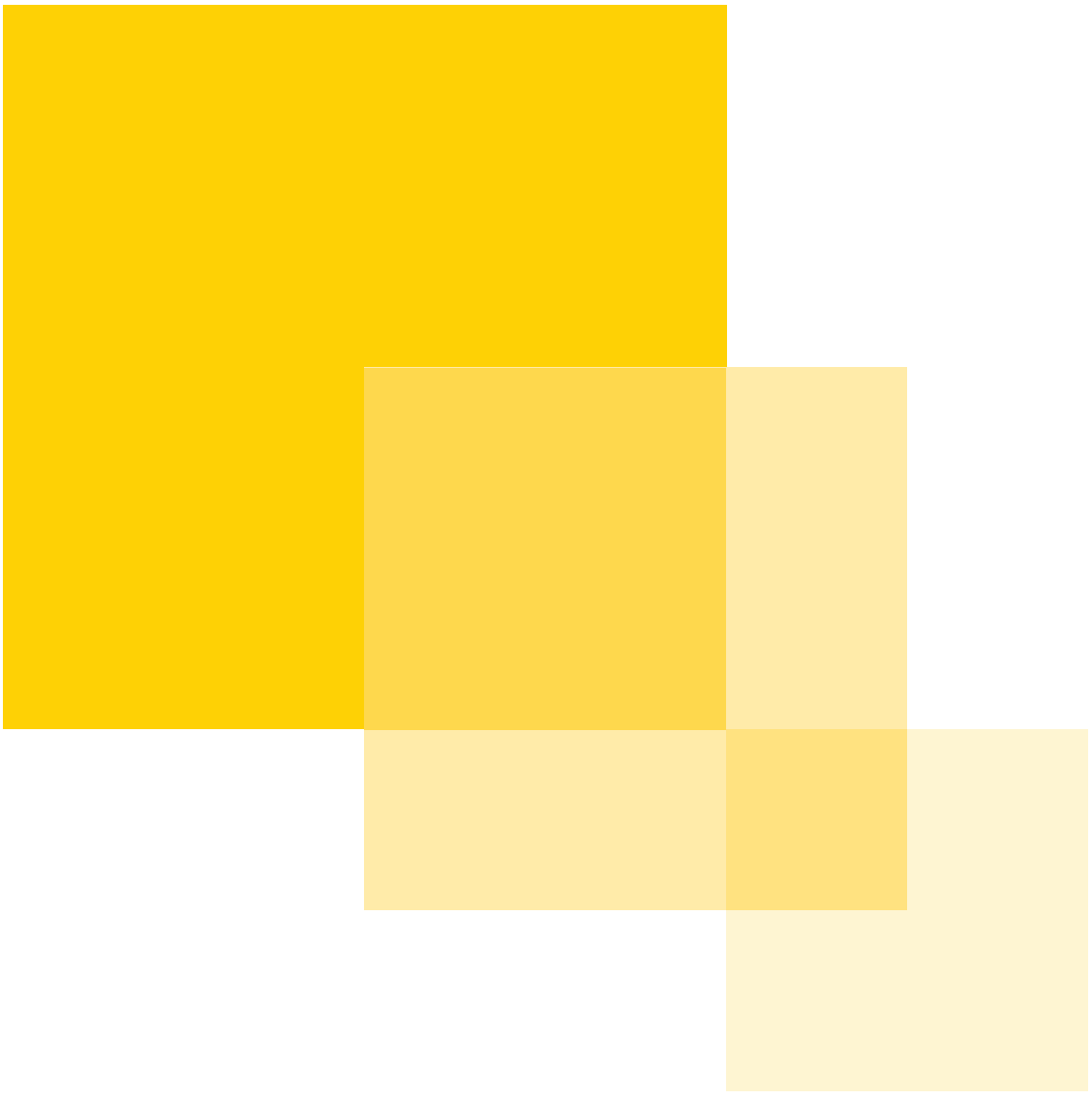
BETER BEWAPEND TEGEN FRAUDE

Hoe wagenparkbeheerders voorop kunnen blijven lopen in de mondiale strijd tegen tankpasfraude



