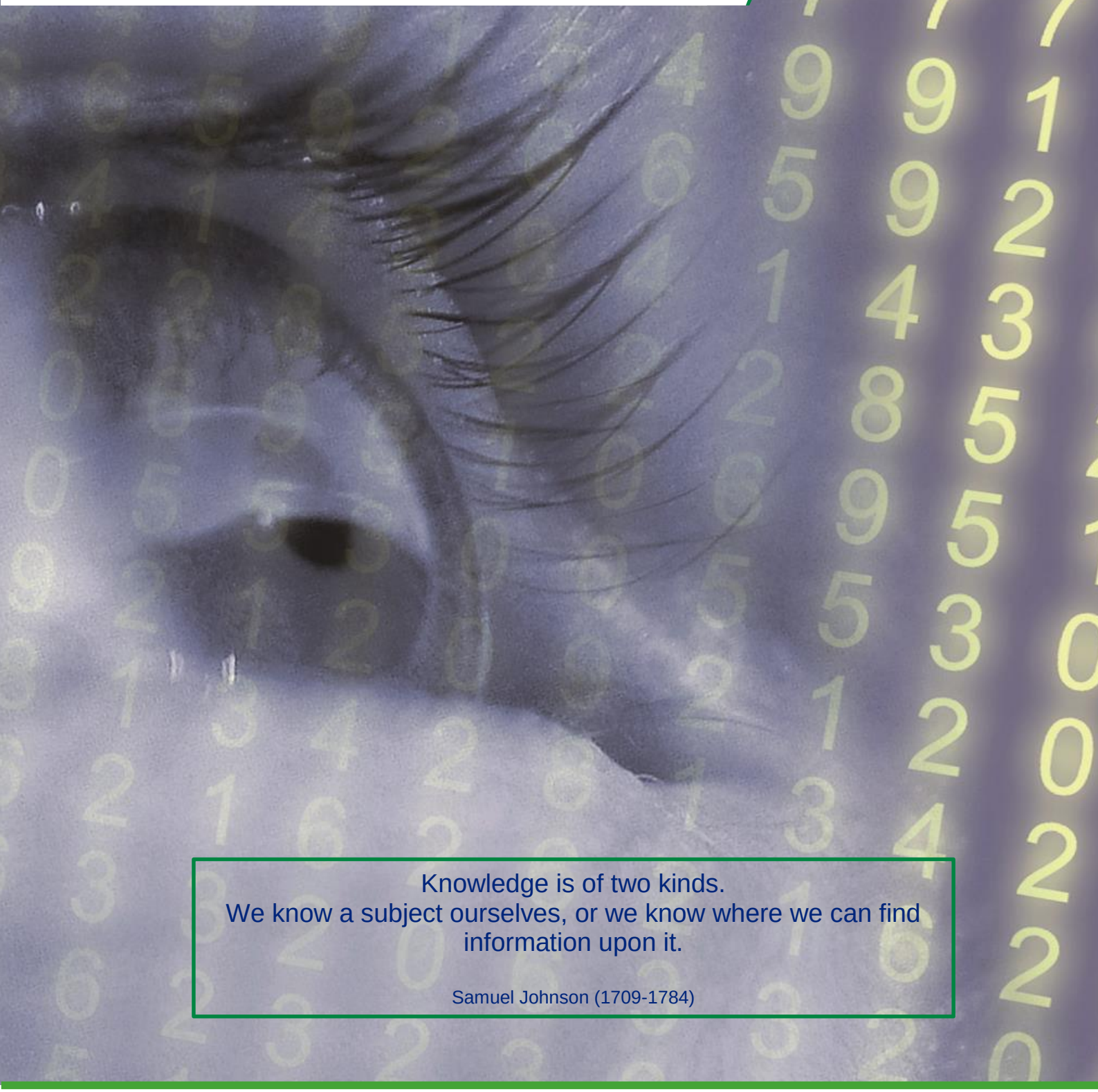
Toekomst in aanpak van verzekerings-fraude



Knowledge is of two kinds.
We know a subject ourselves, or we know where we can find information upon it.

