het manipuleren van producten (abonnement) op de OV-chipkaart of het ongedaan maken van een blokkade van een kaart. Voor elk van deze scenario's zijn één of meerdere fraudedetectieregels in de backoffice actief. Fraude wordt hierdoor opgemerkt, waarna de betreffende kaart op de blokkeringlijst wordt gezet en de kaart bij eerstvolgend gebruik in de komende dagen wordt geblokkeerd.

4.4 Wat is nieuw?

Zwartrijden in het openbaar vervoer door vervoerbewijzen te manipuleren of te reizen zonder vervoerbewijs is van alle tijden. Met de komst van de OV-chipkaart is detectie niet alleen mogelijk in het voertuig, maar ook in de backoffice. Bij gesloten poorten is er een nieuwe barrière ten opzichte van de situatie met papieren vervoerbewijzen. Dat op gezette tijden dieven en fraudeurs nieuwe gaten vinden, die dan weer gerepareerd moeten worden, is een onvermijdelijk fenomeen voor elk betaalsysteem.

Vooralsnog staat vast dat ook bij de huidige stand van zaken de opbrengstderving bij gebruik van de OV-chipkaart kleiner is dan bij het gebruik van de papieren vervoerbewijzen.

5. Maatregelen

In dit hoofdstuk zijn op hoofdlijnen de maatregelen beschreven die wij nemen om de geconstateerde fraude met de OV-chipkaart van de afgelopen weken tegen te gaan. Een aantal maatregelen moet eerst verder uitgewerkt worden, voordat tot invoering kan worden overgegaan. Hierbij worden impact, mogelijke implementatietermijn en benodigde middelen nadrukkelijk onderzocht. Uitwerking en invoering gaan altijd in overleg met de betrokken verantwoordelijke security officers van TLS en de OV-bedrijven. Gezien het vertrouwelijke karakter van deze maatregelen is hieronder een beschrijving op hoofdlijnen opgenomen.

5.1 Procedurele maatregelen

1. Hogere frequentie van controles in de backoffice

Tot medio januari was vrijwel geen sprake van fraude met de OV-chipkaart. Door de verhoogde media-aandacht, maar ook doordat frequenter fraude wordt geconstateerd door de backoffice van TLS, wordt nu met hogere frequentie gecontroleerd. Met name in het weekeinde zijn extra controles ingevoerd om er zeker van te zijn dat gefraudeerde kaarten direct op de blokkeringlijst worden geplaatst. Ook zijn afspraken gemaakt met leveranciers, zoals de leverancier van het transactiebackofficesysteem (OCL in HongKong, het bedrijf achter de Octopus card) om te kunnen ondersteunen als en waar nodig.

2. Beperken restitutiefraude

Het saldo op de kaart kan illegaal opgehoogd worden. Hierdoor bestaat de mogelijkheid dat fraudeurs dit saldo gaan restitueren bij een baliemedewerker. Een baliemedewerker kan niet controleren of er een legale oplaadtransactie heeft plaatsgevonden. De restitutieprocessen aan de balies zijn aangescherpt door identificatie van de kaarthouder aan een balie te vragen. Daarnaast is een maximum te restitueren bedrag van € 30 van toepassing. Volledige restitutie in geval van hogere bedragen vindt plaats door de backoffice van TLS. In de backoffice bestaat de mogelijkheid om de restitutie nauwkeuriger te onderzoeken. Door deze maatregel verwachten wij dat op dit moment deze restitutiefraude zeer onaantrekkelijk en daardoor ook marginaal zal zijn.

5.2 Systeemtechnische maatregelen

1. Het 'thuis inchecken' (vervalste check-in)

Zoals eerder al vermeld, is dit fraudescenario met name van toepassing in de open gebieden waar 'op de wal' wordt ingecheckt. In bus- en tramlijnen met een gesloten instapregime, waarbij toezicht plaatsvindt door bestuurder of conducteur, is dit scenario minder van toepassing. Ook wordt hier op voertuignummer gecontroleerd en dat is moeilijker te manipuleren. Ook bij de metro is dit fraudescenario niet van toepassing, omdat daar toegang wordt verleend via poortjes.
Op dit moment zijn geen controlemogelijkheden voor de vervalste check-in in de open gebieden. De controleapparatuur van de vervoerder ziet een 'geldige' check-in op de OV-chipkaart en laat de reiziger ongemoeid. Doordat bij de controle geen transactie wordt aangemaakt die in de TLS-backoffice kan worden gevalideerd, kan de fraudeur ongehinderd reizen.