BETER BEWAPEND TEGEN FRAUDE

Hoe wagenparkbeheerders voorop kunnen blijven lopen in de mondiale strijd tegen tankpasfraude

TWEE SECTOREN DIE BEIDE GROEIEN

Door de voorkeur van kopers voor het gemak van betalen zonder contant geld is de mondiale betaalkaartsector de afgelopen twintig jaar fors gegroeid. Naar verwachting zullen de betalingen met dit zogeheten 'plastic geld' – bankpassen of creditcards – de komende jaren nog sneller in aantal groeien. Het gebruik van tankpassen stijgt navenant en deskundigen voorspellen verdere wereldwijde groei, vooral onder wagenparkexploitanten van zowel lichte als zware voertuigen.

Meer gebruik betekent helaas ook meer misbruik. Fraude met betaalpassen is bepaald geen nieuw verschijnsel, maar door het groeiende aantal niet-contante transacties krijgen criminelen ook meer kans. Sterker nog, het inbreken in niet-contante betaalsystemen in alle sectoren is inmiddels zelf een groeiende industrie geworden.

Voor wagenparkbeheerders, voor wie brandstof tot wel dertig procent van de operationele kosten vormt, is het nu dus des te meer van belang om de veiligheid van tankpasbetalingen te waarborgen.

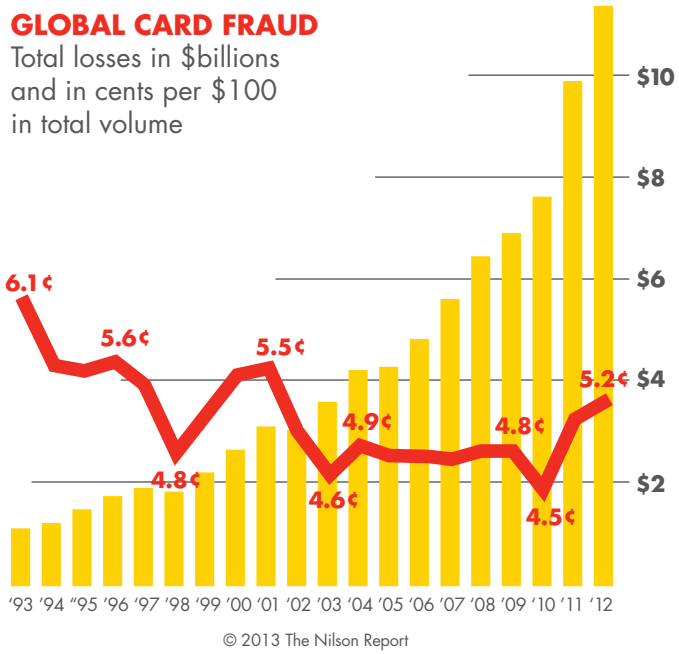
In dit witboek geven wij weer voor welke uitdagingen de snelle mondiale verbreiding van betalen zonder contant geld, en daarmee het groeiende criminaliteitsrisico, ons stelt. Wij kijken daarbij wat dit betekent voor tankpasgebruikers in het bijzonder. Tot slot bespreken wij verschillende moderne technologieën, die klanten kunnen gebruiken om het risico van fraude aan de pomp te bestrijden, zoals een scala aan geavanceerde brandstofmanagementoplossingen, dat Shell biedt.

FRAUDULEUZE ACTIVITEITEN BIJ NIET-CONTANTE TRANSACTIES

Volgens het CapGemini World Payments Report 2013 is het mondiale gebruik van bankpassen in 2011 met 15,8 procent gestegen tot een recordaantal van 124 miljard transacties. Het aantal creditcardbetalingen steeg eveneens, met 12,3 procent tot in totaal 57 miljard transacties. Met de zich ontwikkelende markten in Afrika, Latijns-Amerika en Azië aan kop groeide het totaal van alle niet-contante betalingen – waaronder ook tankpas- en mobiele betalingen - met 8,8 procent, tot 307 miljard afzonderlijke transacties. Over de hele wereldbevolking bezien, is dat gemiddeld meer dan 40 transacties per persoon.

