POLITIE

- Bovenregionale Recherche
- Noordwest & Midden Nederland

Aanbevelingen voor het registreren van prepaid telefoonkaarten

Ervaringen naar aanleiding van het rechercheonderzoek Apollo.

E. Langedijk

Heemskerk, april 2008

POLITIE
- Bovenregionale Recherche
- Noordwest & Midden Nederland

Voorwoord

Deze notitie is geschreven naar aanleiding van bevindingen die zijn opgedaan tijdens het rechercheonderzoek Apollo, uitgevoerd in de periode 2 oktober 2006 tot 1 november 2007. Het onderzoek werd verricht door o.a. de Bovenregionale Recherche Noordwest & Midden Nederland en richtte zich op West-Afrikaanse Criminele Netwerken (WACN) die zich met name bezighouden met oplichting, zogenaamde 419 fraude (zie hierna).

Gedurende het onderzoek werd het anoniem gebruik kunnen maken van prepaid telefoonkaarten door het rechercheteam als een knelpunt ervaren. De vraag rees tevens of ook het maatschappelijk belang niet gediend zou zijn bij identificatie van gebruikers van deze prepaid telefoonkaarten. In deze notitie zal hier nader op worden ingegaan.

Aanleiding

West-Afrikaanse Criminele Netwerken (WACN) zijn actief in diverse vormen van criminaliteit waaronder fraude. Waar de WACN met name actief in zijn is de zogenaamde advance fee fraude, ook wel 419 fraude genoemd naar een artikel in de Nigeriaanse Strafwet. Dit zijn zeer omvangrijke oplichtingpraktijken, waarbij wereldwijd via brieven, faxen of e-mails (internet) mensen massaal worden benaderd. Er wordt dan de suggestie gewekt dat er bijvoorbeeld een familiekapitaal van een overleden of verjaagde machthebber moet worden veiliggesteld of dat de geadresseerde een financiering kan krijgen, erfgenaam is van een overleden ver familielid of een loterijprijs heeft gewonnen. Het gaat hierbij vrijwel altijd om vele miljoenen dollars.
Uiteindelijk komt het er steeds op neer dat om een vooruitbetaling (advance fee) wordt gevraagd waarna men in een oplichtingcircuit getrokken wordt. Naar aanleiding hiervan werd het projectmatige rechercheonderzoek Apollo verricht in samenwerking met andere opsporingsdiensten en een aantal private partners (o.a. telecomproviders).

Gesignaleerd knelpunt

Gedurende de onderzoeksperiode werd vastgesteld dat criminele netwerken door de goede communicatie- en infrastructuur in Nederland op het gebied van telecom en internet, op een eenvoudige manier anoniem kunnen communiceren. Hierbij viel op dat veel gebruik werd gemaakt van prepaid telefoonkaarten. Doordat een prepaid telefoonkaart anoniem kan worden aangeschaft is het moeilijk om de (ware) identiteit vast te stellen van de kaarthouder. Ook het traceren van deze personen wordt hierdoor bijna onmogelijk gemaakt. Dit maakt het opsporingsproces erg lastig en geeft criminelen een vrijbrief.

Maatschappelijke relevantie

Door op deze wijze misbruik te maken van de anonimiteit bij de aankoop van prepaid telefoonkaarten zou gesteld kunnen worden dat providers onbedoeld criminele activitelten faciliteren. Door die criminele activiteiten kan er economische schade ontstaan bij onder meer bancaire- en particuliere instellingen. Daardoor kunnen er verhoogde onrustgevoelens onder de bevolking ontstaan en een verminderd vertrouwen in het fenomeen prepaid telefoons. Uiteindelijk kan dit leiden tot schade aan het internationale imago van Nederland. Er is overigens geen economische reden om het gebruik van anoniem telefoneren te rechtvaardigen.

Onderbouwing

Gedurende het onderzoek Apollo bereikten het onderzoeksteam dagelijks vele tientallen mails/brieven en telefoontjes omtrent 06-nummers waarvan door de dader(s)groepen gebruik werd gemaakt voor het verrichten van criminele activiteiten.

