

Contactpersoon

[redacted]

Contactgegevens

☎ +32 [redacted]
✉ [redacted]@benelux.int

Ons kenmerk

14-FISC-SYS(NO-001)NL

Datum

12.09.2014

Onderwerp

Systeemfraude

AANPAK SYSTEEMFRAUDE IN NEDERLAND, STAND VAN ZAKEN JULI 2014

Inleiding

In Nederland is sinds een aantal jaren het fenomeen systeemfraude onderkend. Naast fiscale fraude, waar de burger zicht richt op het niet of zo weinig mogelijk betalen van belasting, is er een fenomeen ontstaan om de uitbetalingen van de Belastingdienst (in de vorm van teruggaven Omzet- en Inkomstenbelasting en Toeslagen) te verkrijgen middels het indienen van frauduleuze aangiften.

Nederlandse situatie

De Nederlandse belastingssystemen en toeslagssystemen zijn ingericht op het zo soepel mogelijk laten verlopen van massale processen waarbij wordt uitgegaan van het vertrouwensbeginsel richting burgers. Het vooraf uitbetalen op Voorlopige Aangiften of Toeslagen maken deel uit van dat beginsel. Dat betekent beslissen en voorlopig uitbetalen na een summier en voorlopig oordeel op een moment waarop de Belastingdienst nog niet beschikt over bruikbare contra-informatie. Pas later vindt een definitieve beoordeling van aangiften en verzoeken plaats en vindt pas later aan de 'achterkant' controle plaats. Dan worden voorlopige uitbetalingen eventueel herzien en wordt gepoogd hetgeen in eerste aanleg teveel is uitbetaald, weer terug te vorderen. Meest in het oog springende voorbeeld van de afgelopen tijd is de Toeslagenfraude door Bulgaren.

Zoals gemeld is een jaar of twee geleden onderkend dat dit Toeslagensysteem ondermijnd wordt door frauduleuze aanvragen die leiden tot grote teruggave waarbij de verrekenmogelijkheid achteraf uit blijft en oninbaar moet worden geleden.

Definitie systeemfraude

Systeemfraude is elke (georganiseerde) poging tot het laten uitbetalen van geld door de Belastingdienst, die is gebaseerd op gefingeerde of foute gegevens, waarbij gebruik gemaakt wordt van het systeem waarbij eerst wordt uitbetaald en pas daarna gecontroleerd.

Systeemfraude manifesteert dus zich bij die belastingmiddelen die werken met (voorlopige) uitbetalingen van belastinggelden. Dit gebeurt bij de Inkomstenheffing d.m.v. voorlopige teruggaven (van reeds eerder ingehouden Loonheffing), bij Toeslagen (is een vorm van subsidie) en bij de Omzetbelasting in de vorm van negatieve aangiften (uitbetalen van reeds aan voorheffingen betaalde gelden aan derden). Maar ook in de Loonheffing door het opvoeren van gefingeerde dienstbetrekkingen.

Bij het beantwoorden van de vraag hoe systeemfraude kan worden bestreden en voorkomen, dient de gehele keten bekeken te worden. In ieder deel van deze keten zijn mogelijkheden om de fraude aan te pakken. Gezien de hele keten enkele hoofdpunten:

- = Goede duidelijke en eenvoudige wetgeving die goed uitvoerbaar en controleerbaar is.
- = Duidelijke overheid, dienstverlenend waar het kan en streng waar het moet.
- = Gedrag van burgers beïnvloeden. Subjectgericht werken.
- = Werken met Green en Red lane en met gedifferentieerde dienstverlening.
- = De processen en programma's meer fraudeproof maken.
- = Goede fraudedetectie aan de poort en goede intelligence.
- = Tijd om fraude aan te pakken, in de heffing, opsporing en vervolging.
- = Als gehele overheid samenwerken.

Naast fraude door individuele burgers komt ook georganiseerde systeemfraude voor. In deze gevallen wordt de fraude op initiatief van een hoofddader georganiseerd. Deze dient dan verzoeken of aangiften in namens honderden of enkele duizenden burgers.

Uitgangspunten bij de bestrijding van systeemfraude in Nederland

De bestrijding van systeemfraude vindt plaats aan de hand van het principe dat we dit zo vroeg mogelijk na de poort (d.w.z. na binnenkomst van de aangifte of de aanvraag voor een Toeslag) willen laten plaatsvinden. Reden hiervoor is dat het voorkomen van het kunnen frauderen, danwel het voorkomen van het binnendringen in het aangifteverwerkingssysteem van frauduleuze aangiften goedkoper is dan het achteraf herstellen van grote aantallen frauduleuze aangiften. Een tweede principe is dat, in tegenstelling tot vroeger, niet meer m.b.t. alle frauduleuze aangiften geprobeerd wordt om die in het strafrecht te betrekken. Bestuursrechtelijk en soms semi-massaal afdoen gevolgd door een stevig inningstraject geeft, zo blijkt, veelal een goede response op de compliance.

