DATA EN DAADKRACHT

Een impactvolle aanpak van verzekeringscriminaliteit

VERBOND VAN VERZEKERAARS

Inhoudsopgave

Uitgave van het Verbond van Verzekeraars
Centrum Bestrijding Verzekeringscriminaliteit, 2020
Voor meer informatie: cbv@verzekeraars.nl

1. Inleiding

Het Verbond van Verzekeraars heeft in 2016[1] een beeld geschetst van de verwachte ontwikkelingen rondom bestrijding en voorkoming van verzekeringsfraude voor de verzekeringssector. De boodschap was dat verzekeraars 'streetwise' moeten worden door via gedeelde kennis en informatie fraudeurs eerder in het vizier te krijgen. Het Centrum Bestrijding Verzekeringscriminaliteit (CBV) van het Verbond stelt vast dat verzekeraars aan de vijf stappen uit het visiedocument van 2016 goede invulling hebben gegeven Zo wordt inmiddels steeds meer informatie over incidenten en fraudeurs gedeeld en worden samen met diverse stakeholders[2] experimenten uitgevoerd om de aanpak van verzekeringscriminaliteit te versterken.

Er is een sterke groei gerealiseerd in het aantal aangetoonde fraudes; van 8.336 bewezen fraudes in 2015 naar 12.979 bewezen fraudes in 2018. Er zijn initiatieven genomen om meer schade op daders te kunnen verhalen. Verzekeraars weten met hun aanpak van verzekeringscriminaliteit jaarlijks vele tientallen miljoenen aan besparingen te realiseren. Daarmee is echter niet gezegd dat de effecten van verzekeringscriminaliteit zijn afgenomen. Dat meer fraudes worden aangetoond, betekent dat het onderzoek naar en de aanpak van verzekeringscriminaliteit is verbeterd maar de strijd is zeker nog niet gestreden.

De groeiende deskundigheid en toepassing van technologie bij het misleiden van verzekeraars noodzaakt de markt tot meer gezamenlijk optreden, meer uitwisseling van kennis en informatie en meer solidariteit bij de inzet van onderzoekscapaciteit.

Het uitgangspunt van het Verbond dat 'verzekeringscriminaliteit niet mag lonen' is dan ook onverminderd relevant. Zeker gezien het feit dat de verschijningsvormen van deze criminaliteit continu blijven veranderen. Verzekeraars hebben daarom nog steeds een belangrijke rol bij het inperken van de effecten van criminele handelingen. Op basis van hun maatschappelijke verantwoordelijkheid moeten verzekeraars, met de inmiddels opgedane kennis, met nieuwe en aanvullende stappen blijven komen om succesvol impact te hebben en houden op de gevolgen van verzekeringscriminaliteit.

2. Relevante thema's in criminaliteitsaanpak

De maatschappij digitaliseert; technologie beheerst het dagelijks leven van iedereen. We zien voortdurend nieuwe ontwikkelingen die invloed hebben op ons leven en op onze wijze van communiceren. Technologische vernieuwingen veroorzaken beweging in het risicolandschap en beïnvloeden de rol van verzekeraars en het gedrag van hun klanten.

Revolutionaire veranderingen in technologie, solidariteit, risico's en consumentenhouding en complexiteit van regelgeving raken de kern van het verzekeren. De digitale vooruitgang biedt kansen voor iedereen die daar voordeel uit wil halen. Daaronder zitten ook criminelen die voortdurend inspelen op de technologische veranderingen en deze inzetten voor onrechtmatig handelen. De impact van georganiseerde en grensoverschrijdende criminaliteit neemt nog altijd toe en methoden om fraude te plegen worden steeds geavanceerder en lastiger te detecteren. Digitaal gemanipuleerde documenten en 'fake news' zijn niet of nauwelijks meer van echt te onderscheiden. Het

[1] Visiedocument 'Toekomst in aanpak van Verzekeringscriminaliteit', Verbond van Verzekeraars 2016
[2] Proeftuin Aanpak Verzekeringsfraude i.s.m. het Openbaar Ministerie en de politie

onderscheiden van valse zaken van de waarheid is nog steeds een onmisbare stap in de strijd tegen verzekeringscriminaliteit.