Opgemerkt zij dat overigens ook terroristische organisaties gebaat zijn bij onopvallendheid, geslotenheid en anonimiteit die door het gebruik van prepaid telefoonkaarten geboden wordt.

Met andere woorden, het identificeren van personen die gebruik maken van prepaid telefoonkaarten is niet alleen van maatschappelijk belang maar bevordert en versnelt tevens het opsporingsproces. Wanneer de daders bekend zijn, kunnen potentiële slachtoffers eerder worden gewaarschuwd. Daarnaast kunnen mogelijke terroristische activiteiten vroegtijdig worden gesignaleerd en wellicht worden voorkomen.

Advisering

Om criminele activiteiten met prepaid telefoonkaarten aan te pakken en de gebruiker van deze kaarten uit de anonimiteit te halen zou de wetgeving dienen te worden aangepast. In de nieuwe wetgeving dient te worden opgenomen dat registratie van personalia verplicht is bij de aanschaf van een nieuwe prepaid telefoonkaart. De registratie zou op dezelfde manier dienen plaats te vinden als nu voor een abonnement geldt namelijk aan de hand van het originele legitimatiebewijs.

In het nieuwe systeem dienen ook personen die reeds gebruik maken van prepaid telefoonkaarten zich alsnog te legitimeren. In aanvulling daarop worden de gegevens gekoppeld aan het telefoonnummer en opgeslagen in een centraal registratiesysteem. Verwacht wordt dat op deze wijze personen die criminele handelingen willen verrichten of misbruik willen maken van een prepaid telefoonkaart zullen worden afgeschrikt.

Daarnaast dient het Openbaar Ministerie de mogelijkheid te krijgen om telefoonnummers te blokkeren, welke door verdachten gebruikt worden bij het plegen van de strafbare feiten. Afspraken hieromtrent tussen de telecomproviders en het Openbaar Ministerie kunnen worden vastgelegd in een convenant.

Bovenstaande punten sluiten deels aan bij de richtlijnen regelgeving over de opslag van het telefonie- en dataverkeer dat door het Europees Parlement is voorgesteld. De Richtlijn Dataretentie bepaalt hoe en welke gegevens door telefonie- en internetproviders bewaard moeten worden. Providers moeten de communicatiegegevens van al hun klanten voor minimaal 6 maanden opslaan en toegankelijk maken voor politie en Justitie. De richtlijn moet door elke lidstaat ingevoerd worden in de nationale wetgeving.

Als gevolg op de Europese richtlijn kwam het Nederlandse ministerie van Economische Zaken in 2007 met een eigen wetsvoorstel. Het Nederlandse wetsvoorstel gaat op een aantal punten veel verder dan de Europese richtlijn. Zo wil men zelfs de locatiegegevens van iedere mobiele beller vastleggen. Zo kan de reisroute van een mobiele beller gedurende een aantal maanden volledig gevolgd worden. Daarbij zou wel moeten gelden dat die tracering alleen plaatsvindt als men daadwerkelijk belt of gebeld wordt, dus niet als klanten simpelweg hun mobiel aan hebben staan.

Een aantal landen heeft hun wetgeving al aangepast of heeft een registratiesysteem op gezet naar aanleiding van criminele, frauduleuze of terroristische handelingen die werden gepleegd met prepaid toestellen. Voorbeeld van deze landen zijn Thailand, Japan en Singapore.

POLITIE

- Bovenregionale Recherche
- Noordwest & Midden Nederland

Aanbevelingen voor het registreren van internetcafé bezoekers

Ervaringen naar aanleiding van het rechercheonderzoek Apollo.

E. Langedijk

Heemskerk, april 2008

POLITIE
- Bovenregionale Recherche
- Noordwest & Midden Nederland

Voorwoord

Deze notitie is geschreven naar aanleiding van bevindingen die zijn opgedaan tijdens het rechercheonderzoek Apollo, uitgevoerd in de periode 2 oktober 2006 tot 1 november 2007. Het onderzoek werd verricht door o.a. de Bovenregionale Recherche Noordwest & Midden Nederland en richtte zich op West-Afrikaanse Criminele Netwerken (WACN) die zich met name bezighouden met oplichting, zogenaamde 419 fraude (zie hierna).