Samuel Johnson (1709-1784)

VERBOND VAN VERZEKERAARS

VERBOND VAN VERZEKERAARS

Het maatschappelijke belang van fraudebeheersing

Verzekeraars hebben een belangrijke maatschappelijke rol en bijbehorende verantwoordelijkheid. Verzekeraars bieden zekerheid en bescherming bij financiële risico's opdat burgers en bedrijven zich kunnen ontwikkelen en ondernemen. Door digitale en technologische veranderingen vindt een verschuiving plaats in het verzekeringslandschap. Traditionele risico's verdwijnen, klanten veranderen, nieuwe aanbieders en verzekeringsvormen komen op de markt. Risico's en aanbiedingsvormen van verzekeringen wijzigen en verzekeraars moeten daarin mee. De uitdaging is om de veranderende wereld als kans te beschouwen en in te spelen op de wijzigende omstandigheden.[1]

Digitalisering biedt kansen en bedreigingen in fraudebeheersing

In lijn met de toenemende digitalisering worden verzekeringsaanvragen verdergaand geautomatiseerd. Een fraudeur kan zijn verzekeraar eenvoudig digitaal misleiden door middel van een valse identiteit en onjuiste adresgegevens.

De overheid onderkent het probleem van de toenemende cybercriminaliteit. Politie en justitie krijgen hierin meer bevoegdheden en de strafmaat voor cybercriminelen is in 2015 aanzienlijk verhoogd.

Maatschappelijk verantwoord ondernemen betekent ook optreden tegen malafide klanten en relaties. Naleving van regelgeving en de wens de eigen reputatie te beschermen, spelen een rol op het terrein van fraudebeheersing. Het grootste belang om fraudeurs te dwarsbomen, ligt echter in bescherming van de belangen van bonafide klanten.

Om hun rol in de toekomst te blijven vervullen, is het noodzakelijk dat verzekeraars zich richten op innovaties en nieuwe producten. Waar kansen kunnen leiden tot veranderende processen en producten ontstaan helaas ook nieuwe bedreigingen op het gebied van verzekeringsfraude. Een gewijzigd risicolandschap levert nieuwe vormen van fraude op. Bij iedere 'next step' die een verzekeraar zet, is het goed stil te staan bij de veiligheids- en integriteitsrisico's voor de financiële sector.

3 op 1.000 verzekerden pleegt fraude

Per duizend verzekerden worden gemiddeld drie personen betrapt op fraude met een verzekeringsproduct. Eén van hen eindigt in het landelijk waarschuwingssysteem.

Dankzij verbetering van de detectieprocessen zijn verzekeraars steeds beter in staat fraude te detecteren. In 2015 is met 15% minder uitgevoerde incidentonderzoeken bijna 10% meer fraude opgespoord.

[1] Zie onder meer 'No risk, no glory; visie op de toekomst van schadeverzekeraars, juni 2015

Noodzaak voor een nieuwe aanpak

Het is logisch dat verzekeraars processen verder digitaliseren maar dat heeft consequenties voor bijvoorbeeld herkenning van misleidende informatie. Claims kunnen via mobiele applicaties worden ingediend maar de bijbehorende afbeeldingen zijn gefotoshopt. Nota's worden in PDF bestand aangeleverd, maar blijken zelf gefabriceerde facturen en aangepaste aankoopbonnen. Van achter de computer worden zaken bij een internetaanvraag mooier voorgespiegeld dan ze zijn. Opzettelijke misleiding is teruggebracht tot één keer klikken met een muis. Met de toenemende technische mogelijkheden wordt fraude plegen gemakkelijker, geraffineerder en moeilijker te traceren.

Het is allang niet meer alleen een opportunistische gelegenheidsfraudeur die de werkelijkheid verdraait bij zijn polis-aanvraag. Werkprocessen bij verzekeraars worden steeds vaker misbruikt door (georganiseerde) criminelen om geld te verdienen. Interne grenzen voor een claimbeoordeling worden extern bekend en de fraudeur weet hoe hoog zijn claim mag zijn voordat onderzoek wordt ingesteld. Netwerken van computers draaien dag en nacht door om valse aanvragen te genereren. Of het nu de 'first offender' of de criminele professional is, maakt in feite niet uit; de digitalisering van bedrijfsprocessen vraagt van verzekeraars meer inzicht en inzet om fraude te voorkomen of te ontdekken.