De volgende preventieve maatregelen worden uitgewerkt:

- *Aanmaken transactie bij controle aan boord.*
  Dit is een uitbreiding op een bestaande inspectiemaatregel, waarbij ervoor wordt gezorgd dat er bij controle een transactie wordt aangemaakt. Nadat deze transactie naar de TLS- backoffice is verstuurd, wordt daar de vervalste check-in gedetecteerd en wordt de kaart op de blokkeringlijst geplaatst. De vervoerders moeten bij deze maatregel aanpassingen voorzien in de controleapparatuur en TLS moet de validatieregels uitbreiden. Het restrisico bij deze maatregel is dat kaarten die niet gecontroleerd worden vooralsnog in omloop blijven.
- *Toevoegen extra kenmerk aan transacties.*
  Bij deze maatregel wordt een extra kenmerk toegevoegd aan het check-in event, waardoor de vervalste check-in al direct herkend wordt bij de detectieapparatuur. Deze maatregel biedt ook een oplossing voor frauduleus saldo laden en productmanipulatie. Deze maatregel wordt eerst verder gespecificeerd en de risico's van invoering worden geanalyseerd.

2. ***Verbeteren blacklistfunctionaliteit***

   De blokkeringlijst is een effectief middel om gefraudeerde kaarten ontoegankelijk voor het systeem te maken. Een aantal voorzieningen wordt uitgewerkt om de effectiviteit van het blokkeringproces te verbeteren.

   Er zijn maatregelen die positief effect hebben op de distributie van de blokkeringlijst. Hierbij wordt ervoor gezorgd dat de blokkeringlijst sneller bij alle validatieapparatuur aanwezig is, maar ook vaker wordt gedistribueerd. Kaarten worden dan sneller geblokkeerd.

   Andere maatregelen hebben betrekking op de capaciteit van de blokkeringlijst en de exacte werking van de blokkeringlijst voor het permanent blokkeren van kaarten.

5.3 Invoeringsstrategie

Invoering van de maatregelen wordt uitgevoerd conform de governance, zoals die is afgesproken voor het OV-chipkaartsysteem. Binnen het OV-chipkaartsysteem zijn alle Deelnemers verantwoordelijk voor hun eigen componenten. Door het interoperabele karakter van het OV-chipkaartsysteem is het belangrijk om aanpassingen zorgvuldig te onderzoeken voordat deze bij de afzonderlijke Deelnemers worden geïmplementeerd.

Globaal worden 5 stappen onderscheiden:

Stap 0. Analyse. Het resultaat is vaak een zogenaamd High Level Design.

Stap 1. Change request. Aanvragen worden ingediend bij de Scheme provider. De Scheme provider heeft als taak de kernwaarden kaartinteroperabiliteit, productinteroperatibiliteit en systeemcompatibiliteit van het OV-chipkaartsysteem te bewaken

Stap 2: Het assessment. Binnen het assessment worden met name aan de hand van de kernwaarden en de risico's die gepaard gaan met de change beoordeeld.

Stap 3. Accepteren van de change door het NCAB. Hierin zijn alle Deelnemers vertegenwoordigd.

Stap 4. Uitwerken specificaties change. Dit mondt uit in een scheme note. Deze note wordt door het NCAB en NRB beoordeeld. Hier wordt besloten de change in te voeren.

Stap 5 Uitvoering. In deze fase gaan alle Deelnemers binnen hun eigen verantwoordelijkheid op basis van de Scheme note aanpassingen aan hun eigen systemen doorvoeren. Dit gaat middels de governance van iedere afzonderlijke Deelnemer. Kosten en doorlooptijd wordt door iedere Deelnemer zelf bepaald. Dit vaak in overleg met hun leveranciers. Iedere Deelnemer voert de change zelfstandig uit.