Gedurende het onderzoek werd het anoniem gebruik kunnen maken van internetcafés door het rechercheteam als een knelpunt ervaren. De vraag rees tevens of ook het maatschappelijk belang niet gediend zou zijn bij identificatie van gebruikers van internetcafés. In deze notitie zal hier nader op worden ingegaan.

Inleiding

West-Afrikaanse Criminele Netwerken (WACN) zijn actief in diverse vormen van criminaliteit waaronder fraude. Waar de WACN met name actief in zijn is de zogenaamde advance fee fraude, ook wel 419 fraude genoemd naar een artikel in de Nigeriaanse Strafwet. Dit zijn zeer omvangrijke oplichtingpraktijken, waarbij wereldwijd via brieven, faxen of e-mails (internet) mensen massaal worden benaderd. Er wordt dan de suggestie gewekt dat er bijvoorbeeld een familiekapitaal van een overleden of verjaagde machthebber moet worden veiliggesteld of dat de geadresseerde een financiering kan krijgen, erfgenaam is van een overleden ver familielid of een loterijprijs heeft gewonnen. Het gaat hierbij vrijwel altijd om vele miljoenen dollars.
Uiteindelijk komt het er steeds op neer dat om een vooruitbetaling (advance fee) wordt gevraagd waarna men in een oplichtingscircuit getrokken wordt. Naar aanleiding hiervan werd het projectmatige rechercheonderzoek Apollo verricht in samenwerking met andere opsporingsdiensten en een aantal private partners (o.a Internetproviders).

Gesignaleerd knelpunt

Gedurende de onderzoeksperiode werd vastgesteld dat criminele netwerken door de goede communicatie- en infrastructuur in Nederland op het gebied van telecom en internet, op een eenvoudige manier anoniem kunnen communiceren. De faciliteiten van Internet kunnen worden aangewend voor allerlei oplichtingspraktijken en via e-mail kunnen duizenden potentiële slachtoffers worden benaderd. Door de grenzeloze omvang van het net is het aantal potentiële slachtoffers zeer groot, net als de mogelijkheid om bijzonder grote criminele winsten te genereren.

De verdachten gebruiken vooral Internetcafés om anoniem het Internet op te gaan, maar ook andere voor het publiek toegankelijke gebouwen worden gebruikt zoals bibliotheken en belhuizen. Doordat er geen registratieplicht geldt voor bezoekers van internetcafés is het voor de politie moeilijk om de identiteit vast te stellen van personen die misbruik maken van het Internet. Ook het traceren van deze personen wordt hierdoor vrijwel onmogelijk gemaakt. Dit maakt het opsporingsproces erg lastig en geeft criminelen een vrijbrief.

Maatschappelijke relevantie

Door op deze wijze misbruik te maken van het internet kan er economische schade ontstaan bij onder meer bancaire- en particuliere instellingen maar ook bij de overheid (anoniem inbreken op systemen). Daardoor kunnen er verhoogde onrustgevoelens onder de bevolking ontstaan en een verminderd vertrouwen in het medium internet. Uiteindelijk kan dit leiden tot schade aan het internationale imago van Nederland en tot een minder open en toegankelijk internet. Er is overigens geen enkele maatschappelijke en of economische reden om anoniem gebruik te maken van internet.

Onderbouwing

Uit onderzoek Apollo is naar voren gekomen dat vaak anonimiteit gekoppeld kan worden aan illegaliteit en criminaliteit. In twee deelonderzoeken van het Apollo project zijn in vier verschillende Internetcafés controles verricht waarbij een aantal personen werd aangetroffen die illegaal in Nederland verbleven.

Opgemerkt zij dat overigens ook terroristische organisaties gebaat zijn bij onopvallendheid, geslotenheid en anonimiteit die door het gebruik van internet geboden wordt.

Met andere woorden, de gegevens van de personen die gebruik maken van internetcafés zijn van groot belang. Een juiste registratie bevordert en versnelt de opsporing van criminele activiteiten van de daders. Wanneer de daders bekend zijn, kunnen potentiële slachtoffers eerder worden gewaarschuwd. Tevens kunnen mogelijke terroristische activiteiten vroegtijdig worden gesignaleerd en wellicht worden voorkomen.

