Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2013–2014

Aanhangsel van de Handelingen

Vragen gesteld door de leden der Kamer, met de daarop door de regering gegeven antwoorden

1073

Vragen van het lid **Nijboer** (PvdA) aan de Minister van Financiën over *storingen en fraude bij online bankieren* (ingezonden 24 januari 2014).

Antwoord van Minister **Dijsselbloem** (Financiën) (ontvangen 30 januari 2014).

Vraag 1
Bent u bekend met het artikel «Rabobank vaakst plat»?[1]

Antwoord 1
Ja

Vraag 2
Hoeveel storingen in het online betalingsverkeer (ook via mobiele apps) van de Nederlandse banken zijn bij u bekend sinds 1 januari 2013 en wat was de totale en gemiddelde storingsduur per bank in 2013? Hoe verhouden deze bij u bekende storingsgegevens zich tot de meldingen op de website www.allestoringen.nl?

Antwoord 2
Uit onderzoek, uitgevoerd in opdracht van het MOB, waar ik uw Kamer in november vorig jaar over heb geïnformeerd[2], blijkt dat banken qua internetbankieren in 2012 een beschikbaarheidspercentage van 99,6%[3] lieten zien. In de eerste helft van 2013 hebben zich verschillende storingen binnen het internetbankieren voorgedaan, grotendeels veroorzaakt door meerdere grootschalige DDoS-aanvallen bij verschillende banken. In reactie hierop hebben banken inmiddels verschillende maatregelen[4] genomen. Ondanks dat banken nog steeds geregeld te maken hebben met DDoS-aanvallen, zijn er als gevolg hiervan sindsdien geen of nauwelijks langdurige verstoringen meer geweest.

---

[1] De Telegraaf. «Rabobank vaakst plat». 14 januari 2014 (p.23)
[2] Kamerstukken II, 2013–2014, 27 863, nr. 52
[3] Dit cijfer is een gewogen gemiddelde van de opgave van de vier grootste banken, gebaseerd op door hen zelf gehanteerde definities, en moet dus met enige voorzichtigheid gehanteerd worden.
[4] Belangrijke maatregelen zijn het vergroten van de capaciteit in het verwerken van dataverkeer in combinatie met het plaatsen van filters, die ongewenst, massaal data-aanbod afkomstig van de DDoS-aanval scheiden van het bonafide dataverkeer, waardoor de webservers niet «verstopt» raken.

ah-tk-20132014-1073
ISSN 0921 - 7398
's-Gravenhage 2014

Het is mij niet bekend hoe www.allestoringen.nl het aantal storingen en de storingsduur per bank meet.

Vraag 3
Hoe verhoudt het aantal storingen in het Nederlandse online betalingsverkeer zich tot het gemiddelde aantal storingen in het buitenland (o.a. Verenigd Koninkrijk, België en Duitsland)? Presteren Nederlandse banken beter of slechter?

Antwoord 3
Ik beschik niet over cijfers van het gemiddelde aantal storingen in het online betalingsverkeer in onze buurlanden. Daarbij merk ik op dat niet in alle andere EU-landen al in dezelfde grote mate gebruik gemaakt wordt van online betaalfaciliteiten als in Nederland. Binnen verschillende lidstaten hebben zich zeer diverse betaalmarkten ontwikkeld. Zo wordt in een aantal zuidelijk en oostelijk gelegen EU-lidstaten nog maar zeer beperkt gebruik gemaakt van elektronische betaalmogelijkheden. In een aantal andere lidstaten wordt wel veel elektronisch betaald, maar gebruikt men vaker een creditcard dan een debitcard (pinpas), zeker voor betalingen op internet. Een dienst als het Nederlandse iDEAL is in Europees opzicht uniek. In weinig lidstaten bestaat zo'n betaalmogelijkheid en waar dit wel het geval is, is het gebruik daarvan nog zeer beperkt. De grote verschillen in het gebruik van online betalingsverkeer maken vergelijkingen tussen diverse EU-lidstaten weinig zinvol.

Vraag 4
Onder welke omstandigheden zijn banken verplicht een storing bij de financiële toezichthouder te melden? Zijn er normen afgesproken voor het beschikbaarheidspercentage van het girale betalingsverkeer?

Antwoord 4
DNB houdt toezicht op onder meer de bedrijfsvoering van individuele financiële ondernemingen aan wie een vergunning is verstrekt. Daar past ook het toezicht op een goed betaalsysteem bij. In dat kader en vanuit de oversight-rol van DNB onderhoudt DNB nauw contact met banken mochten er (grote) verstoringen in het betalingsverkeer plaatsvinden. Banken melden ernstige storingen aan DNB. Van een ernstige storing is sprake als deze de bedrijfsvoering van de betreffende bank ernstig hindert, een grote impact kan hebben op de solvabiliteit en liquiditeit van de instelling, lang duurt of een andere instelling kan raken.
Daarnaast wordt er gewerkt aan een aantal Nederlandse en Europese wetgevingsinitiatieven[5] die het (verplicht) melden van storingen, die direct of indirect leiden tot maatschappelijke ontwrichting, in meer detail zullen regelen.
Er zijn geen absolute normen vastgesteld voor het beschikbaarheidspercentage van het girale betalingsverkeer. Zowel de banken zelf, als ook toezichthouder DNB en alle overige stakeholders die participeren in het MOB, hebben belang bij een goed werkend elektronisch betalingsverkeer. Door DNB wordt dit gemonitord zowel in het kader van het reguliere toezicht als vanuit de oversight-taak van DNB.