De ambitie van de verzekeringssector blijft het zoveel mogelijk terugdringen van schade die criminelen aan de financiële sector, verzekeraars, hun klanten en relaties toebrengen. Verzekeringscriminaliteit kent vele vormen en steeds weer nieuwe methoden. Dit vraagt om een aanpak langs diverse lijnen en met meerdere partijen. In aansluiting op de visie van 2016 wil het Verbond voor de komende jaren de focus leggen op:

1. Preventie;
2. Informatie- en datadeling;
3. Inzet van moderne technologie;
4. Samenwerking keten- en publieke partners;
5. Aanpak van georganiseerde criminaliteit en verhaal op daders.

3. Preventie: klantcommunicatie, product- en procesontwikkeling

De behoefte van verzekeraars aan snelle verwerking van klantvragen en claims lijkt vaak haaks te staan op het belang van gedegen onderzoek ten behoeve van fraudebeheersing. Toepassing van Straight Through Processing (STP) is goed voor de klantervaring maar niet bepaald gunstig voor de schadelast als gevolg van onrechtmatig claimen.

Er vindt relatief veel inspanning plaats op het traceren van de kleine(re) frauduleuze aanvragen en claims. Bewijs vergaren is vaak lastig waardoor zaken niet kunnen worden afgerond[3]. Verzekeraars moeten de focus leggen op preventie ter afschrikking van de ‘kleine fraudeur’ om tijd vrij te spelen om beschikbare onderzoekscapaciteit meer op grotere zaken te kunnen richten.

Verzekeraars kunnen gebruik maken van afschrikking van gelegenheidsfraudeurs door bijvoorbeeld tijdens de beoordelingen van claims in te zetten op aangekondigde ‘trajectcontroles’ en ‘vliegende brigades’ die steekproeven doen op claims. Leg dit vooraf uit aan klanten en laat zien dat secure afhandeling van aanvragen relevant is. Goede beoordeling van claims is in het belang van de klant en juist daarom vindt betaling niet altijd binnen 24 uur plaats.

Voorkomen van oplichting is meestal goedkoper dan achteraf terughalen wat onterecht is uitbetaald. Verzekeringsproducten en diensten moeten vanaf het moment van ontwikkeling tot en met de uitvoering in de praktijk beoordeeld worden op het risico van oneigenlijk gebruik. Bij het inrichten en vormgeven van aanvraag- en claimprocessen wordt aandacht besteed aan fraudegevoeligheid en de bewijspositie van de verzekeraars.

- **Verzekeraars communiceren op maatschappijniveau over consequenties van fraude en informeren klanten over fraudeaanpak**

- **Verzekeraars zorgen bij het ontwikkelen en aanpassen van producten en processen dat deze misbruikbestendig worden ingericht**

[3] In 2018 zijn bijna 43.000 onderzoeken uitgevoerd waarbij in 30% van de gevallen fraude is bewezen.

4. Informatiedeling: betrouwbaar omgaan met data

Verzekeringsoplossingen vragen om inzicht in risico's; het gaat onder meer om inzicht in het te verzekeren object en in de kans dat een verzekerde op onrechtmatige wijze gaat handelen. Meer verschillende en meer gedetailleerde data dragen bij aan betere risico-inschatting en fraudebeheersing. Van verzekeraars wordt verwacht, zowel door klanten als vanuit instanties op het gebied van financieel- of privacy-toezicht, dat hier op een integere wijze mee wordt omgegaan.