Advisering

Om misbruik van internet aan te pakken, is het van belang de bezoeker van de internetcafés uit de anonimiteit te halen, waarmee tevens het opsporingsproces tegemoet zou kunnen worden gekomen. Hiervoor kunnen de onderstaande maatregelen genomen worden.

Maatregel 1
Het toezicht op een aanbieder van openbare communicatiediensten zoals de internetcafés kan worden verbeterd door de invoering van een vergunningstelsel voor internetcafés, waardoor zij komen te vallen onder de Wet Bevordering Integratiebeoordelingen door het Openbaar Bestuur (BIBOB). Hierdoor worden de mogelijkheden van de gemeente om ongewenste criminele activiteiten te voorkomen, verruimd. Door middel van het vergunningstelsel worden criteria gesteld waaraan een exploitant of beheerder moet voldoen. Zo mag deze niet onder curatele staan of jonger zijn als eenentwintig jaar. Ook zijn er in het vergunningsstelsel weigeringsgronden opgenomen. Op deze manier kunnen extra voorwaarden gesteld worden aan de integriteit van aanvragers van vergunningen en kan een vergunning worden ingetrokken / geweigerd bij (vermoeden van) misbruik. Indien er wordt geconstateerd dat er frauduleuze handelingen worden gepleegd vanuit het betreffende internetcafé kan de vergunning worden ingetrokken.

De gemeenteraden van Bergen op Zoom en Roosendaal hebben reeds in 2005 besloten om een vergunningstelsel in te voeren voor o.a. internetcafés op grond van de Wet BIBOB.

Maatregel 2
Aansluitend op de wet BIBOB kan in een nieuwe wet worden opgenomen dat aanbieders van openbare communicatiediensten zoals internetcafés, worden verplicht om de identiteitsgegevens van de gebruikers van hun dienst vast te leggen aan de hand van een origineel identiteitsbewijs (op grond van de Wet op de Identificatieplicht). Wanneer achteraf blijkt dat er criminele handelingen zijn gepleegd met een computer afkomstig uit het betreffende internetcafé, kan worden nagegaan welke bezoekers het internetcafé hebben bezocht. Dit vergemakkelijkt niet alleen het opsporingproces maar draagt tevens bij aan een integer gebruik van het internet.

Uiteraard zal er rekening mee moeten worden gehouden dat de privacy van de bezoekers niet wordt geschonden door het vaststellen van de identiteit. In de Wet Bescherming Persoongegevens worden al regels gesteld met betrekking tot persoonsgegevens, zoals het verzamelen, vastleggen, ordenen, bewaren, bijwerken, wijzigen, opvragen, raadplegen, gebruiken, verstrekken door middel van doorzending, verspreiding of enige andere vorm van terbeschikkingstelling, samenbrengen, met elkaar in verband brengen, evenals het afschermen, uitwissen of vernietigen van gegevens;

Maatregel 3
Internetcafés verplichten om bij te houden wie op welk tijdstip van welke computer gebruik maakt. Tevens kan met behulp van al bestaande trackingsoftware worden bijgehouden welke sites er worden bezocht. De logs moeten kunnen worden opgevraagd op het moment dat er criminele activiteiten hebben plaatsgevonden bij de aanbieder van de communicatiediensten. Deze mogelijkheid zal bij wet te dienen worden vastgelegd.

POLITIE
- Kennemerland
- Bovenregionale Recherche

Misbruik van Money Transfers

Een onderzoek naar het misbruik van de legale Money Transfer door criminele netwerken, de West-Afrikaanse criminele netwerken in het bijzonder.

N. Ploeger
In samenwerking met
C. Schep

Heemskerk, november 2007

Samenvatting

Dit rapport bevat de bevindingen van het onderzoek naar het misbruik van Money Transfers door criminele netwerken, uitgevoerd door Niels Ploeger en Cees Schep[1]. Het onderzoek is geïnitieerd door de Bovenregionale Recherche Noordwest en Midden Nederland. De aanleiding voor dit onderzoek is het project Apollo, waarin geconstateerd werd dat in het kader van de 419 fraude (oplichting) door West-Afrikaanse criminele netwerken (WACN) grootschalig misbruik wordt gemaakt van Money Transfers om onder andere geld afkomstig van slachtoffers in het buitenland te verkrijgen en geld door te sturen naar landen als Nigeria en of andere betalingen te verrichten.

