Ministerie van Justitie en Veiligheid

> Retouradres Postbus 20301 2500 EH Den Haag

Aan de Voorzitter van de Tweede Kamer
der Staten-Generaal
Postbus 20018
2500 EA DEN HAAG

Directoraat-Generaal Politie en Veiligheidsregio's
Programma Politiële Taken

Turfmarkt 147
2511 DP Den Haag
Postbus 20301
2500 EH Den Haag
www.rijksoverheid.nl/jenv

Projectnaam
Politiële beleidsontwikkeling

Ons kenmerk
2705778

Bij beantwoording de datum en ons kenmerk vermelden. Wilt u slechts één zaak in uw brief behandelen.

Datum 15 november 2019
Onderwerp Aanpak internetoplichting (online handelsfraude)

Tijdens het Algemeen Overleg Strafrechtelijke onderwerpen (17 april 2019) heb ik toegezegd uw Kamer nader te informeren over de aanpak van internetoplichting (online handelsfraude). Specifiek informeer ik u in deze brief over de ontwikkelingen rond en borging van het Landelijk Meldpunt Internetoplichting (LMIO) van de politie en actuele cijfers van het LMIO en fraude met online handel in het algemeen. Verder informeer ik u over het gesprek dat ik heb gevoerd met banken over gegevensdeling met slachtoffers. Ik ga daarbij in op de samenwerking met de politie en voorlichting over de wijze van internetoplichting.

Ontwikkelingen en borging LMIO

Ik heb u eerder per brief [1] en ook tijdens het laatste Algemeen Overleg over FINEC (oktober 2018) gemeld dat de functionaliteiten van het LMIO geborgd worden en dat een projectleider in opdracht van de politie onderzoekt en adviseert (over) wat de beste manier is om het meldpunt structureel binnen de politieorganisatie te beleggen. De leiding van de nationale politie heeft -in afstemming met het OM en de PPS-partners- de koers voor borging en vernieuwing van de functionaliteiten van het LMIO op 14 augustus jl. vastgesteld. De hoofdlijnen van deze koers zijn:

- De functionaliteiten m.b.t. publiek-private samenwerking (PPS), intake, kwaliteitscontrole, analyse, media en projectvoorbereiding worden kwalitatief versterkt en geborgd op landelijk niveau.
- De positie van de regionale eenheden in het aanpakken van internetoplichting (online handelsfraude) wordt versterkt door meldingen hiervan zoveel mogelijk geautomatiseerd door te zetten naar de Basisvoorziening Handhaving (BVH) van de regionale eenheid waar de verdachte woont.

Het implementatietraject is gestart. Hierbij wordt steeds in overleg met het OM en de PPS-partners bekeken of de beoogde werkwijze in de praktijk werkt. De politie onderzoekt of gekomen kan worden tot een gezamenlijk portaal van private en

[1] Kamerstuk nr. 34615, nr. 11 en 12

publieke partijen voor meldingen en afwikkeling van internetoplichting. Het LMIO is een effectief samenwerkingsverband van private en publieke partijen. De implementatie vindt daarom in nauwe samenwerking tussen alle betrokken partijen plaats. Ik zal uw Kamer periodiek over de werking van het LMIO informeren.

Cijfers en trends online handelsfraude

Jaarlijks publiceert het LMIO van de politie actuele cijfers van aangiften van internetoplichting (online handelsfraude).

2018
In 2018 zijn in totaal 43.779 aangiften bij het LMIO binnen gekomen, een stijging van ruim 14% ten opzichte van 2017 (38.343 aangiften). Van de 43.779 aangiften zijn er 7.190 intrekkingen geweest en 13.174 niet vervolgbare aangiften. In 2018 bleven na aftrek van de intrekkingen en de niet vervolgbare aangiften 23.415 aangiften over. Van deze aangiften zijn er 5.121 door het LMIO in behandeling genomen.

In 2018 zijn 281 verdachten van fraude met online handel door de politie bij het OM aangeleverd[2]. Hierbij dient te worden opgemerkt dat een zaak tegen één verdachte veelal meerdere aangiften kan bevatten. Er zijn 218 zaken tegen verdachten van online handelsfraude door het OM afgedaan.
Bijna de helft van de verdachten is gedagvaard voor de strafrechter (48%) en een klein deel van de verdachten heeft een OM-strafbeschikking opgelegd gekregen (3%). De overige zaken zijn al dan niet voorwaardelijk geseponeerd of gevoegd bij andere strafzaken tegen een verdachte.

Bij genoemde cijfers dient in ogenschouw te worden genomen dat niet elke aangifte bij de politie een rechtsgeldige aangifte blijkt te zijn. Na kwaliteitscontrole wordt een aantal aangiften ingetrokken. Bijvoorbeeld omdat er geen strafbaar feit is, omdat het goed later geleverd is of het geld is terug betaald of omdat er sprake blijkt te zijn van wanprestatie e.d. Ook kan er sprake zijn van niet vervolgbare aangiften, dat wil zeggen dat de analyse is dat de aangifte onvoldoende aanknopingspunten voor succesvolle opsporing en vervolging biedt, bijvoorbeeld omdat een aangifte niet te koppelen is aan andere aangiften.

