Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2018–2019

29 911 Bestrijding georganiseerde criminaliteit

Nr. 237 **BRIEF VAN DE MINISTER VAN JUSTITIE EN VEILIGHEID**

Aan de Voorzitter van de Tweede Kamer der Staten-Generaal

Den Haag, 5 april 2019

Tijdens het Algemeen Overleg over Financieel-economische criminaliteit op 4 oktober 2018 heb ik uw Kamer toegezegd met de banken in gesprek te gaan over hun bijdrage aan de bestrijding van internetoplichting en de mogelijkheden van banken om burgers, die aangifte hebben gedaan van dergelijke fraude, te ondersteunen bij het civielrechtelijk verhaal van hun schade door (eerdere) verstrekking aan het slachtoffer van gegevens van de tenaamstelling van de bankrekening van de fraudeur[1]. Tevens heb ik uw Kamer toegezegd met het Openbaar Ministerie (OM) in gesprek te gaan over de door uw Kamer geuite zorg dat het OM mogelijk terughoudend zou zijn om op verzoek van de Autoriteit Financiële Markten (AFM) conservatoir beslag te leggen om te voorkomen dat mogelijk frauduleus vermogen naar het buitenland verdwijnt[2]. Met deze brief informeer ik u over de uitkomsten van de door mij gevoerde gesprekken.

1. Gesprek met de banken

Op 30 november 2018 heb ik gesproken met de voorzitter van de Nederlandse Vereniging van Banken (NVB), de heer Buijink, over de vraag wat banken doen aan de preventie van fraude, waarvan burgers en bedrijven slachtoffer worden, de zogenaamde horizontale fraude. Daarbij is specifiek internetoplichting aan de orde gekomen. Ook heb ik gesproken over wat banken doen voor slachtoffers van fraude en welke (verdere) maatregelen banken kunnen nemen.
Tijdens dat gesprek heeft de voorzitter van de NVB mij geïnformeerd over de huidige activiteiten van banken op het gebied van fraudepreventie. Daarbij maakte hij onderscheid tussen de zogenaamde *bancaire* fraude en *niet-bancaire* fraude. Bij *bancaire fraude* is sprake van de situatie dat criminelen de controle overnemen van de betaalmogelijkheden van een slachtoffer, zoals fraude met internetbankieren (bijvoorbeeld door verkrijging via phishing van de benodigde persoonlijke gegevens en

[1] Kamerstuk 29 911, nr. 210, p. 16, 17.
[2] Kamerstuk 29 911, nr. 210, p. 12, 13.

kst-29911-237
ISSN 0921 - 7371
's-Gravenhage 2019

beveiligingscodes van slachtoffers) en fraude met betaalpassen. Bij *niet-bancaire* fraude is sprake is van de situatie dat een slachtoffer onbewust of onder valse voorwendsels *zelf* de betaling aan de fraudeur initieert, op basis van een door hem ingevoerd rekeningnummer. Dit is bijvoorbeeld het geval bij internetoplichting via een online markplaats of factuurfraude.

De omvang van *bancaire* fraude is gedaald. De banken werken bij de preventie hiervan nauw samen. Banken komen slachtoffers van deze vorm van fraude tegemoet door actief onderzoek te doen en door het uit coulance grotendeels vergoeden van de geleden schade. Daarbij nemen banken wel in beschouwing of klanten hebben gehandeld overeenkomstig de zogenaamde uniforme veiligheidsregels, die zich richten het veilig omgaan door de klant met elektronisch bankieren en elektronisch betalen. Het gaat dan bijvoorbeeld om het geheim houden van beveiligingscodes, het ervoor zorgen dat een bankpas niet door een ander gebruikt wordt en beveiliging van de apparatuur die gebruikt wordt voor bankzaken[3].

Bij *niet-bancaire* fraude, zoals internetoplichting, is de rol van banken anders. Wanneer een klant zelf een betaalopdracht initieert en de fraudedetectiesystemen geen aanleiding geven tot twijfel, is de bank gehouden om de opdracht van de klant uit te voeren. De banken hebben echter aangegeven dat dit niet betekent dat de sector er niet alles aan doet om ook niet- bancaire zoveel mogelijk te voorkomen.

Ik heb de NVB en banken verzocht in kaart te brengen hoe men fraude probeert te voorkomen en op welke punten zij verdere mogelijkheden zien voor verbetering van de preventie en bestrijding van (met name) niet-bancaire fraude en de ondersteuning van slachtoffers hiervan.