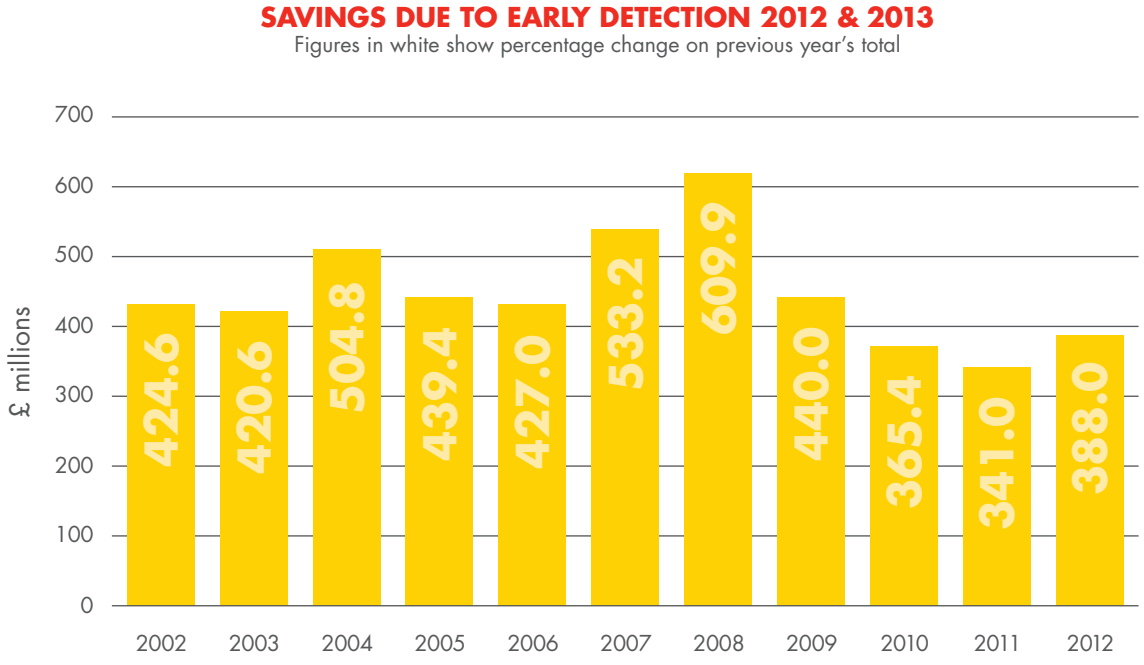
Bij wagenparken stijgt het aantal betalingen met tankpassen eveneens. Steeds meer wagenparkbeheerders kiezen ervoor om hun chauffeurs de vrijheid, het gemak en de controle geven om met een tankpas op kosten van het bedrijf te tanken. Feit is dat wereldwijd jaarlijks tot wel 260 miljoen transacties met Shell-tankpassen worden gedaan.

Maar ook criminelen volgen deze ontwikkeling nauwlettend. Volgens recente gegevens van Nilson bedroegen de wereldwijde kosten van betaalpasfraude in 2012 ruim elf miljard dollar, tegen slechts $ 1 miljard in 1993 [Zie Figuur 1]. Dit cijfer omvat alles, van aanhoudende, gecoördineerde aanvallen door georganiseerde criminele groepen tot specifieke, eenmalige acties van individuen die uit zijn op wat snel geld of een keer gratis winkelen of tanken.



FIGUUR 1: jaarlijkse mondiale verliezen door betaalpasfraude sedert 1993

Het probleem beperkt zich geenszins tot ontwikkelingsmarkten; betaalpasfraude gebeurt nog steeds overal ter wereld. In het Verenigd Koninkrijk, bijvoorbeeld, bedroegen de jaarlijkse verliezen in 2012 388 miljoen pond, 14 procent hoger dan in 2011 . Wel interessant om op te merken is dat beide cijfers lager zijn dan de piek van 610 miljoen pond in 2009, toen de wereldeconomie op instorten stond [Zie Figuur 2]. In de Verenigde Staten waren de jaarlijkse verliezen volgens een recente schatting ruim vijf miljard dollar.