Deze rapportage beoogt een antwoord te geven op de vraag of de aanpak van het misbruik van Money Transfers in Nederland een hoge (opsporings)prioriteit dient te krijgen. Hiertoe wordt onderzocht wat de aard en omvang is van het misbruik door de criminele netwerken en welke problemen optreden bij het voorkomen, detecteren en opsporen ervan.

De rapportage kent een viertal doelstellingen, te weten:

1. een analyse geven van de aard en (gemiddelde) omvang van het misbruik van Money Transfers door leden van de WACN;
2. het uiteenzetten van casussen en voorbeelden ten aanzien van misbruik van Money Transfers door (internationale) criminele netwerken;
3. een analyse geven van factoren (knelpunten) die een verstorende rol spelen bij het voorkomen, detecteren en opsporen van het misbruik van Money Transfers op het niveau van de Money Transfer maatschappijen, de toezichthouder, de Financial Intelligence Unit Nederland (FIU-NL) en de opsporing;
4. aanbevelingen doen aan de branche, de toezichthouder, de FIU-NL, de opsporing en de wetgever ten behoeve van het tegengaan van misbruik van Money Transfers.

De basis voor dit rapport is de analyse van verschillende grote opsporingsonderzoeken, zoals het onderzoek Apollo, waarin is gebleken dat internationale criminele netwerken misbruik maken van Money Transfers, een door de FIU-NL uitgevoerde analyse van 65 bij 419 fraude betrokken personen en het interviewen van personen en instanties die actief zijn in de gehele Money Transfer keten, zoals Money Transfer kantoren[2], de toezichthouder, de FIU-NL en de opsporing. De 419 fraude / het onderzoek Apollo is in dit rapport als uitgebreide casestudy opgenomen.

[1] Niels Ploeger is criminoloog bij de Bovenregionale Recherche Noordwest en Midden Nederland; Cees Schep is senior-expert bij de Dienst Nationale Recherche Informatie van het Korps Landelijke Politie Diensten.

[2] Providers, zoals Western Union en MoneyGram, zijn de beheerders van de diverse Money Transfer netwerken en maken bij de uitvoering van transacties gebruik van agentschappen. Met de term Money Transfer kantoren worden in dit rapport zowel providers als agentschappen bedoeld.

Conclusies

De conclusies die betrekking hebben op de 419 fraude dienen in een breder verband geïnterpreteerd te worden; niet alleen zeggen de conclusies iets over de problematiek rond de 419 fraude, tevens laat de casus van de 419 fraude zien wat de mogelijkheden voor criminele netwerken zijn die vanuit Nederland willen opereren.

De Money Transfer is bij de 419 fraude een belangrijk instrument om (snel) geld te verkrijgen van slachtoffers afkomstig uit meer dan 50 verschillende landen.

Bij 419 fraude worden slachtoffers willekeurig[3] wereldwijd onder andere per e-mail benaderd met een financieel voorstel, bijvoorbeeld een loterijprijs, erfenis of zakelijk voorstel, waarbij een hoge beloning in het vooruitzicht wordt gesteld en eerst de nodige kosten gemaakt moeten worden, alvorens deze beloning in ontvangst kan worden genomen. Dit creëert een geldstroom die afkomstig is van meer dan 50 verschillende landen, met de Verenigde Staten als hofleverancier, waarover de WACN snel en met weinig risico over willen beschikken. Daarnaast dient een deel van de opbrengsten naar 'mededaders' gestuurd te worden en of gebruikt te worden voor bepaalde betalingen, zoals de aankoop van goederen. De Money Transfer is bij uitstek geschikt om in deze behoeftes te voorzien. De door de FIU-NL uitgevoerde analyse van 65 personen die betrokken zijn bij 419 fraude, laat een geldstroom zien van € 11 miljoen, waarvan het overgrote deel binnenkomende Money Transfers betreft. Gezien het feit dat personen die betrokken zijn bij de 419 fraude meestal gebruik maken van verscheidene (valse) identiteiten en de FIU-NL analyse uitsluitend betrekking heeft op de als *ongebruikelijk* gemelde transacties, moet de € 11 miljoen als een ondergrens gezien worden.