Activiteiten banken ter preventie van fraude

De banken hebben mij aangegeven dat zij (al dan niet in samenwerking met Betaalvereniging Nederland) ter *preventie* van fraude:

- zich actief bezig houden met *voorlichting* met als doel als klanten bewust te maken van potentiele frauderisico's. Daartoe worden onder andere vanuit de Takforce Veilig Bankieren interbancaire voorlichtingscampagnes geïnitieerd, zoals de campagne «Hang op, klik weg, bel uw bank». Ook informeren banken hun klanten via hun websites, social media en nieuwsbrieven. Daarbij hebben banken speciale aandacht voor kwetsbare groepen zoals senioren en scholieren.
- een aantal systemen en producten hebben ontwikkeld om de *veiligheid van de betaalinfrastructuur* verder te verbeteren en klanten zo te ondersteunen bij het veilig betalen. Te denken valt aan de IBAN-naamcheck (naam-nummercontrole) en systemen zoals iDEAL, iDEAL QR en iDEAL-betaalverzoeken. Maar ook aan de zogenaamde «gelijkoversteken»-service, die klanten van een online marktplaats kunnen inzetten om hun transacties veilig te laten verlopen.
- Werken met verschillende *fraudedetectie-systemen* om fraudeleuze transacties op te sporen en te onderzoeken. Iedere bank richt zelfstandig zijn fraudedetectie in. Onderdelen van de fraudedetectie zijn:
  - o Real time fraudedetectiesystemen: dit zijn complexe beslissingssystemen die continue (24/7) draaien en alle transacties van klanten monitoren. Daarbij gaat het om miljarden transacties. De systemen worden door een grote hoeveelheid informatie gevoed, waaronder meldingen van klanten zelf. De monitoring vindt plaats op basis van vele indicatoren, zoals de locatie, hoogte van het bedrag en naar

[3] https://www.betaalvereniging.nl/wp-content/uploads/Uniforme-veiligheidsregels-particulieren.pdf.

welke tegenpartij geld wordt overgemaakt. Een transactie wordt automatisch geparkeerd of tegengehouden als uit de fraudedetectie het vermoeden voortkomt dat een transactie frauduleus kan zijn.

- Operationele opvolging van signalen en meldingen: de door het fraudedetectiesysteem gegenereerde signalen (alerts) worden onderzocht door medewerkers van de bank. Daarbij wordt vrijwel altijd contact met de klant gezocht. De beschikbaarheid van personeel hiervoor verschilt per bank. Naast signalen uit fraudedetectiesystemen ontvangen medewerkers van banken ook meldingen over fraude van klanten zelf. Fraudemedewerkers van banken zetten zich in om die klanten zo goed mogelijk te helpen en schade voor de klant zoveel mogelijk te beperken.
- Intensieve samenwerking tussen banken op gebied van kennis, expertise en intelligence, bijvoorbeeld over (nieuwe) modus operandi van criminelen en inzet van nieuwe technologieën, zoals kunstmatige intelligentie en machine learning. Dit wordt gefaciliteerd door de NVB en Betaalvereniging Nederland.

De banken hebben bij vorenstaande aangegeven dat fraudedetectie bij bancaire fraude succesvoller is dan fraudedetectie bij niet-bancaire fraude. Dit heeft te maken met het feit dat er voor de detectie van niet-bancaire fraude minder bruikbare data beschikbaar zijn. Dit komt doordat een klant bij niet-bancaire fraude gebruik maakt van eigen apparatuur, bijvoorbeeld pc of mobiel, en ook zelf de transactie verricht.

Daarnaast is de realiteit altijd complexer dan een systeem kan detecteren: normale transacties kunnen ten onrechte als frauduleus worden bestempeld. En fraudeleuze transacties kunnen ten onrechte als normaal worden gezien, bijvoorbeeld wanneer gebruik is gemaakt van rekeningen van katvangers.

Banken zijn afhankelijk van de fraudedetectiesystemen gezien de hoeveelheid aan transacties in Nederland. Het is niet mogelijk om elke transactie «handmatig» te onderzoeken en zou bovendien leiden tot een verstorende werking op het betalingsverkeer.

Desalniettemin geven banken aan de ambitie te hebben om ook niet-bancaire fraude verder te kunnen detecteren en voorkomen en continue bezig zijn om hun processen en tools met het oog op het voorkomen van eventuele schade voor benadeelden te verbeteren.

Naast het genoemde fraudepreventie-activiteiten zetten banken nog andere middelen in om fraude te bestrijden. Zo kunnen banken rond hun internetbankier-omgevingen via de Account Monitored Information infrastructuur (AMI) waarschuwingen uit de fraudedetectiesystemen over bankrekeningnummers van frauduleuze begunstigden met elkaar delen. Daarnaast maken banken gebruik van het zogenaamde Externe Verwijzingsregister (EVR) door middel waarvan banken elkaar kunnen waarschuwen voor personen die een strafbaar feit hebben begaan of daartoe een poging hebben ondernomen. Het EVR werkt als een extra waarschuwingssysteem bij de acceptatie van nieuwe klanten.