Het streven van een verzekeraar naar efficiënte werkprocessen, producten en diensten heeft invloed op zijn gevoeligheid voor fraude. De behoefte aan snelheid en servicegerichtheid brengt nieuwe risico's op fraude met zich mee. De invloed van technologische toepassingen heeft gevolgen voor het ouderwetse onderbuikgevoel van de oplettende medewerker. Om toch voor- en vroegtijdig fraude te blijven zien, is het meer gaan combineren van verschillende databronnen van groot belang.

Verbindingsproblemen

Het Centrum Bestrijding Verzekeringscriminaliteit (CBV) van het Verbond van Verzekeraars vervult sinds 2007 voor de verzekeringssector, en partijen daarbuiten, een belangrijke rol op het terrein van belangenbehartiging en informatie(ver)deling bij het bestrijden van verzekeringscriminaliteit. Met behulp van het CBV hebben verzekeringsmaatschappijen een actief fraudebeleid binnen de eigen organisaties geïmplementeerd en zijn grote fraudezaken gezamenlijk aangepakt. Op het gebied van bewustwording en bestrijding van gepleegde verzekeringsfraude hebben de verzekeraars veel bereikt. Het fundament voor de aanpak van verzekeringsfraude is stevig maar het effect kan groter.

Voor een succesvolle strijd tegen verzekeringsfraude is samenwerking op strategisch en operationeel niveau cruciaal. Hier zit op dit moment een belangrijk knelpunt. Verzekeraars communiceren nog weinig met elkaar en met het CBV. Door deze verbindingsproblemen – onder meer op technisch niveau – wordt nog niet alle relevante data tussen private (en publieke) partners gedeeld. Waar beschikbare data niet of nauwelijks wordt gekoppeld of verrijkt, ontstaat slechts weinig nieuwe informatie om fraudeurs vroegtijdig in het oog te krijgen. Het effect van samenwerking en datadeling in de aanpak van verzekeringsfraude is nog niet optimaal en vraagt om nieuwe impulsen.

Ook veranderingen in wijze waarop fraudes worden gepleegd, vergroten het probleem voor de verzekeraars. Groeiende aandacht van de georganiseerde criminaliteit voor de financiële sector leidt tot grotere schades en lastiger te traceren fraudes. De professionaliteit en geraffineerdheid van fraudeurs neemt toe. Ook hun deskundigheid en toepassing van technologie bij het misleiden van verzekeraars noodzaakt de markt tot meer gezamenlijk optreden en optimale informatie-uitwisseling.

Impact van fraude

Verzekeraars weten dat ze altijd doelwit van oplichters blijven. Op basis van de cijfers over 2014 hebben de fraude-onderzoekers van de verzekeraars bijna 99 miljoen euro aan fraude opgespoord.[2] Een onderzoek levert in één op de drie gevallen een bewezen fraude op. Daarmee is gemiddeld een bedrag van meer dan € 12.000,00 per getraceerd geval gemoeid.

Voorkomen van misbruik van een verzekeringsproduct is lastig maar over het algemeen goedkoper dan achteraf opsporen van fraude en terugvorderen van ten onrechte uitbetaalde bedragen. Door producten en processen vooraf te beoordelen op fraude-risico's leveren productontwikkelaars, marketeers en ICT-ers een belangrijke bijdrage aan de aanpak van verzekeringscriminaliteit. Wat niet verdwijnt, hoeft niet opgespoord te worden.

Non-concurrentiële aanpak

Ten aanzien van de bestrijding van verzekeringsfraudeurs hanteren verzekeraars sinds jaren het uitgangspunt dat non-concurrentieel wordt gehandeld. Het Verbondsbeleid 'verzekeringscriminaliteit mag niet lonen' werkt door in gezamenlijk optreden van verzekeraars. Waar een verzekeraar geholpen kan worden door informatie en inzichten van een andere financiële instelling wordt dit gedeeld.