De Money Transfer vervult een belangrijke rol bij de criminele activiteiten van de WACN.

De WACN houden zich bezig met uiteenlopende criminele activiteiten, waaronder mensensmokkel, mensenhandel, illegale prostitutie en drugshandel. Personen die betrokken zijn bij 419 fraude verrichten vaak ook transacties die hoogstwaarschijnlijk verband houden met andere delicten. Voorbeelden hiervan zijn binnenkomende geldstromen afkomstig uit Italië (mensenhandel en illegale prostitutie) en uitgaande geldstromen naar Zuid-Amerika en de Nederlandse Antillen (drugshandel). Doordat de in Nederland opererende leden van de WACN veelal in Amsterdam Zuidoost woonachtig zijn en vanuit dit stadsdeel opereren, vindt hier ook het belangrijkste gedeelte van het misbruik door de WACN plaats.

[3] Afhankelijk van het soort scenario, bijvoorbeeld loterij, erfenis of zakelijk voorstel, wordt soms wel eerst een specifieke doelgroep uitgekozen. Denk hierbij bijvoorbeeld aan artsen en mensen met een eigen bedrijf. Ook zijn er signalen dat er een wereldwijde handel is in 'suckerlists': lijsten met personalia van (potentiële) slachtoffers.

Het product Money Transfer blijkt kwetsbaar te zijn voor misbruik door verschillende criminele organisaties, onder andere in het kader van mensenhandel, (419) fraude[4], illegale prostitutie, bankpasfraude, drugshandel en vormt een internationaal probleem.

In Nederland zijn het niet alleen de WACN die zich schuldig maken aan oplichting, mensenhandel, illegale en gedwongen prostitutie en drugshandel; ook andere criminele netwerken zijn in Nederland actief die zich bezighouden met soortgelijke delicten, zoals Bulgaarse criminele netwerken (mensenhandel / gedwongen prostitutie), Roemeense criminele netwerken (E-bay fraude en skimming) en Colombiaanse criminele netwerken (drugshandel). Ook deze criminele netwerken maken grootschalig misbruik van Money Transfers. Daarnaast blijkt misbruik van Money Transfers een internationaal probleem te zijn waarmee biljoenen euro's gemoeid zijn.

Misbruik van Money Transfers schaadt zowel de integriteit van het financiële stelsel als de integriteit van het product zelf.

Misbruik van Money Transfers gaat vaak gepaard met meerdere inbreuken op de integriteitswetgeving[5]. In een aantal gevallen is er sprake van bewuste betrokkenheid van de Money Transfer kantoren bij witwassen of worden er zelfs kantoren speciaal opgericht om criminele groeperingen te faciliteren. In toenemende mate wordt het product Money Transfers geassocieerd met criminele activiteiten, zowel door consumenten als (internationale) opsporingsdiensten. Doordat de vanuit Nederland geïnitieerde oplichting veel buitenlandse slachtoffers kent, kan dit tot een vermindering leiden van het (buitenlandse) vertrouwen in het Nederlandse financiële stelsel.
De totale omvang van misbruik van Money Transfers laat zich moeilijk meten (dark number). De jaarlijkse *verdachte* geldstroom van Money Transfers ligt de laatste jaren rond de 100 miljoen euro[6], maar de hoogte van de jaarlijkse verdachte geldstroom hangt echter samen met het aantal ongebruikelijke transacties dat jaarlijks als zodanig herkend, vervolgens gemeld en onderzocht wordt. Gezien de omvang van het jaarlijkse aantal ongebruikelijke Money Transfers (meer dan 170.000 per jaar) en het feit dat ongebruikelijke transacties die nog niet onderzocht of verdacht verklaard zijn, alsnog verdachte transacties kunnen betreffen, moet rekening gehouden worden dat de werkelijke jaarlijkse omvang van de verdachte geldstroom (het misbruik) van Money Transfers aanzienlijk hoger zal zijn.