Activiteiten van banken ten behoeve van fraudeslachtoffers

Voor wat betreft het «veilig stellen» of «terughalen» van gelden van fraudeslachtoffers (door banken genoemd: «recovery van gelden») hebben de banken aangegeven dat zij zoveel mogelijk doen om frauduleuze betalingen te detecteren en dat zij proberen de gelden veilig te stellen of gelden in samenwerking met andere banken terug te halen. Dit is overigens veel lastiger wanneer de andere bank zich buiten Nederland bevindt.

In geval van *bancaire* fraude, zoals malware en phishing, wordt de schade uit coulance grotendeels vergoed. Hierbij wordt door de banken, zoals ik

eerder benoemde, wel het volgen van de veiligheidsregels door de klant in de afweging meegenomen.
De recovery van gelden bij *niet-bancaire* fraude ligt volgens de banken complexer. In dat geval geeft immers de klant zelf opdracht tot betaling. Als de fraudedetectie geen aanleiding geeft tot twijfel moet de bank de verplichting nakomen om deze betaalopdracht uit te voeren. Overigens geven banken ook aan dat klanten in enkele gevallen juist boos reageren als blijkt dat banken transacties tijdelijk parkeren in verband met mogelijke fraude.
Banken kennen voor de situatie dat per vergissing geld wordt overgeboekt naar een niet-beoogd rekeningnummer een procedure onverschuldigde betaling. Deze procedure omvat een uniforme werkwijze die de bank van de betaler hanteert als een niet-beoogde begunstigde het geld dat hij ten onrechte heeft ontvangen, niet terugboekt en de betaler niet zelf in contact kan komen met de begunstigde. De bank van de betaler kan dan de begunstigde vragen het ten onrechte ontvangen geld terug te boeken[4]. Indien sprake is van fraude kan een bank, in tegenstelling tot bijvoorbeeld het storneren van incasso's, het geld niet zo maar terughalen, omdat ervaring leert dat juist bij fraude het bedrag snel wordt opgenomen of overgeboekt naar het buitenland.

Meer specifiek heeft uw Kamer tijdens genoemd AO gevaagd waarom banken geen NAW-gegevens (naam, adres, woonplaats) van de tegenrekening van de (vermoede) fraudeur kunnen verstrekken aan een slachtoffer, zodat dat slachtoffer zelf civielrechtelijke actie kan ondernemen. Banken geven aan dat dat vanwege de geldende privacywetgeving niet is toegestaan. Daarnaast is het niet automatisch zo dat degene op wiens naam een tegenrekening staat daadwerkelijk zelf de fraudeur is. Het komt voor dat deze veronderstelde begunstigde zelf slachtoffer is van fraude, bijvoorbeeld van identiteitsfraude. Dat maakt dat uiterst zorgvuldig met dit soort gegevens moet worden omgegaan.
Banken zullen een slachtoffer wel helpen met het doen van aangifte. De politie kan op basis van het wetboek van Strafvordering informatie, waaronder de NAW-gegevens, opvragen bij de banken. Met de komst van het verwijzingsportaal Bankgegevens per 2020 zal dit proces naar verwachting een aanzienlijke versnelling krijgen.

Banken werken bij de preventie van fraude en de zorg voor fraudeslachtoffers samen in een aantal publiek-private samenwerkingsverbanden, bijvoorbeeld de Electronic Crimes Task Force (banken, OM en politie) en het Landelijk Meldpunt Internetoplichting van de politie (banken, OM, politie en Marktplaats). In 2017 is vanuit Currence iDEAL een vergelijkbaar samenwerkingsverband tussen het LMIO en betaalinstellingen gestart. Zo worden nu ook niet-bancaire betaaldienstverleners gewaarschuwd voor malafide webshops als er drie of meer meldingen bij de politie zijn gedaan.

Conclusie naar aanleiding van mijn gesprekken met de banken

Zoals ik ook in mijn brief aan uw Kamer van 13 juni 2018[5] en tijdens het genoemde AO aangaf is in ons betalingsstelsel een betaling aan een begunstigde een onherroepelijke betaling, die de begunstigde zekerheid verschaft. Banken moeten er bij een overboeking in opdracht van een rekeninghouder voor zorgen dat opdrachten conform de door die rekeninghouder ingevoerde gegevens verwerkt worden. Dat beperkt de

[4] https://www.betaalvereniging.nl/betaalproducten-en-diensten/europese-overschrijving/procedure-onverschuldigde-betalingen/.
[5] Kamerstuk 34 615, nr. 12.