De OVC Security en Fraude manager bewaakt de samenhang van de maatregelen, maar ook dat het totaal aan beveiligingsmaatregelen wordt doorgevoerd. De maatregelen worden afzonderlijk behandeld en doorgevoerd.

5.4 Het migratieplan

TLS en de OV-bedrijven werken verder aan het migratietraject, dat voorbereidingen treft om over te kunnen gaan naar een nieuwe chip in de OV-chipkaart. Dit traject is reeds in 2009 in gang gezet, overeenkomstig de aanbevelingen van RHUL. In 2010 kon, door een financiële ondersteuning vanuit het ministerie en vanuit FENS, de feitelijke implementatie van de voorbereidingen in de backoffice en bij de apparatuur in het veld worden gestart. Het migratietraject is gebaseerd op de zogeheten SmartMX-chip van NXP. Dit is een processorchip met een hoger niveau van beveiliging. Op het chipplatform wordt de OV-functionaliteit door een applicatie (OV-applet) geladen. Per eind van het jaar kan volgens de huidige planning worden gestart met het uitgeven van de nieuwe chip in de OV-chipkaart. Hieraan voorafgaand zal een intensieve veldtest worden uitgevoerd met een gecontroleerde groep testreizigers.

Deze nieuwe chip biedt een hoger beveiligingsniveau dan de Mifare Classic chip die nu in gebruik is. 100% beveiliging bestaat echter niet. Ook met de nieuwe chip blijft het een 'ratrace' tegen fraudeurs en hackers. Het voornemen is om de chip in de OV-chipkaart te vervangen volgens natuurlijke vervanging. Dat wil zeggen dat wordt aangesloten bij het moment dat een OV-chipkaart (na vijf jaar) vervangen moet worden.

In de tussenliggende tijd is sprake van een duale situatie, waarbij Mifare classic en SmartMX naast elkaar in de markt bestaan. Om dit technisch te realiseren is de SmartMX chip in staat om de Mifare classic te emuleren, oftewel in een Mifare classic modus te werken. In die modus zijn de kaarten nog gevoelig voor fraude, hoewel ze wel bescherming bieden tegen een aantal van de huidige zwakheden van de Mifare classic. Als alle kaarten zijn vervangen en alle kaartleesapparatuur is aangepast, dan kan (in de software) de volgende verbetering van de beveiliging worden aangebracht. Dan kan het hogere beveiligingsniveau dat met de SmartMX-chip mogelijk is, worden bereikt. Een dergelijke laatste stap in de migratie is op dit moment, gezien de huidige schadeposten van fraude, omwille van bedrijfseconomische redenen nog niet te rechtvaardigen.

Opgemerkt wordt dat dergelijke migratietrajecten van grote systemen en grote hoeveelheden kaarten zorgvuldigheid vereisen en een langere doorlooptijd kennen.

5.5 Worst case scenario

Het migratieplan voorziet in een mogelijkheid tot versnelde vervanging. Als de fraude met de kaart onverhoopt grote vormen aanneemt, is er de mogelijkheid om niet via natuurlijke vervanging maar versneld een nieuwe chip uit te geven. Dit versnelde scenario gaat gepaard met 'geforceerde' vervanging van kaarten. Ook moet geforceerd kaartleesapparatuur worden aangepast. Een en ander brengt last voor de reizigers en hoge kosten met zich mee. Daarom wordt dit alleen dan uitgevoerd als er sprake is van noodzaak. De besluitvorming hieromtrent

is vastgelegd door de OV-bedrijven en TLS in het zogeheten 'decision framework' dat ook in de tijd door RHUL is beoordeeld.

TLS en de OV-bedrijven vinden het zeer onwaarschijnlijk dat we als gevolg van gefraudeerde OV-chipkaarten in een slechtere situatie zullen belanden dan in de tijd van de papieren vervoerbewijzen en strippenkaart het geval was.

6. NVB wel-uitzetten versus NVB niet-uitzetten

In dit hoofdstuk wordt, aanvullend op de vorige hoofdstukken, waarin is beargumenteerd dat sprake is van een beheerste en gecontroleerde situatie voor de fraudemogelijkheden met de OV-chipkaart, een aantal elementen benoemd die specifiek zijn voor het wel of niet uitzetten van het NVB (waaronder de strippenkaart) in een bepaald gebied.