2019
Tot 1 juli 2019 zijn 26.333 aangiften binnen gekomen (in dezelfde periode in 2018 waren dat er 19.769). Van deze aangiften zijn in de periode 1 januari tot 1 juli 2019 2.526 aangiften door het LMIO in behandeling genomen.
In het eerste half jaar 2019 zijn 4.264 aangiften ingetrokken. De politie merkt hierbij op dat het aantal aangiften weliswaar is gestegen, maar dat van deze aangiften ook een toegenomen aantal weer is ingetrokken.

Tot en met juli 2019 zijn 142 verdachten van fraude met online handelsfraude door de politie bij het OM aangeleverd. In die periode zijn door het OM 180 zaken afgedaan tegen verdachten van online handelsfraude.

[2] Dit cijfer is afkomstig uit de Fraudemonitor OM 2017-2018 (Kamerstuk 17050, nr. 581)

Directoraat-Generaal Politie en Veiligheidsregio's
Programma Politiële Taken

Datum
15 november 2019

Ons kenmerk
2705778

De politie geeft aan dat de stijging van het aantal aangiften ten aanzien van online handelsfraude niet specifiek te wijten is aan één fenomeen of trend. De stijging heeft betrekking op het totale speelveld van online handelsfraude. Wel wordt een toename gezien van fraude waarbij de betaling heeft plaatsgevonden via een betaalverzoek. Mogelijk dat aandacht via de media voor internetoplichting en oproepen tot het doen van aangifte een stijging heeft veroorzaakt.

Om sneller vast te stellen of sprake is van een strafbaar feit hebben aangevers sinds 26 september de keuze om gebruik te maken van de 'slimme keuzehulp', die werkt met kunstmatige intelligentie. Mensen krijgen daarmee eerder duidelijkheid en een handelingsperspectief indien geen sprake is van een strafbaar feit. Hiermee wordt de dienstverlening vergroot. Onterechte aangiftes kunnen hiermee worden voorkomen en de politie kan zich concentreren op de zaken die wel strafbaar zijn, zoals het geval is bij moedwillige oplichting. Als er alleen sprake is van wanprestatie, is het geen zaak voor de politie.

Naast het strafrechtelijke traject vinden ook alternatieve interventies door de politie plaats zoals een 'stopgesprek'. Dit is een alternatieve afdoening waarbij een verdachte/rekeninghouder uit de anonimiteit wordt gehaald door het gesprek met hem/haar aan te gaan. De rekeninghouder wordt bewogen tot het terugbetalen van de ontvangen geldbedragen, waardoor benadeelden de aangifte kunnen intrekken en strafvervolging wordt voorkomen. Voldoet hij/zij daar niet aan dan zal alsnog een strafrechtelijk traject worden ingezet.

Gesprek met banken

In mijn brief van 5 april jl. aan uw Kamer[3] heb ik uiteengezet wat banken doen om fraude te voorkomen en slachtoffers te ondersteunen, bijvoorbeeld door middel van fraudedetectie, waarbij verdachte transacties worden gesignaleerd en onderzocht en contact met de klant wordt opgenomen. Ook werken banken samen door bijvoorbeeld het delen van modus operandi en bij voorlichtingsactiviteiten ten behoeve van burgers en bedrijven. Het voorkomen van fraude en schade voor benadeelden heeft de continue aandacht van banken, waarbij steeds wordt gezocht naar verbetering van processen en tools.

Daarbij gaven banken aan dat het voorkomen van zogenaamde bancaire fraude, waarbij sprake is van misbruik van betaalmogelijkheden die de bank aan klanten ter beschikking stelt, eenvoudiger is dan het voorkomen van niet-bancaire fraude, waarbij de klant zelf geld overmaakt. Internetoplichting is hier een voorbeeld van. Bij niet-bancaire fraude zijn de mogelijkheden van banken om in te grijpen beperkt omdat banken verplicht zijn een betaalopdracht van een klant uit te voeren. Banken hebben overigens aangegeven de ambitie te hebben om ook niet-bancaire fraude beter te kunnen voorkomen, welke ambitie ik heb onderschreven.

Zoals ik in het Algemeen Overleg op 17 april jl. heb gezegd voerde ik op dat moment nog gesprekken met de banken over het punt van gegevensdeling. Het gaat hierbij om het verstrekken van gegevens over naam, adres en woonplaats (NAW-gegevens) van een (vermeende) fraudeur door banken aan een slachtoffer zodat het slachtoffer civielrechtelijke actie in geval van (vermeende) fraude kan

[3] Kamerstuk nr. 29 911, nr. 237

Directoraat-Generaal Politie en Veiligheidsregio's
Programma Politiële Taken

Datum
15 november 2019

Ons kenmerk
2705778

nemen. Ik heb ook bij die gesprekken aangegeven dat ik van banken verwacht dat ze zich verantwoordelijk tonen voor het voorkomen van fraude en dat ze zich inspannen voor slachtoffers hiervan.