---

[4] Het gaat hier om meerdere vormen van fraude. Zo houden WACN zich bijvoorbeeld ook bezig met creditcardfraude.

[5] De integriteitswetgeving bestaat uit: de Wet op het financieel toezicht (Wft), de Wet inzake de geldtransactiekantoren (Wgt), de Wet identificatie bij dienstverlening (Wid), de Wet melding ongebruikelijke transacties (Wet MOT) en de Sanctiewet 1977.

[6] De hoogte van de jaarlijkse geldstroom Money Transfers over 2006 is door DNB geschat op € 1 miljard.

Het gebruik van valse namen en adressen door criminele netwerken (zoals de WACN en in toenemende mate ook Roemeense criminele netwerken) frustreert de opsporing.

Doordat criminele netwerken als de WACN en Roemeense criminele netwerken gebruik maken van meerdere valse identiteiten en bijbehorende valse identiteitsdocumenten, zijn zij moeilijk traceerbaar voor de opsporing: hoe vind je iemand met een valse naam en vals adres? Indien de identiteitscontrole aan de balie van Money Transfer kantoren optimaal uitgevoerd zou worden, zou het niet mogelijk zijn transacties te kunnen verrichten met valse identiteitsdocumenten. Bij dit probleem spelen ook nog andere knelpunten een belangrijke rol. Deze knelpunten komen verderop in deze samenvatting aan de orde.

De bestrijding van het misbruik van Money Transfers, met name het opsporen van (notoire) misbruikers, heeft binnen de opsporing onvoldoende aandacht en prioriteit (gekregen).

Het opsporen van personen die misbruik maken van Money Transfers is nooit een prioriteit geweest binnen de opsporing. Ook de in het verleden door de FIU-NL proactief aangeleverde zaken waarin sprake was van subjecten die grootschalig misbruik maken van Money Transfers, werden door de opsporing terzijde gelegd. Opsporingsonderzoeken richten zich op het gronddelict, waarbij de verrichte transacties hoofdzakelijk als aanvullend bewijs worden gebruikt en of om inzichten te verkrijgen in de criminele netwerken. Aanvullend wordt wel vaak witwassen ten laste gelegd. Personen die in lopende onderzoeken niet het onderwerp van onderzoek zijn, kunnen in de huidige praktijk jarenlang misbruik maken van Money Transfers. Daarbij kan het totaalbedrag aan misbruik bij deze personen in een paar jaar tijd oplopen tot meer dan een half miljoen euro per persoon.

Money Transfer kantoren leven in veel gevallen de integriteitswetgeving onvoldoende na, hetgeen invloed heeft op de duur en de omvang van het misbruik.

De integriteitswetgeving heeft als doel witwassen en terrorismefinanciering zoveel mogelijk buiten het financiële stelsel te houden. Integriteit speelt een belangrijke rol bij het aanbieden van (financiële) diensten. In de praktijk blijkt er bij de naleving van de integriteitswetgeving door Money Transfer kantoren een aantal knelpunten op te treden:

- de identiteitscontrole is onvoldoende;
- de deskundigheid van de baliemedewerker / het Money Transfer kantoor over bepaalde bevoegdheden, verantwoordelijkheden en verplichtingen is onvoldoende;
- Money Transfer kantoren doen onvoldoende eigen onderzoek en cliënten met een hoog witwasprofiel worden onvoldoende geweerd;

- doordat onvoldoende eigen onderzoek wordt gedaan, is het meer dan aannemelijk dat niet alle daarvoor in aanmerking komende transacties subjectief worden gemeld; deze transacties kunnen dan ook niet door de FIU-NL worden onderzocht;
- Money Transfer kantoren hanteren een eigen (anti witwas) beleid, waardoor uit concurrentiemotieven transacties vermoedelijk niet altijd even nauwkeurig bekeken worden;
- er is geen gemeenschappelijke blokkeerlijst, hetgeen tot gevolg heeft dat transacties verspreid kunnen worden over de verschillende Money Transfer kantoren;
- een aantal Money Transfer agentschappen beschikt (nog) niet over een eigen blokkeerlijst, hetgeen tot gevolg heeft dat cliënten misbruik kunnen blijven maken, totdat een provider het misbruik opmerkt;
- Money Transfer kantoren wisselen onderling geen informatie uit over cliënten met een hoog witwasrisico, hierbij speelt onder andere de privacywetgeving een rol.