Melding van een kwart miljoen

Een verzekeraar meldt een incidentonderzoek naar een verdachte claim wegens overlijden bij het CBV. Het blijkt dat nog vier andere maatschappijen met dezelfde klant te maken hebben. Gecoördineerd onderzoek van de vijf verzekeraars heeft tot ontmaskering van de fraudeur geleid. De besparing voor de marktpartijen bedraagt minimaal € 250.000,00.

De vroege melding van het onderzoek bij het CBV door een verzekeraar heeft de vijf maatschappijen bij elkaar gebracht. Door gezamenlijk onderzoek te doen, zijn de kosten per maatschappij beperkt en is de beschikbare kennis optimaal ingezet.

Veel van de mogelijkheden tot samenwerking en (vooral) informatiedeling zijn de afgelopen jaren vastgelegd in gedragsregels en protocollen van het Verbond. De rechtmatigheid, kwaliteit, integriteit van samenwerking en van informatiedeling zijn in die afspraken geborgd. Veranderingen die van invloed zijn op de sector vragen van verzekeraars dat deze samenwerking verder wordt geïntensiveerd.

[2] CBV Factsheet, nummer 2, juli 2015

Oorzaak en gevolg

Om effectief potentiële fraudeurs af te schrikken, moeten de gevolgen vooraf duidelijk zijn. Waar het besef ontbreekt dat men een strafbaar feit pleegt, worden grenzen makkelijk overschreden. Zaken als hoogte van de pakkans, civiele boetes en strafrechtelijke sancties hebben effect op de keuze die een mens zal maken. Weten dat je voor een eenvoudige fraude acht jaar geregistreerd kunt worden in het landelijk waarschuwingssysteem[3], en in de toekomst problemen kan ondervinden bij het afsluiten van een verzekering, is van invloed op de keuze om 'het maar eens te proberen'. Voorafgaande en heldere berichtgeving over de gevolgen van het plegen van fraude is een belangrijke stap bij preventie.

Informatiedeling voorkomt in diensttreden van fraudeur

Bij een pre-employment screening heeft een verzekeraar, via het CBV informatie van een andere verzekeraar gekregen. Diens eerdere melding had betrekking op financiële malversaties. Op grond van de informatie is voorkomen dat de sollicitant bij de raadplegende verzekeraar in dienst kon komen.

De CBV toets die wordt gebruikt voor de screening levert zes keer per maand een resultaat op. Effectieve en structurele incidentmeldingen aan het CBV kunnen het aantal treffers naar schatting verhogen tot boven 40 signalen per maand.

Het CBV wil dat verzekeraars, al dan niet gezamenlijk of via het Verbond, in de toekomst meer communiceren over de fraudeaanpak. Succesverhalen van fraudebestrijders moeten breed gedeeld worden. Via dergelijke publiciteit weet de bonafide klant dan ook welk belang verzekeraars hechten aan de bescherming van zijn klantbelang.

Streetwise fraude bestrijden

Een oplichter is van oudsher vindingrijk in manieren om anderen om de tuin te leiden. Van de verzekeraar wordt in zijn strijd tegen de fraudeur een vergelijkbare scherpzinnigheid en assertiviteit gevraagd. Door steeds meer informatie te gaan verwerken, zoals over gehanteerde modus operandi, kan de verzekeringsmarkt zich op termijn steeds beter wapenen tegen oplichterspraktijken.

Fraudegevoeligheid van een werkproces

Klanten hebben recht op bedenktijd bij een polis en de mogelijkheid een aanvraag te annuleren. Dit leidt vaak automatisch tot restitutie van de betaalde premie. Fraudeurs kennen de regels goed en storneren de premie ook nog een keer.

Via een CBV-waarschuwingsbericht is deze werkwijze bij alle verzekeraars onder de aandacht gebracht. Zij kunnen onmiddellijk optreden en de eigen procedures herzien om deze vorm van oplichting verder te voorkomen.