Er is steeds meer informatie van en over de (aspirant) klant beschikbaar. De klant zelf is, bewust en onbewust, belangrijk als dataleverancier. Het blijft voor verzekeraars noodzakelijk te kijken naar manieren om het waarheidsgehalte van die informatie te controleren en te beoordelen welke informatie mag en kan worden ingezet. Bij uitbreiding met nieuwe databronnen, of bij andere toepassing van bestaande informatie, moet steeds nagedacht worden over de juistheid van de informatie en betrouwbaarheid en bruikbaarheid van de bron.

Vanuit de maatschappelijke rol van de sector ligt de nadruk op het thema 'verzekerbaarheid'. Toegang tot steeds meer data moet niet leiden tot een spiraal van onverzekerbaarheid voor klanten die het hoogste of meest voorspelbare risico vormen. Verzekeraars moeten zuiver en transparant met al de beschikbare data omgaan, ook als het om het traceren van onbetrouwbare (aspirant) klanten en foute gedragingen gaat.

- **Verzekeraars maken bij aanpak van verzekeringscriminaliteit geen bovenmatig gebruik van informatie en zetten optimaal in op hoogwaardige databeveiliging**
- **Verzekeraars maken bij inzet en toepassing van nieuwe databronnen en -partners vooraf een afweging tussen opbrengst en impact op de betrokkene**
- **Verzekeraars hanteren bij onderzoek van incidenten en registratie van personen hoge eisen voor de gehanteerde procedures**

5. Moderne technologie: inzet van mens en machine

Het inzetten van technologie en combineren van databronnen is nodig om de crimineel de voet dwars te zetten. Maar datagebruik kent zijn grenzen. Naast de wettelijke begrenzing in datatoepassing is er zoveel data beschikbaar dat één persoon dit niet meer alleen kan verwerken, bevatten, filteren en analyseren. Maar een fraudepreventie- of detectiesysteem wordt nooit 'streetwise' zonder de inzet en oplettendheid van de fraudeonderzoeker en de signaleringsfunctie van alle verzekeringsmedewerkers. Investeren in systemen vraagt om investeren in de mensen die er mee omgaan.

Personeel dat fraudesignalen moet oppikken, moet weten waar ze naar moeten kijken en wat van ze verwacht wordt. Verzekeringspersoneel begrijpt de ins & outs van informatieverwerking en wordt met regelmaat geïnformeerd over methoden om fraude te herkennen en te bestrijden. Fraudeonderzoekers veranderen meer en meer in data-analisten en -specialisten.

Computers voeren steeds meer taken en activiteiten uit die normaal gesproken een vorm van menselijke intelligentie vragen; dit wordt Artificial Intelligence (AI) of kunstmatige intelligentie genoemd. Het kan om relatief eenvoudige taken gaan (denk aan robotgrasmaaiers en -stofzuigers) maar ook om systemen die beslissingen nemen met een grote impact op de betrokkene. Bij fraudeaanpak valt te denken aan gezichts- en stemherkenning, het signaleren van afwijkende patronen in claims en het doen van onderzoek naar schadeoorzaken en klanten.

Toepassing van AI in bedrijfsprocessen wordt al op allerlei terreinen – ook in de verzekeringssector - doorgevoerd. Besluitvorming over acceptatie en claimbeoordeling wordt gebaseerd op systemen die heel veel informatie afwegen. Dat geldt ook voor systematische analyse van mogelijke afwijkingen en onrechtmatigheden. Gezien de impact van een onjuist besluit op basis van algoritmen (van het afwijzen van een claim tot het ten onrechte beticht worden van fraude) moet de sector de noodzakelijke waarborgen toepassen. De verzekeraar moet zijn besluiten kunnen toelichten en uitleggen aan de klant; zeker als dat besluit autonoom door een kunstmatig intelligent systeem tot stand is gekomen. Besluiten moeten controleerbaar zijn[4].