De huidige situatie creëert de mogelijkheid voor criminele netwerken om in veel gevallen ongestoord, zeer frequent, gedurende meerdere jaren, criminele gelden te ontvangen en te verplaatsen. Ook het toezicht op de Money Transfer kantoren kan niet voorkomen dat misbruik van Money Transfers plaatsvindt.

Het misbruik van Money Transfers dient in Nederland een hoge (opsporings)prioriteit te krijgen; maatregelen zijn nodig om het misbruik van Money Transfers zowel preventief als repressief tegen te gaan.

Aanbevelingen

Om het misbruik van Money Transfers te bestrijden wordt een aantal maatregelen voorgesteld. Deze aanbevelingen hebben primair als doel misbruik van Money Transfers te voorkomen en tegen te gaan, maar zullen ook positief bijdragen aan:

- het onaantrekkelijker maken van Nederland voor criminele netwerken;
- het tegengaan van (verdere) imagoschade voor Nederland en het product Money Transfers;
- het verbeteren van de naleving van de integriteitswetgeving;
- het verbeteren van de informatiepositie van DNB, de FIU-NL en de opsporing;
- het verbeteren van de samenwerking tussen DNB, de FIU-NL, de opsporing en de Money Transfer kantoren;
- het behoeden van Money Transfer kantoren voor strafrechtelijke vervolging.

Puntsgewijs overzicht van de in dit rapport voorgestelde aanbevelingen[7]:

1. Er dient een brancheorganisatie opgericht te worden;
2. Er dient een branchebreed uniform beleid ingesteld te worden;
3. Er dient een gemeenschappelijke lijst met ongewenste personen te komen (blokkeerlijst);
4. De kwaliteit van de baliemedewerkers dient naar een hoger niveau getild te worden;
5. De veiligheid van de baliemedewerkers dient dusdanig te worden geregeld dat het niet langer mogelijk is dat transacties met een hoog witwasrisico uit angst en of bedreiging toch uitgevoerd worden;
6. Money Transfer kantoren dienen te worden verplicht voorafgaand aan elke transactie een scan of kopie te maken van het identiteitsdocument;
7. Transacties waarvan de kans groot geacht wordt dat ze verband houden met oplichting, dienen door Money Transfer kantoren geweigerd te worden, óók indien het slachtoffer de opdrachtgever is, op straffe van mede-aansprakelijkheid;
8. Money Transfer kantoren dienen verplicht klantenprofielen op te stellen;
9. De opsporing dient een hogere prioriteit toe te kennen aan het gebruik en de handel in valse identiteitsdocumenten;
10. De opsporing dient een hoge capaciteit toe te kennen aan het misbruik van Money Transfers;
11. Integrale samenwerking en projectmatige aanpak van het misbruik van Money Transfers is noodzakelijk;
12. Money Transfer kantoren die (structureel) niet-integer handelen, dienen strafrechtelijk aangepakt te worden;
13. De wettelijke mogelijkheden voor de politie om Money Transfer kantoren te informeren over cliënten die misbruik maken van het product, dienen te worden vergroot;
14. In het kader van 419 fraude en andere vormen van oplichting kan de oplichting en het misbruik van Money Transfers gefrustreerd worden door het waarschuwen van slachtoffers.

Tot slot is het ontvangen van Money Transfers in Nederland een mogelijk onderwerp van discussie, waarbij tevens gekeken zou kunnen worden naar:

- het stellen van een periodieke limiet van het bedrag dan wel het aantal transacties dat een persoon in Nederland kan ontvangen (en versturen);
- het beperken van het aantal geldtransactiekantoren in een bepaald gebied, waardoor de (wets)kennis, techniek en ervaring zich concentreert in een klein aantal kantoren;
- het koppelen van het versturen en ontvangen van Money Transfers aan een bankrekening.

[7] Zie hoofdstuk 8 voor een nadere toelichting.