6.1 Geen verhoogd frauderisico

Op dit moment is het in nagenoeg heel Nederland (met uitzondering van Groningen/Drente) mogelijk om te reizen met de OV-chipkaart. In gebieden waar een besluit voorligt om het NVB af te schaffen en over te gaan op alleen de OV-chipkaart is het al langere tijd mogelijk met de OV-chipkaart te reizen. Als men wil frauderen, dan kan dat nu dus al. Door het wel of niet uitzetten van het NVB wordt dit frauderisico niet groter (of kleiner). In die zin staat dus een besluit over het uitzetten van NVB los van het potentiële frauderisico. In de voorgaande hoofdstukken is beargumenteerd dat voor de fraude met de OV-chipkaart sprake is van een gecontroleerde en beheerste situatie en dat bonafide reizigers geen hinder ondervinden van het frauderen met de OV-chipkaart. Dit aangevuld met de maatregelen die TLS en de OV-bedrijven nemen om fraude verder te voorkomen of onaantrekkelijk te maken. Daarmee kan geconcludeerd worden dat de planning voor het uitzetten van het NVB en de besluitvorming daaromtrent onverkort kan worden doorgezet.

6.2 Fraude met papier

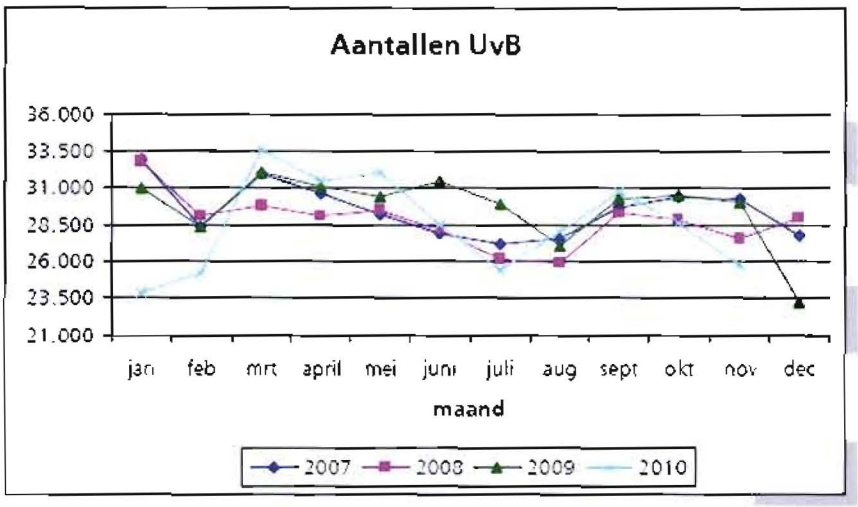
Ook met de papieren vervoerbewijzen vindt en vond fraude plaats. Dit geldt voor de strippenkaart, het treinkaartje, etc. Bij de meeste vervoerbedrijven en landelijke organisaties, zoals VBN, ontbreken betrouwbare cijfers over gefraudeerde vervoerbewijzen. In breder verband kan worden opgemerkt dat alles van waarde kan worden nagemaakt en dat er altijd gezocht blijft worden naar mogelijkheden om beveiliging van waardepapieren of betaalmiddelen te doorbreken en fraude te plegen. Het is een continu spel van kat en muis om beveiliging te ontwerpen en beveiliging te omzeilen of te doorbreken. 100% beveiliging is dus niet mogelijk.

Hieronder worden enkele voorbeelden van vervoerders genoemd, die een indruk geven van de fraude met papieren documenten.

Bij NS zijn in 2009 en 2010 bijna 10.000 vervoerbewijzen ingenomen. Het betreft hier verschillende vormen van fraude zoals personen die reizen met verloren of gestolen kaarten, maar ook aangepaste papierenkaartjes (traject/datum wijziging of verwijdering stempel). Daarnaast zijn personen aangehouden met grote hoeveelheden vervalste papieren kaartjes.

Het is moeilijk om in de papieren wereld vast te stellen wat de totale omvang van de fraude is, daar dit slechts vastgesteld kan worden met handmatige controle.