- **Verzekeraars zetten bij toepassing van preventie- en detectiesystemen en besluitvorming rondom verzekeringscriminaliteit, optimaal getraind en deskundig personeel in**
- **Verzekeraars kunnen aan hun klanten uitleggen wat ze met data doen bij afhandeling van een verzekeringsaanvraag of claim**
- **Verzekeraars spelen in op de mogelijkheden die intelligente computersystemen bieden in de strijd tegen criminaliteit, maar gebruiken deze uitsluitend als hulpmiddel bij signalering van of besluitvorming over fraude of ander crimineel gedrag**
- **Verzekeraars oordelen niet op basis van systemen maar op basis van feiten**

6. Samenwerking: partners in crime

De strijd tegen verzekeringscriminaliteit door middel van dataverwerking en informatiedeling vraagt om een netwerk van experts. Deskundigen uit verschillende disciplines die in staat zijn grote hoeveelheden informatie te ontsluiten, te ontleden en te duiden in het belang van de markt. Binnen de bestrijding van verzekeringscriminaliteit ligt de uitdaging in het herkennen van modus operandi en onderkennen van zwakke plekken in de eigen bedrijfsvoering en producten.

[4] Zie ook Ethisch kader voor verzekeraars en data gedreven besluitvorming, Verbond van Verzekeraars 2020

Het Verbond heeft met het Data Competence Centre (DCC) een mogelijkheid gerealiseerd om data van, voor en door de sector te verwerken en analyseren. Het DCC fungeert als bron van informatie en ondersteunt de ontwikkeling van nieuwe processen en instrumenten. Samenwerking met het DCC leidt tot inzichten die de individuele verzekeraar kan inzetten bij risico-inschatting en het voorkomen en bestrijden van verzekeringscriminaliteit.
Doorontwikkeling van het DCC en de centrale verzameling van gegevens over risico's en claims draagt bij aan de ontwikkeling en verfijning van patroonherkenningsmodellen en betere validatie van informatie. Het DCC biedt de mogelijkheid om door middel van experimenten met geaggregeerde data, algoritmes en AI modellen te realiseren die de sector van dienst zijn bij het efficiënt en effectief herkennen van patronen en het tijdig signaleren van diverse vormen van verzekeringscriminaliteit.

Naast inzet van data en expertise uit de eigen gelederen richt het Verbond zich namens de sector op samenwerking met andere partijen in de (strafrecht)keten. Brede samenwerkingsverbanden, uniforme processen en afspraken met private en publieke partners moeten leiden tot meer barrières tegen crimineel gedrag en disruptief optreden tegen criminele verdienmodellen. Dit dient niet alleen het belang van de sector maar vindt ook plaats op verzoek van andere partijen ten behoeve van de bescherming van de maatschappij als geheel.

- **Verzekeraars delen data vanuit de eigen organisatie met het DCC met als doel op geaggregeerd niveau modellen te ontwikkelen en kennis over verzekeringscriminaliteit te vergroten**

- **Verzekeraars dragen actief bij aan samenwerkingsverbanden binnen en buiten de sector gericht op gezamenlijk optreden tegen verzekeringscriminaliteit**

Cyber-gerelateerde criminaliteit neemt nog steeds toe. Met i-CERT[5] beschikken de verzekeraars sinds enige jaren over een centrale waarschuwingsdienst voor cyberdreigingen. Verzekeraars kijken gezamenlijk naar cyberdreigingen en informeren elkaar via het meldpunt van i-CERT over potentiële dreigingen en daadwerkelijke inbreuken. Via deze lijn worden gedigitaliseerde fraudevormen gesignaleerd, gedeeld en aangepakt.

Cybercrime behelst meer dan alleen grootschalige DDOS-aanvallen of ransomware. Ook het digitaal manipuleren van bewijs voor een verzekeringsclaim valt hieronder en de financiële gevolgen daarvan zijn fors. Verzekeraars krijgen meer oog voor de zwakke schakels in het schadeafhandeling-proces en verbeteren deze punten. In geautomatiseerde bedrijfsprocessen moet digitale onderbouwing van een claim of aanvraag snel en effectief op juistheid kunnen worden gescreend.