FIGUUR 2: jaarlijkse verliezen door betaalpasfraude in het verenigd koninkrijk sedert 2002

Wat de data in toenemende mate duidelijk maken, is dat er tegen betaalpasfraude op mondiaal niveau moet worden opgetreden. In veel landen slaan overheid, rechtshandhavingsinstanties, bedrijfsleven en consumentengroepen inmiddels de handen ineen in een gecoördineerde poging om die fraude te bestrijden.

Voor wagenparkbeheerders is het essentieel dat zij eerst inzien welke specifieke misdrijven met hun tankpassen kunnen worden gepleegd, voordat zij actief maatregelen treffen om die te voorkomen.

"Het belangrijkst om te onthouden is dat een tankpas eigenlijk gewoon een creditcard of een bankpas is. Ik ben ervan overtuigd dat als wagenparkexploitanten en chauffeurs de veiligheid van hun tankpas even serieus zouden nemen als die van hun eigen betaalpas, zij veel minder risico zouden lopen om slachtoffer van fraude te worden."

Aran Kankiwala, Shell Global Fraud Case Manager

FRAUDE AAN DE POMP... EN DAARBUITEN

Brandstof is en blijft een van de meest waardevolle goederen ter wereld. Dit betekent dat veel criminelen er een dagtaak van hebben gemaakt om dit te bemachtigen, door brandstof te stelen of door lekken in het betaalsysteem uit te buiten. Daardoor verliest de wagenparksector jaarlijks miljoenen aan tankpasfraude. Het is een probleem dat alle landen en alle tankpasaanbieders treft.

Bovendien worden de fraudetechnieken steeds geavanceerder. Recente trends laten zien dat criminelen inmiddels het onderscheid tussen wagenparkbeheerders van zware vrachtwagens (HGV) en van bestelauto's (LGV) begrijpen. Deze kennis benutten ze om wagenparkbeheerders op verschillende manieren aan te vallen om er maximaal profijt van te behalen.

Om dit te illustreren, vermeldt onderstaande Figuur 3 de meest voorkomende soorten fraude waar de tankpassector last van heeft. Figuur 4 laat zien hoe die verschillende soorten fraude specifiek op bepaalde typen klanten worden gericht.

Gekopieerde tankpas: Dit gebeurt als de magneetstrip van de betaalpas illegaal wordt gekopieerd Dit wordt meestal gedaan nadat een crimineel op een andere manier al achter de pincode is gekomen Het is belangrijk om te vermelden dat de pincode niet van de magneetstrip zelf kan worden afgelezen.

Valse tankpassen: Er worden compleet valse kaarten gemaakt, waarmee vervolgens frauduleuze aankopen worden gedaan.

Misbruik van verloren of gestolen tankpas: Een betaalpas wordt gestolen of raakt kwijt en wordt vervolgens misbruikt, meestal zodra de pincode op een andere manier is afgekeken.

Misbruik van echte tankpas: De originele betaalpas wordt boven de betaallimiet of afwijkend van het normale tankpatroon gebruikt, bijvoorbeeld het bijtanken van meerdere auto's, die niet van de zaak zijn, met een tankpas van een wagenparkbeheerder.

Aanvraagfraude: Er worden valse klantgegevens en/of spookbedrijven gecreëerd om valse bankrekeningen te openen waarop het negatieve saldo nooit wordt ingelost. Ook worden legitieme klantrekeningen 'gekaapt' zodat daarvoor extra betaalpassen kunnen worden aangevraagd, die vervolgens voor frauduleuze doeleinden worden gebruikt.

FIGUUR 3: de meest voorkomende soorten tankpasfraude

Gekopieerde tankpas: Het aantal gevallen van gekopieerde tankpassen onder LGV- en HGV-klanten ontloopt elkaar niet veel. Meestal gebeurt dit met mobiele, draagbare apparaten, omdat de veiligheidsmaatregelen op tankstations en betaalterminals het voor criminelen lastig maken om skimapparatuur te plaatsen.

Namaaktankpassen: Deze worden uitsluitend zonder pincode gebruikt, omdat het nooit de bedoeling is geweest om aan de tankpas een pincode toe te wijzen. Namaakfraude kwam vroeger vaak voor maar is dankzij pincodetechnologie grotendeels uitgeroeid en vormt nog maar een gering percentage van het totaal aantal gevallen van pasfraude.