In genoemde gesprekken benadrukten de banken opnieuw dat het voor hen vanwege geldende privacywetgeving niet mogelijk is om de NAW-gegevens van (vermeende) fraudeurs te verstrekken aan (vermeende) slachtoffers. Ook hebben banken opnieuw benadrukt dat een dergelijke gegevensdeling gecompliceerd is omdat het voor banken ondoorzichtig is en zeer moeilijk is vast te stellen of er bij een overboeking op een rekening echt sprake is van strafrechtelijke (internet)oplichting. Of dat er wellicht sprake is van een civielrechtelijk geschil, waarbij een persoon geen slachtoffer is van fraude maar bijvoorbeeld ontevreden is over een geleverde prestatie. Daarnaast is het moeilijk vast te stellen of de desbetreffende tegenrekening daadwerkelijk van de fraudeur zelf is of dat er bijvoorbeeld sprake is van identiteitsfraude en de houder van de rekening dus zelf slachtoffer is. Ook kan er sprake zijn van een katvanger, waardoor de feitelijke fraudeur buiten beeld blijft. Het onder die omstandigheden verstrekken van NAW-gegevens van een (vermeende) fraudeur aan een (vermeend) slachtoffer zou onzorgvuldig en wellicht zelfs onrechtmatig zijn. Bovendien zou dit kunnen leiden tot eigenrichting, dat weer ernstige gevolgen kan hebben voor de vermeende dader én het vermeende slachtoffer.

Banken gaven aan dat wanneer slachtoffers het niet eens zijn met de terughoudendheid van banken om NAW-gegevens te verstrekken zij dit altijd kunnen voorleggen aan de civiele rechter, die dan bepaalt welk belang prevaleert.

Ik begrijp de positie van banken als het gaat om het verstrekken van NAW-gegevens van (vermeende) fraudeurs aan (vermeende) slachtoffers. Van banken kan niet verwacht worden dat zij gegevens van betrokkenen delen met (vermeende) slachtoffers, wanneer dit strijdig is met de geldende privacywetgeving. Ook begrijp ik het standpunt van de banken dat het onzorgvuldig zou zijn om NAW-gegevens van een vermeende dader te verstrekken aan een persoon, die meent slachtoffer te zijn van fraude, als banken onvoldoende (hebben) kunnen vaststellen of er werkelijk sprake is van fraude en of de vermeende fraudeur daadwerkelijk de fraudeur is. Dat zou kunnen leiden tot door de banken gesignaleerde ongewenste gevolgen, zoals eigenrichting.

Al eerder heb ik uw Kamer bericht[4] dat ook de politie heeft aangegeven dat het verstrekken van NAW-gegevens van vermeende fraudeurs onaanvaardbare risico's voor de persoonlijke levenssfeer van betrokkenen met zich mee kan brengen. Er dient steeds zorgvuldig te worden onderzocht en vastgesteld dat er sprake is van een strafbaar feit en een (strafbare) dader. Het verstrekken van NAW-gegevens van een persoon, waarbij dit nog niet zeker is, kan disproportioneel en dus onrechtmatig zijn.

De politie kan, zoals ik in mijn brief aan uw Kamer van 18 december 2017[5] heb aangegeven, na zorgvuldig onderzoek op grond van artikel 18 eerste lid van de Wet Politiegegevens en artikel 4:2, eerste lid, onder n van het Besluit Politiegegevens gegevens over een fraudeur verstrekken aan een slachtoffer t.b.v. een civielrechtelijk geding.

[4] Kamerstuk 34615, nr. 11, p.3
[5] Kamerstuk 34615, nr. 11, p.2

Samenwerking politie en banken

Directoraat-Generaal Politie en Veiligheidsregio's
Programma Politiële Taken

Datum
15 november 2019

Ons kenmerk
2705778

Het vorenstaande neemt niet weg dat alle mogelijkheden om internetoplichting te voorkomen en –als het zich toch heeft voorgedaan- slachtoffers van internetoplichting te ondersteunen ingezet moeten worden, ook als het gaat om gegevensverstrekking aan slachtoffers.

Zoals ik ook in mijn genoemde brief van 5 april jl. aangaf werken banken en de politie momenteel al samen om fraudeurs op te sporen. De samenwerking tussen banken en het LMIO en binnen de Electronics Crime Taskforce (ECTF) zijn hier voorbeelden van. Deze samenwerkingen worden periodiek geëvalueerd en op details bijgestuurd en verbeterd. Bovendien treffen politie en banken elkaar geregeld in diverse werkoverleggen, waarbij gesproken wordt over het tegengaan van nieuwe fraudevormen, verbetering van de fraudedetectie en voorlichting van het publiek.

De banken hebben mij aangegeven bereid te zijn verder in gesprek te gaan met de politie en te verkennen of de samenwerking in het kader van de doorontwikkeling van het LMIO geïntensiveerd kan worden en hoe dit kan leiden tot betere preventie en opsporing van internetoplichting. Deze verkenning zal zich bijvoorbeeld richten op data-analyse en het beter laten aansluiten van werkprocessen van banken en politie. Deze gesprekken tussen banken en politie lopen momenteel.

De Minister van Justitie en Veiligheid

Ferd Grapperhaus