De technische controlemogelijkheden om een opgegeven identiteit te verifiëren of ingestuurde foto's van een schade te onderzoeken worden geavanceerder. Toepassing van data-screening leidt tot betere selectie van onderzoeksignalen, verhoogt de pakkans en voorkomt meer fraude.

- **Verzekeraars wisselen informatie uit via i-CERT om cyberdreigingen te signaleren en daar samen tegen op te treden**

[5] Insurance Computer Emergency Response Team – samenwerking van IT afdelingen van aangesloten verzekeraars om elkaar te kunnen attenderen op en adviseren over cybercrime.

7. Georganiseerde criminaliteit en schadeverhaal

Iedere kwaadwillende particulier met een laptop kan tegenwoordig oplichter worden. Naast het groeiend aantal incidentonderzoeken naar de 'amateur'-fraudeur die zijn eigen verzekeraar probeert te tillen, ziet het CBV een toename in het aantal incidenten met modus operandi die bij meerdere verzekeraars tegelijkertijd worden toepast. Als één verzekeraar getroffen wordt door een dadergroep, volgen er al snel meer[6]. Bij grootschaliger fraudezaken is vaak sprake van professionele, georganiseerde criminaliteit die verder reikt dan alleen de verzekeringssector.

Groeiende aandacht vanuit de georganiseerde criminaliteit voor de financiële sector leidt tot grotere schades door professioneel uitgevoerde fraudes. De geraffineerdheid van beroepsfraudeurs neemt toe.

In 2016 is al aangegeven dat samenwerking op strategisch en operationeel niveau een vereiste is voor het effectief bestrijden van verzekeringscriminaliteit. Het delen van kennis en ervaringen door verzekeraars onderling en met het CBV moet doorgroeien. Wat betreft operationele samenwerking zijn verbindingsvraagstukken tussen de verzekeraars en het CBV op technisch en organisatorisch niveau steeds beter overbrugbaar.

Om professionele, georganiseerde criminaliteit de baas te kunnen, is eenzelfde mate van professionaliteit en georganiseerdheid aan de kant van de sector nodig. Verzekeraars breiden om die reden de deling van kennis en informatie verder uit om effectief te zijn in het waarschuwen van de markt. Door krachten op operationeel niveau tussen verzekeraars, en met andere stakeholders, verder te bundelen wordt meer bereikt in de fase voordat de fraudeur kan toeslaan. Inzet van methoden om informatie te delen[7] en meer samenwerking met publieke opsporingsdiensten moet leiden tot betere aanpak van professioneel handelende verzekeringscriminelen.

Verhalen van schade op criminelen is – zeker per individuele verzekeraar – vaak een kostbare aangelegenheid waarbij onzeker is of de kosten van verhaal opwegen tegen het resultaat. Door krachten te bundelen en gezamenlijk op te treden in onderzoek en procedures worden de kansen op succesvol terughalen van de geleden schade vergroot en kan de financiële impact per maatschappij worden beperkt. Gezamenlijke initiatieven van gedupeerde verzekeraars en publieke partners om crimineel vermogen af te pakken, dragen er aan bij dat verzekeringscriminelen hun focus minder op de financiële sector richten.

- **Verzekeraars richten bij fraudeaanpak meer onderzoekscapaciteit op de aanpak van georganiseerde verzekeringscriminaliteit**

- **Verzekeraars dragen actief bij aan het verhalen van schade op verzekeringscriminelen**

[6] Na de marktwaarschuwing over fraude met 'Mijn omgeving' bij een verzekeraar ontving het CBV direct signalen van meer getroffen verzekeraars. Alle maatschappijen waren getroffen door dezelfde dadergroep.
[7] Denk onder meer aan deelname aan het Protocol Incidentenwaarschuwingssysteem Financiële Instellingen en de CIS Referentie Tool – zie hierover o.a. www.verzekeraars.nl en www.stichtingcis.nl