Misbruik van verloren of gestolen tankpas: Hoewel ook het aantal gevallen van gestolen tankpassen onder LGV- en HGV-klanten elkaar niet veel ontloopt, zijn de verliezen onder HGV-klanten tot wel vier maal zo hoog, omdat hun tankpassen meestal een hogere limiet per tankbeurt hebben. Daardoor kunnen criminelen meer brandstof tanken voordat de fraude wordt ontdekt. Bovendien vormen HGV-klanten een makkelijker doelwit, omdat criminelen de gebruikelijke transportroutes kennen en weten welke parkeerplaatsen onveilig zijn en waar diefstal dus het eenvoudigst is. Het merendeel van de tankpassen wordt uit voertuigen gestolen en niet van de chauffeurs zelf.

Misbruik van originele tankpas: Dit komt vaker bij LGV-beheerders voor omdat die in veel gevallen hun tankpassen minder streng kunnen controleren. Vaak heeft zo'n bedrijf meerdere chauffeurs, die op dezelfde dag dezelfde tankpas gebruiken, wat het lastiger maakt om misbruik te signaleren. Maar ook HGV-klanten kunnen dit ondervinden door ploegendiensten en doordat meerdere chauffeurs dezelfde truck gebruiken.

Aanvraagfraude: Gevallen van aanvraagfraude komen het vaakst voor in de LGV-sector, want door de geringere bedrijfsgrootte van LGV-klanten zijn hun bedrijfsgegevens eenvoudiger te vervalsen.

FIGUUR 4: fraude met tankpassen bij lgv- en hgv-klanten

EEN OUD PROBLEEM; EEN AANTAL NIEUWE OPLOSSINGEN

Te midden van al deze uitdagingen is het goede nieuws dat, ook al worden criminele tactieken steeds geavanceerder en gerichter, ook de technieken om hen te bestrijden steeds verfijnder worden. Veel van de instrumenten, die nodig zijn om frauduleus gedrag voor met name wagenparkbeheerders te bestrijden, bestaan al, ondanks dat het aantal individuele tankpastransacties blijft groeien.

Bij deze oplossingen gebruikt men de meest geavanceerde fraudebestrijdingstechnologieën die er zijn, zoals online brandstofmanagementsystemen, telematica en vierentwintiguurs-bewaking rond de klok, met proactieve reactie. Zorgen dat iedereen toegang tot deze hulpmiddelen heeft, kan dus een grote stap vooruit zijn om het probleem uit de wereld te helpen.

Maar zoals bij veel van de problemen waarmee bedrijven in de loop der jaren te maken hebben gehad, zou de eerste en belangrijkste stap die wagenparkbeheerders moeten nemen, wel eens de meest voor de hand liggende kunnen zijn …

FRAUDE VASTPINNEN

Veruit de meeste gevallen van tankpasfraude zijn toe te schrijven aan kaartmisbruik met de pincode. Omdat de pincode niet van de betaalpas zelf kan worden afgelezen, wordt die meestal met verschillende technieken bemachtigd - die allemaal zijn gebaseerd op onzorgvuldig omgaan met de pincode.

Simpel gezegd, maken mensen die onzorgvuldig met hun pincode omgaan het voor criminelen erg makkelijk. Door de pincode op te schrijven en bij de betaalpas te bewaren of door het pinapparaat tijdens het pinnen niet met de andere hand af te schermen, krijgen fraudeurs de kans om bij de betaalgegevens van het bedrijf te komen en criminele aankopen te doen. Volledige voorlichting en training voor chauffeurs en personeel over het correct omgaan met hun pincode kunnen dus veel fraudegevallen binnen de tankpassector uit de wereld helpen en dat vrijwel van de ene op de andere dag.