Vraag 5
Hoeveel schadegevallen door fraude bij online bankieren waren er over de jaren 2011–2013, welk percentage van deze gevallen kreeg enige vorm van compensatie aangeboden en welk percentage van deze zaken loopt nog?

[5] Een wetsvoorstel om security breaches te melden is in procedure en de voorgestelde EU Cyber Security Directive (Proposal for a Directive of the European Parliament and of the Council concerning measures to ensure a high common level of network and information security across the Union)

Antwoord 5
Uit cijfers van de Nederlandse Vereniging van Banken (NVB) maak ik op dat de schade als gevolg van fraude met internetbankieren in de eerste helft van 2013 4,2 miljoen euro bedraagt. Over heel 2012 bedroeg de fraude met internetbankieren 34,8 miljoen euro; in 2011 was dit 35 miljoen euro.
Van de NVB heb ik begrepen dat er in 2011 ongeveer 7.600 schadegevallen bij de banken bekend waren als gevolg van fraude met internetbankieren. In 2012 waren dit er ca. 11.000 en in het eerste halfjaar van 2013 ca. 2.000. Ik beschik niet over het percentage van fraudegevallen waarbij de bank de schade heeft gecompenseerd en een percentage van welke zaken nog lopen. Een overeenkomst tot compensatie is doorgaans vertrouwelijk, de inhoud ervan is dan alleen bij betrokken partijen bekend.

Vraag 6
Kunt u een uitsplitsing geven naar de aard van de fraude bij online bankieren; hoeveel gevallen zijn er jaarlijks en wat is het aandeel van fraude door phishing of malware binnen het totaal van het aantal online fraudegevallen?

Antwoord 6
Van de NVB heb ik begrepen dat de focus van internetfraudeurs de laatste jaren is verschoven van het «hengelen» naar vertrouwelijke gegevens (phishing), naar de ontwikkeling van malware waarbij criminelen speciale software schrijven om computers te infiltreren.
Volgens de NVB zouden van de ongeveer 11.000 schadegevallen in 2012 vanwege fraude met internetbankieren er ongeveer 2.000 te wijten zijn aan phishing en ongeveer 9.000 aan malware. Van de ongeveer 2.000 schadegevallen in de eerste helft van 2013 zijn er volgens de NVB bij benadering 500 te wijten aan phishing, 1.300 aan malware, 200 aan overige fraudevormen zoals fraude met machtigingen.

Vraag 7
Hoe staat het met de uitvoering van de aangenomen motie Nijboer c.s.[6] die de regering verzoekt helderheid te verschaffen over de normen die de Nederlandsche Bank (DNB) hanteert voor het vereiste veiligheidsniveau en de beschikbaarheid van het (online) betalingsverkeer, inclusief pinbetalingen in Nederland, deze te beoordelen op volledigheid en effectiviteit?

Antwoord 7
Zoals hiervoor aangegeven wordt er niet een bepaalde beschikbaarheidsnorm gehanteerd door toezichthouder DNB. Wel vormt het functioneren van het elektronisch betalingsverkeer een continue aandachtspunt, zowel in het reguliere toezicht als vanuit de oversight-taak van DNB. Daarbij neemt DNB mee, zoals hierna ook toegelicht in het antwoord op vraag 8, of banken en andere schakels in de betaalketen voldoen aan de aanbevelingen die vanuit de ECB worden gedaan.
In de rapportage «Analyse van de robuustheid van het elektronisch betalingsverkeer» is onderzocht hoe diverse stakeholders het elektronisch betalingsverkeer in Nederland beoordelen. Uit deze rapportage blijkt dat de diverse stakeholders over het algemeen tevreden zijn over de robuustheid van het elektronisch betalingsverkeer in Nederland. Wel zijn er in deze rapportage drie verbeterpunten gesignaleerd die te maken hebben met de betaalkanalen iDeal, internetbankieren en pinnen en het tegengaan van Ddos-aanvallen. Deze verbeterpunten zijn of worden opgepakt door alle betrokken stakeholders, zo heb ik begrepen. Banken zijn bezig om de ICT-systemen voor iDeal en internetbankieren minder afhankelijk van elkaar te maken, zodat een storing in het ene systeem niet direct consequenties hoeft te hebben voor het andere systeem. Van de NVB en Detailhandel Nederland heb ik begrepen dat een verdere verbetering van de robuustheid van de pinketen onderwerp is van het Convenant Betalingsverkeer.