De verzekeringsmarkt moet meer 'streetwise' worden door zoveel mogelijk kennis over fraudes te verzamelen. Het doel is uiteindelijk de denk- en handelwijze van een fraudeur beter te doorgronden en te voorspellen. Verzekeraars moeten benadeling door onrechtmatige handelingen bestrijden door min of meer te leren denken als een fraudeur. Zo kan de verzekeraar een fraudeur uiteindelijk voor zijn en voorkomen dat hij slachtoffer wordt.

[3] Het Externe Verwijzingsregister conform het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen

Eén bron is geen bron

Informatie, informatie, informatie. Bij effectieve fraudebeheersing draait alles om data. Voor preventie en detectie van fraude in een digitale omgeving is informatie een must. Als de fraudehandeling zelf niet meer goed te herkennen is, moet je de potentiële fraudeur vooraf beter in beeld krijgen. Cruciaal is datadeling en data-analyse. Verzekeraars moeten de bestaande protocollaire ruimte tot informatiedeling optimaal benutten. Kleine oplichtingstrends en grote fraudezaken kunnen alleen herkend worden als verzekeraars van elkaar weten wat er speelt.

Fraudeurs doen het met iedereen

Uit onderzoek blijkt dat een bedrijf dat fraude pleegt ten koste van een verzekeraar gemiddeld met nog vier andere maatschappijen vergelijkbare zaken doet. Als een verzekeraar getroffen wordt, is de kans groot dat anderen met dezelfde schade worden geconfronteerd.

Het CBV biedt via het register Zakelijke Relaties een oplossing om andere verzekeraars te waarschuwen over de risico's van de betreffende relatie. Deze informatiestroom voorkomt dat andere maatschappijen onwetend blijven en met de fraudeur zaken blijven doen.

Eén informatiebron is niet meer genoeg om fraude te vinden. Het combineren van gegevens uit verschillende bestanden draagt bij aan de ontdekking van mogelijke frauduleuze handelingen. Door meer en betere data bij elkaar te brengen, kunnen patronen worden gesignaleerd. Dat geldt voor te verzekeren risico's in algemene zin maar ook voor patronen die passen bij verzekeringsfraude. Door met en via het Centrum Bestrijding Verzekeringscriminaliteit (CBV) van het Verbond informatie over te onderzoeken en onderzochte fraudezaken beschikbaar te maken, kan op dossier-, branche- en sectoraal niveau voordeel worden bereikt. Zo weet een individuele verzekeraar meer over zijn klant als potentiële fraudeur, weet de branche meer over product-gerelateerde frauderisico's en weet de sector meer ten aanzien van de veiligheid en integriteit als geheel. Deelnemen en bijdragen aan de informatiestroom over verzekeringsfraude dient de gehele bedrijfstak. Daarom is het van groot belang dat alle verzekeraars meedoen en gebruik maken van de data die om hen heen beschikbaar is.

Combineren van bronnen beperkt zich niet tot de eigen marktpartijen. Het biedt verzekeraars voordeel om meer gebruik te gaan maken van de informatie die zich in de periferie van hun activiteiten bevindt en samen te werken met andere partijen. Van allerlei publieke en private partners mag worden verwacht dat informatieverstrekking twee richtingen op gaat.

Het belang van datadelen

Via het samenwerkingsverband van het Landelijk Informatiecentrum Voertuigcriminaliteit (LIV) delen publieke partners en verzekeraars informatie over vermiste voertuigen. De partners binnen LIV zorgen dat een diefstalsignaal direct in alle relevante systemen staat. De registratie is versneld van enkele dagen naar binnen twee uur. Hierdoor zijn auto's steeds beter en sneller terug te vinden.

Inzet van technologie

Big data is een veelvoorkomend begrip als het om klantinformatie gaat. Voor risico- en fraudebeheersing voegen we daar 'big analyse' aan toe. Alleen het bijeen brengen van grote hoeveelheden data biedt nog niet het antwoord op de vraag wie een fraude kan plegen. Het

geautomatiseerd matchen van adressen, rekeningnummers en klantgegevens biedt de mogelijkheid netwerken bloot te leggen die een acceptant of schadebehandelaar in eerste aanleg zullen ontgaan. Door verbanden te leggen met andere data wordt afwijkend gedrag in beeld gebracht.