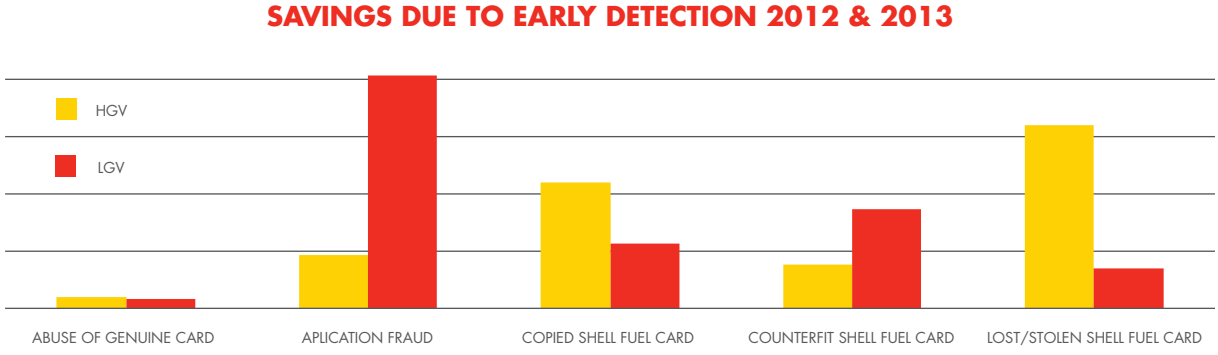
"De meeste mensen zouden nooit een papiertje met daarop hun pincode bij hun betaalpas of creditcard in hun portemonnee bewaren. Maar als het om tankpassen gaat, zien wij bij chauffeurs nog steeds talloze voorbeelden daarvan. Daarmee maak je het voor criminelen wel erg makkelijk."

Aran Kankiwala, Shell Global Fraud Case Manager

Hoewel het van vitaal belang is om chauffeurs te leren zorgvuldiger met de pincode van hun tankpas om te gaan, is dit natuurlijk allerminst een allesomvattende oplossing. Veel van de meer geavanceerde soorten crimineel gedrag, waaronder het kopiëren van tankpassen, valse rekeningnummers en misbruik van echte tankpassen, vergen technisch hoogstaande fraudebestrijdingsoplossingen.

De brandstofmanagementinstrumenten van Shell zijn er dan ook op gemaakt om precies datgene te doen: geavanceerde fraudedetectietechnologie, die de veiligheidsrisico's minimaal houdt, gecombineerd met een snelle, proactieve reactie in het zeldzame geval waarin van crimineel handelen sprake is.

Dit kan op zijn beurt weer helpen om drukbezette fleetmanagers meer armslag te geven, zodat zij zich niet uitsluitend op beveiligingsaspecten hoeven te richten, maar ook aandacht kunnen schenken aan de bredere operationele aspecten van hun hele wagenpark, zoals verlaging van de CO^2-uitstoot, prestatieverbetering en minimalisering van de kosten.



FIGUUR 5: besparingen door shell-klanten in de laatste twee jaar, dankzij technieken voor vroegtijdige detectie en waarschuwing voor lgv- en hgv-beheerders die mogelijk doelwit van fraude zijn

Belangrijke onderdelen van het totale fraudepreventiepakket van Shell zijn onder meer:

Shell Card Online is een multifunctioneel, online brandstofmanagementsysteem, dat specifiek is ontworpen om de veiligheid van een wagenpark gemakkelijker en efficiënter te kunnen beheren. Het systeem biedt toegang tot iedere Shell-tankpastransactie op een bepaald rekeningnummer. Transactierapporten vermelden in detail waar, wanneer en door wie (als de tankpas op naam van een chauffeur staat) een tankpas is gebruikt, plus type en hoeveelheid van de gekochte brandstof. Gebruikers kunnen ook maximale tankvolumes instellen en per e-mail gepersonaliseerde signaleringen op basis van specifieke criteria krijgen, zoals een tankpas die buiten werktijd wordt gebruikt of een maximumvolume dat bij een bepaalde transactie wordt overschreden. Hierdoor kan potentieel frauduleus gedrag vroegtijdig worden opgespoord en, wat belangrijker is, men kan snel ingrijpen.