Bij NS worden dagelijks ongeveer 1.000 'uitstel van betalingen' (zie grafiek) uitgeschreven en zijn er vele reizigers die bewust niet afstempelen met de verwachting er bij controle 'mee weg te komen'.



Bij GVB in Amsterdam werd ten tijde van de strippenkaart bij de metro in 14% van de gevallen zwart gereden. Dit is op dit moment gedaald tot circa 4%. Dit laatste wordt niet veroorzaakt door fraude met de OV-chipkaart, maar door het forceren van poortjes of door illegaal met meerdere mensen tegelijk door een poortje te gaan. Zwartrijden in de metro in Amsterdam is per jaar met € 4 miljoen gereduceerd.

Bij RET in Rotterdam is het percentage zwartrijders gedaald van 10-12% in het papieren tijdperk naar 3,3% bij het reizen met de OV-chipkaart. Zwartrijden in de metro in Rotterdam is per jaar met € 3 tot 4 miljoen gereduceerd.

Na een volledige overgang naar de OV-chipkaart neemt de totale fraude naar verwachting af. OV-chipkaarten kunnen bij diefstal/verlies en fraude eenvoudig worden geblokkeerd en reizigers hebben een grotere kans op controle, doordat controle ook bij poortjes en paaltjes plaatsvindt. Ook is fraude met de OV-chipkaart veel zichtbaarder dan fraude met een strippenkaart. Zo is het voor de medereiziger niet te zien dat er te weinig strippen worden afgestempeld, terwijl te vroeg uitchecken opvalt.

TLS en de OV-bedrijven hebben verschillende maatregelen doorgevoerd om fraude te detecteren en blijven dit doen om fraude tegen te gaan. Fraude wordt zichtbaar en daarmee beheersbaar in het openbaar vervoer. Fraude wordt voor een groot deel geautomatiseerd gedetecteerd. Een situatie die in de 'oude' wereld niet mogelijk was.

In algemene zin kan worden gesteld dat de fraude met papieren vervoerbewijzen altijd nog groter en minder zichtbaar was dan met de OV-chipkaart nu mogelijk lijkt. Op basis van de informatie van enkele vervoerders is er sprake van een daling van het zwartrijden van 14% naar ca 4%. Dit komt neer op een reductie van het zwartrijden van ongeveer 70%.

6.3 Dubbele kosten

Twee systemen naast elkaar betekent dubbele kosten. Het in de lucht houden van papieren vervoerbewijzen (waaronder de strippenkaart) met bijbehorende distributie en verkoopkanalen naast het OV-chipkaartsysteem is een kostenfactor. In de huidige situatie (waarbij dus alleen het NVB in de stadsregio's Rotterdam en Amsterdam is uitgezet) wordt uitgegaan van een kostenpost voor stad- en streekvervoerders van tussen de € 10 à 15 miljoen voor 2011 (GVB en RET hebben beiden geen kosten NVB meer). NS raamt de kosten om twee systemen naast elkaar te laten bestaan op minimaal € 10 miljoen per jaar.

6.4 Verwarrend voor de reiziger

Twee systemen naast elkaar betekent ook dat in de praktijk verwarrende situaties kunnen ontstaan voor de reiziger en dat operationele problemen het gevolg kunnen zijn. Dit betreft onder andere het reizen van een volledig verchipt gebied naar een gebied waar de strippenkaart nog geldig is (en vice versa). Hier worden tijdelijke maatregelen getroffen waarover verwarring ontstaat. Daarnaast geldt dat de voordelen van het OV-chipkaartsysteem nog niet in alle gevallen ten volste kunnen worden aangewend. Het wennen aan de OV-chipkaart en de overgang van papier naar chip wordt gespreid over een veel langere periode, waardoor de gewenning veel langzamer verloopt.

NS koerst op sluiting van de poortjes eind 2012. Daarvoor is randvoorwaardelijk dat het papieren vervoerbewijs is afgeschaft. Tot die tijd bestaan bij NS het papieren kaartje en de OV-chipkaart naast elkaar. Het zou dus om diverse redenen onwenselijk zijn deze situatie langer te handhaven.