Met de inzet van informatie-verwerkende technologie (bijvoorbeeld via predictive analyses[4]) in combinatie met de expertise van deskundige fraudeanalisten kunnen inzichten gerealiseerd worden die misbruik van verzekeringen helpen traceren en voorkomen.

Meer fraude bij Acceptatie

In een paar jaar tijd is de verhouding van het aantal fraudezaken bij schadeafhandeling en acceptatie steeds dichter bij elkaar gekomen. Waar in 2012 nog ruim 64% van de onderzoeken op claims betrekking had, heeft in 2015 bijna de helft van alle onderzoeken betrekking op fraude in de acceptatie-fase.

Door vergelijking van data uit meerdere bronnen vallen afwijkingen eerder op.

Voordeel van melden

Speerpunt in het verder brengen van fraudebeheersing-activiteiten door verzekeraars is verbetering van de bestaande informatie-uitwisseling tussen verzekeraars zelf. Uitwisseling betekent twee-richtingen-communicatie en is daarmee afhankelijk van de evenredige bijdrage van alle verzekeraars. Verzekeraars die actief werken aan fraudebeheersing, en hun bijdrage leveren aan de strijd tegen verzekeringscriminaliteit, verkrijgen het voordeel dat zij de opgedane kennis, uitgevoerde analyses en individuele signalen van andere maatschappijen ontvangen.

Het belang van bedrijfstak bij brede informatiedeling, en de bindende zelfregulering van het Verbond, betekent dat alle verzekeraars bijdragen aan informatie-uitwisseling rondom verzekeringscriminaliteit. Het CBV gaat monitoren hoe informatiedeling door Verbondsleden wordt uitgevoerd. Verzekeraars die, in verhouding tot hun positie in de branche, relatief weinig bijdragen aan de incidenten-dataverzameling zullen worden aangezet hun rol in de aanpak van verzekeringsfraude op te pakken c.q. te vergroten.

Aandacht voor privacy

De noodzaak om in fraudebeheersing meer data te verwerken, lijkt op gespannen voet te staan met de toenemende roep om privacy. Door transparant en correct verwerken van persoonsgegevens is die tweestrijd echter niet nodig. Verzekeraars moeten nu en in de toekomst zorgvuldig omgaan met informatie die zij over personen verwerken. Maatregelen op het gebied van databeveiliging moeten van de hoogste orde zijn. Niet alleen om te voorkomen dat verzekeraars zelf slachtoffer worden van cybercrime maar ook om het grootste goed van hun organisatie, namelijk de informatie van en over hun klanten, optimaal te beschermen.

Fraudebeheersing van de toekomst

Meegaand en rekening houdend met nieuwe trends en ontwikkelingen blijven verzekeraars de behoefte aan veiligheid en zekerheid vervullen. Bij het zoeken van nieuwe verzekeringsoplossingen wordt rekening gehouden met fraudegevoeligheid van bestaande en nieuwe producten en processen. Data uit verschillende bronnen zal worden ingezet om te analyseren welk frauderisico iemand als klant vormt of welke claim nader onderzoek vraagt. De kennis die dit oplevert, wordt vervolgens gedeeld met de markt. Ieder incident op zich draagt zo bij aan het verbeteren van de informatiepositie van de verzekeraars in hun aanpak van verzekeringsfraude.

[4] Predictive analyses haalt informatie uit bestaande databronnen met als doel patronen, trends en uitkomsten vast te stellen. De techniek voorspelt niet de toekomst maar geeft met een zekere betrouwbaarheid wel aan wat mogelijk kan gebeuren.

Alle verzekeraars laten zien dat ze de aanpak van verzekeringscriminaliteit serieus nemen. Dat kan door transparant te zijn over fraudebeleid en de effecten daarvan. Via trendonderzoeken en communicatie naar aanleiding van afgeronde onderzoeken, wordt voortaan publiekelijk aandacht gegeven aan de successen van de markt-brede samenwerking tegen fraudeurs. Iedere eerlijke klant weet dat zijn verzekeraar zijn belangen[5] zo goed mogelijk beschermt; iedere potentiële fraudeur beseft welk risico hij aangaat.