Real Time Detection (RTD) is de nieuwe fraudeopsporingstechnologie van Shell, waarmee zij binnen enkele seconden crimineel gedrag kan signaleren. Volgens hetzelfde systeem dat banken gebruiken om fraude met creditcards op te sporen, filtert RTD op basis van specifieke betaalparameters de 260 miljoen transacties die jaarlijks met Shell-tankpassen worden gedaan. Vervolgens gebruikt zij die informatie om verdachte handelingen in real time, dus direct, te markeren. Voor de klant betekent dit dat frauduleuze handelingen die eerder misschien onopgemerkt bleven, nu sneller en nauwkeuriger dan ooit tevoren kunnen worden gesignaleerd en dat daarop passende actie kan worden genomen.

Shell FuelSave Partner biedt geavanceerde brandstof- en fleetmanagementoplossingen voor beheerders van zware wagenparken. De gebruiker kan het brandstofverbruik van de voertuigen en de chauffeursprestaties volgen en daarna suggesties voor operationele verbetermogelijkheden doen. Aangetoond is dat dit tot wel tien procent brandstof bespaart en daardoor ook de brandstofgerelateerde CO^2-uitstoot verlaagt. Omdat het systeem is geïntegreerd met de euroShell Card kan het fleetmanagers helpen om potentieel frauduleuze handelingen te identificeren, door aankoopgegevens met een tankpas en de feitelijke brandstofinformatie uit de tank tegen elkaar aan te houden.

Shell beschikt over een speciaal team van casemanagers en analisten op het gebied van fraude die elke betaling met een Shell-tankpas, waar ook ter wereld, met geavanceerde software kunnen volgen. Daardoor kunnen zij een vermoedelijk frauduleuze handeling op een bepaalde rekening snel en proactief opsporen – en kunnen ze vervolgens met grote precisie reageren. Alleen al in 2013 hebben klanten dankzij de fraude-experts van Shell ruim vier miljoen dollar bespaard.

De beveiliging op Shell-stations voldoet aan de nieuwste internationale normen. Er is een team van terreinbeheerders en veiligheidsadviseurs, dat als specifieke opdracht heeft om de veiligheid van elke afzonderlijke site en de betaalsystemen daarvan te garanderen. Veel Shell-stations gebruiken ook een gesloten televisiesysteem.

DE STRIJD GAAT VERDER

Zolang de wereld naar niet-contante betalingen verlangt, zal ook betaalpasfraude blijven bestaan. En hoewel aanvallen zelden voortdurend één onderneming treffen, lopen bedrijven die bij de ontwikkelingen achterblijven meer risico om aanhoudend doelwit van fraude te worden.

Voor wagenparkbeheerders is het van vitaal belang om met een tankpasaanbieder te werken, die een volledig scala aan hulpmiddelen en technologieën ter bestrijding van crimineel gedrag biedt. De tactieken, die fraudeurs gebruiken, worden constant verfijnd. Voor fleetmanagers betekent dit, dat gebruik maken van de meest geavanceerde antifraudetechnieken de optimale route naar succesvolle beveiliging is. Deze systemen moeten bovendien worden aangevuld met constante personeelsvoorlichting over het belang van goed omgaan met de pincodes van tankpassen.

Voor ons, als Shell, is onze plicht intussen duidelijk: de tegenstander een stap vóór blijven. Fraude is er altijd geweest en zal er altijd blijven, maar met onze speciaal opgeleide medewerkers en onze geavanceerde managementsoftware lopen wij nu al voorop bij het opsporen van en het ingrijpen bij criminele activiteiten met tankpassen. Tegelijkertijd blijven wij ook nieuwe en geavanceerde technieken onderzoeken, om de fysieke veiligheid van tankpassen in de toekomst te kunnen verbeteren.

Wat betekent dit alles in de strijd tegen betaalpasfraude? Zeker - naarmate bedrijven beter toegerust raken om fraude te voorkomen en op te sporen, trekken diegenen die aan de goede kant van de wet staan steeds vaker aan het langste eind. Maar alleen door onze fraudepreventiemethoden constant verder te verfijnen, opnieuw uit te vinden en te vernieuwen kan de wereldwijde strijd ooit daadwerkelijk worden gewonnen.

Voor meer informatie over dit witboek of om te bespreken hoe uw bedrijf van de verschillende antifraudeoplossingen van Shell kan profiteren, kunt u contact opnemen met uw accountmanager.