Aanpak detectie

Onderscheid gemaakt moet worden tussen de verschillende belastingmiddelen en toeslagen. Voor wat betreft de Inkomstenbelasting begint de detectie van fraude al op het moment dat een burger zijn aangifte verzendt en die aangifte onze firewalls passeert. Op dat moment wordt de digitale fingerprint van die ingezonden aangifte vastgelegd en geautomatiseerd (d.m.v. Splunk) geanalyseerd op fraude. Aangiften die risicovol (op m.n. fraude) zijn worden apart gezet om te kunnen worden beoordeeld, de andere aangiften gaan verder het systeem in. Verdere analyse. Elke week wordt een gehele weekinzending, na afloop van die week m.b.v. een 40-tal queries verder geanalyseerd op de aanwezigheid van vermoedelijke fraude. Zo dit het geval is, dan worden die aangiften ter behandeling aan de belastingkantoren gezonden.

Voor wat betreft toeslagen is het nu reeds mogelijk om nog voordat een fraudeur daadwerkelijk een frauduleus verzoek indient, te onderkennen dat op onze website een fraudeur aan het surfen is. Deze mogelijkheid stelt ons in staat om tijdig een vlaggetje te zetten bij een binnenkomend bericht.

Nieuwe vormen van detectie

Er wordt veel onderzoek gedaan naar de manier waarop fraudeurs frauderen en hetgeen daarbij wordt ontdekt wordt vastgelegd. Doel daarbij is om kenmerken van fraudeurs te ontdekken en vast te leggen. Met die kenmerken is het mogelijk om aan de poort niet allen te kunnen selecteren op frauduleuze aangiften, maar ook om daar te kunnen selecteren op de persoon, het subject, dat die aangifte indient. Niet alleen handmatig en kennis gedreven worden die kenmerken bepaald. Sinds kort maken we bij de bepaling van de kenmerken van een fraudeur ook gebruik van zgn. data-scientist die d.m.v. algoritmen in onze bestanden groepen van fraudeurs, maar ook van niet-fraudeurs bepaalt. Op die manier bepaalt als het ware de computer de kenmerken. Als vervolgens die kenmerken worden toegepast op de gehele populatie van belastingplichtigen (datamining) worden nieuwe, nog reeds onbekende fraudeurs ontdekt. Deze vorm van profiling kan volgens de eerste ervaringen daarmee succesvol zijn. Daarom wordt nu gezocht naar software die het ontdekken van die kenmerken (door oa. modelling etc.) aanmerkelijk kan verkorten en vereenvoudigen. Doel is dat in de toekomst op veel meer plaatsen profielen worden toegepast met als doel het in een zo'n vroeg mogelijk stadium tegenhouden van fraudes.

Onderzoek van de fraudeur en zijn relaties

Als op bovenbeschreven wijze fraudes zijn ontdekt en lijsten met fraudeurs zijn opgesteld zijn we in staat om elke fraudeur apart te bekijken op de relaties die hij heeft. Onze ervaring is dat dergelijk onderzoek zeer nuttig kan zijn als wordt gestuurd op het in een keer onschadelijk maken van een groep van fraudeurs. Gezocht wordt dan handmatig in bronsystemen, maar sinds kort beschikt Nederland over een dynamisch zoekssysteem aan de hand waarvan op eenvoudige wijze alle relaties (telefoon, adres, bestuursfuncties in allerlei NV's etc.) die blijken uit de gegevens van de Kamer van Koophandel van een fraudeur kunnen worden weergegeven. Het voordeel van een dergelijk dynamisch systeem is dat voortdurend delen van een samenwerkende fraudegroep apart getoond en weer ingeklapt kunnen worden. Op deze manier ontstaat een zeer compleet beeld van de fraudeur en al zijn relaties. Bij het inactief maken van een dergelijke fraudegroep kan dan niet een deel daarvan buiten het zicht van de fiscus blijven.

Slot

Fraudeurs en hun fraudes vinden uiteindelijk hun neerslag in onze computersystemen. Dat is voor Nederland nog steeds geen reden geweest om het systeem waarbij eerst wordt uitbetaald en pas daarna gecontroleerd los te laten. Wel is er geïnvesteerd in een betere geautomatiseerde detectie aan de poort en beter analysetechnieken waarmee meer fraudeurs konden worden ontdekt en aangepakt.