Als frauduleus gedrag toch heeft plaatsgevonden, zal het onderzoek vanuit de verzekeraar vroegtijdig met de markt worden gedeeld. Alle Verbondsleden beschikken uiteindelijk over een incidentenregister van waaruit zij gegevens uit eigen fraudeonderzoeken ten algemeen nut doorgeven aan het CBV. Iedere incidentmelding die daarvoor aanleiding geeft, wordt tussen belanghebbende verzekeraars gedeeld. Het CBV, als centraal informatieknooppunt voor leden en stakeholders, draagt vervolgens met de verzamelde informatie en door middel van fraude-analyses en CBV-waarschuwingen over fraudetrends bij aan het terugdringen verzekeringsfraude.

Vijf vervolgstappen

1. Verbreden informatiestroom verzekeraars van en naar CBV
2. Verzamelen van meer, en meer diverse, data
3. Verdiepen samenwerking met publieke en private partijen en databronnen
4. Verbeteren analyse-mogelijkheden in het belang van preventie en detectie
5. Vergroten transparantie rondom beleid, aanpak en gevolgen van verzekeringsfraude

Wil een aanpak van verzekeringsfraude langdurig effect hebben, dan is het van belang dat de gehele markt zich daarvoor blijvend inzet. Verzekeraars en overige betrokken partijen - zoals politie, justitie en politiek - trekken in de toekomst steeds vaker samen op om het spreekwoordelijke net rond de verzekeringscrimineel te sluiten. Vanuit het CBV wordt daarom de samenwerking met diverse stichtingen op het gebied van de bestrijding van verzekeringscriminaliteit[6] verder geïntensiveerd. Het Verbond streeft er naar op deze manier meer beschikbare informatiebronnen en bestaande deskundigheid bijeen te brengen. Samen met al deze partijen wordt toegevoegde waarde gerealiseerd in de strijd tegen verzekeringsfraude en -criminaliteit.

[5] Zo bieden gedragsregels klanten kaders over wat zij van hun verzekeraar mogen verwachten; bijvoorbeeld rondom afhandelen van aanvragen en claims, de eerbiediging van de privacy maar ook dat men niet zomaar onderwerp van persoonlijk onderzoek wordt.
[6] Denk aan Stichting CIS, Stichting VbV, Stichting EPS, Stichting PV. Deze stichtingen zijn van oudsher al sterk gericht op het bijeenbrengen van verzekeraars en informatie.

Toekomst: fraudeaanpak in 2020

Een anonieme tipgever meldt bij een verzekeraar dat een bedrijf fraude pleegt met een ziekteverzuimverzekering. De informatie wordt gedeeld met het CBV en vergeleken met diverse databronnen. De gegevens uit de tip leiden tot een data-gerelateerd sneeuwbaleffect.

- Via controle op klant- en claimregistraties van verzekeraars wordt vastgesteld dat de fraudeur bij meerdere verzekeraars ziekteverzuimproducten afsluit;
- Vergelijking van de persoonsgegevens met andere publieke en private bronnen toont aan dat in de claims niet-bestaande personeelsleden worden opgevoerd;
- Controle van het bankrekeningnummer leidt tot de vaststelling dat meerdere ‘bedrijven’ hetzelfde nummer hanteren;
- Informatie uit het Handelsregister laat zien dat de directeur van de verdachte firma bestuurder is bij nog meer BV’s die weer voorkomen in de klant- en claimregistraties van andere verzekeraars.

De eerste tip leidt via dataverrijking en –duiding naar de onbetrouwbare bestuurder en zijn netwerk aan BV’s. Deze informatie wordt automatisch weer gekoppeld aan partijen die daardoor (kunnen) worden geraakt. Door de snelle signalering en informatie-uitwisseling wordt verdere schade bij deze maatschappijen voorkomen.