mogelijkheden van banken om in te grijpen bij met name *niet-bancaire* fraude, zoals internetoplichting.
Dat neemt niet weg dat ik van banken verwacht dat zij zich verantwoordelijk tonen voor het voorkomen van het gebruik/misbruik van hun infrastructuur door fraudeurs en zich proactief (blijven) inspannen om bancaire en zeker ook niet-bancaire fraude te voorkomen en als het zich toch voordoet zich zoveel mogelijk in te spannen voor slachtoffers. Ik zie dat banken hier met de vorengenoemde activiteiten invulling aan geven en stel tegelijkertijd vast dat zij de ambitie uitspreken om fraude, bancair en niet-bancair, (nog) beter te detecteren, te voorkomen en hun klanten te beschermen. Ook spreken zij de ambitie uit om de samenwerking met andere publiek en private partijen ter preventie van fraude verder te versterken, zoals bijvoorbeeld binnen de samenwerking met het Landelijk Meldpunt Internetoplichting van de politie (LMIO), dat men wil verbreden en effectiever wil maken. Ik onderschrijf die ambities, zal de banken hier nauwgezet bij blijven volgen en hen hierop blijven aanspreken.

2. Gesprek met OM en AFM over conservatoir beslag ten behoeve van de AFM

Tijdens het AO is door uw Kamer de vraag gesteld of onderzocht zou moeten worden of de Autoriteit Financiële Markten (AFM) zou moeten kunnen beschikken over een bestuurlijke bevoegdheid tot het leggen van conservatoir beslag. Ik heb uw Kamer toen aangegeven dat in ons rechtssysteem voor het leggen van conservatoir beslag een rechterlijke machtiging nodig is en dat het mij niet wenselijk lijkt als de AFM zonder een dergelijke toestemming beslag zou kunnen leggen. Indien er noodzaak is tot het leggen van conservatoir beslag, bijvoorbeeld in fraudezaken, kan de AFM in overleg treden met het Openbaar Ministerie (OM) en de FIOD.

De samenwerking tussen AFM, OM en FIOD is gebaseerd het Convenant ter voorkoming van ongeoorloofde samenloop van bestuurlijke en strafrechtelijke sancties[6]. Dit convenant bevat afspraken tussen het OM, de Minister van Financiën, de AFM, de Nederlandsche Bank en de Belastingdienst / FIOD-ECD over de informatieverstrekking tussen partijen, de afstemming over de wijze van afdoening van zaken en hoe hierover wordt overlegd.
Criteria die een rol spelen bij de afweging of bestuurlijk of strafrechtelijk moet worden opgetreden zijn o.a. de mate van impact op de maatschappij en een evenwichtige rechtshandhaving, de (maatschappelijke) status van de verdachte en een eventuele voorbeeldfunctie, recidive, of een bestuurlijke boete mogelijk is, of er sprake is van een combinatie van delicten (waaronder commune delicten), of er sprake is van medewerking van een facilitator, of er sprake is van een bepaalde thematische aanpak of wat er nodig is ten behoeve van waarheidsvinding.

Overleg tussen het OM, de AFM en Belastingdienst/FIOD vindt plaats binnen het zogenaamde tripartiete overleg, ook wel de weeg- en stuurploeg genoemd. In dit overleg worden door de AFM geconstateerde overtredingen besproken en wordt bepaald welke interventie door welke partij gepleegd moet worden gelet op de afspraken in genoemd convenant. Indien aan de orde wordt daarbij ook het eventueel leggen van conservatoir beslag besproken.
Naast dit tripartiete overleg spreken het OM, de AFM en de FIOD elkaar op maandelijkse basis in een laagdrempelig overleg, waarin signalen, casussen, ontwikkelingen en mogelijke interventies met elkaar worden verkend.

---

[6] Stcrt. 2009, nr. 665.

Ik heb met het OM en de AFM gesproken over het signaal van uw Kamer dat het Openbaar Ministerie mogelijk terughoudend zou zijn om conservatoir beslag te leggen op verzoek van de AFM.
Uit deze gesprekken is mij gebleken dat het OM de samenwerking met de AFM als goed bestempelt en hierin geen problemen ervaart. De AFM bevestigt dit. Beide gaven aan hun samenwerking juist te waarderen en dat men elkaar goed en tijdig weet te vinden. Ook als het gaat om zaken waarin conservatoir beslag moet worden gelegd om te voorkomen dat criminele gelden naar het buitenland verdwijnen. Het OM gaf aan dat conservatoir beslag – indien aan de orde – snel gelegd kan worden. De lijnen tussen AFM en OM en tussen het OM en de Rechter-Commissaris zijn kort, wat ook door de AFM wordt onderschreven.
Gelet op het vorenstaande ben ik van mening dat binnen het huidige rechtssysteem rond conservatoire beslaglegging de samenwerking tussen OM, AFM en FIOD adequaat is.

De Minister van Justitie en Veiligheid,
F.B.J. Grapperhaus