[6] Kamerstuk 27 863, nr. 46

Vraag 8
Zijn de Nederlandse banken compliant met de ECB-aanbevelingen[7] voor de beveiliging van internetbetalingen in het bijzonder ten aanzien van de klantidentificatie en risicoanalyse, de monitoring van betaaltransacties en het zetten van betaallimieten? Hoe wordt gevolg gegeven aan de aanbevelingen van de ECB en evalueert DNB de voortgang van Nederlandse banken?

Antwoord 8
De Recommendations waaraan gerefereerd wordt, zijn begin 2013 door de ECB gepubliceerd. De ECB geeft de banken tot 1 februari 2015 de tijd om aan deze set van aanbevelingen te voldoen. Dit op basis van het «*comply or explain*» principe. Dit betekent dat banken elke aanbeveling op te dienen volgen, tenzij op basis van degelijke risico-overwegingen afwijkingen hierop uitgelegd kunnen worden. DNB heeft aangegeven dat de Recommendations worden meegenomen in het reguliere toezicht.
De banken en DNB schatten in dat er bij de Nederlandse banken geen grote wijzigingen in procedures en IT-systemen nodig zijn om tijdig aan de aanbevelingen te voldoen. Zo passen de Nederlandse banken al sinds jaar en dag «*strong authentication*» (één van de ECB Recommendations) voor klantidentificatie toe bij internetbankieren. Voor klantidentificatie bij mobielbankieren gebruiken de meeste banken «*static*» in plaats van «*strong authentication*». Dergelijke afwegingen kunnen banken goed uitleggen, en zijn altijd gebaseerd op zorgvuldig uitgevoerde risicoanalyses. De meeste banken bieden klanten de mogelijkheid om via internetbankieren limieten in te stellen voor de bedragen die via internet- en/of mobielbankieren kunnen worden overgemaakt.

Vraag 9
Welke maatregelen nemen banken nu reeds om de maximale schade per klant te beperken en wordt de klant ook expliciet een keuze gegeven voor meer of minder functionaliteit?

Antwoord 9
Het veilig inrichten en veilig houden van internetbankieren is voor banken uiteraard van groot belang, ook om het vertrouwen van klanten te behouden. Via geavanceerde 24/7 fraudedetectie en transactiemonitoring herkennen banken fraude steeds beter en sneller. Verder werken banken intensief samen met het Openbaar Ministerie en de politie in het Electronic Crimes Task Force (ECTF) om internetcriminelen aan te pakken.
Banken hebben verder een divers scala aan maatregelen ingevoerd om de klant zelf meer regie te geven om, mocht hij/zij slachtoffer worden van fraude via internetbankieren, de maximale schade te verkleinen. Een dergelijke maatregel is bijvoorbeeld «*geoblocking*» voor internetbankieren, waarbij overboekingen via internetbankieren naar landen buiten Europa standaard geblokkeerd worden. Klanten kunnen dit zelf aanpassen via internetbankieren en zowel tijdelijk als permanent buitenlandoverboekingen «aan» zetten. Een ander voorbeeld is het zelf via internetbankieren kunnen instellen van limieten voor bedragen die via internet- en/of mobielbankieren kunnen worden overgemaakt. Daarnaast zijn er banken waarbij klanten via mobielbankieren enkel naar rekeningnummers geld kunnen overmaken waar zij reeds eerder geld naar hebben overgemaakt.

Vraag 10
Indien banken de nieuwe uniforme veiligheidsvoorwaarden opnemen in hun algemene voorwaarden is dan gelet op artikel 7:524 lid 1 sub a van het Burgerlijk Wetboek[8] geen sprake van een verschuiving van verplichtingen richting de consument (de uniforme veiligheidsvoorwaarden kleuren dan via de algemene voorwaarden immers de standaard in waarlangs een rechter de «grove nalatigheid» van een consument zal toetsen)?

---

[7] European Central Bank. «Recommendations for the security of internet payments». Januari 2013. Frankfurt.

[8] Dit artikel bepaalt: [de betaaldienstgebruiker] «gebruikt het betaalinstrument overeenkomstig de voorwaarden die op de uitgifte en het gebruik van het betaalinstrument van toepassing zijn (...)».

Antwoord 10
De uniforme veiligheidsregels zijn op zichzelf niet nieuw, zij waren alleen niet bij elke bank identiek. De onderlinge verschillen tussen banken zijn geschrapt, zodat voor iedereen dezelfde regels gelden. Ook zijn verouderde regels geschrapt, zoals het verbod te internetbankieren en/of mobielbankieren via onbeveiligde draadloze netwerken. De regels komen op mij niet onredelijk over. Dit gevoel wordt nog gesterkt door de wetenschap dat de uniforme veiligheidsregels tot stand zijn gekomen in nauw overleg met de Consumentenbond. Van de NVB en de Consumentenbond heb ik begrepen dat de uniforme veiligheidsregels over enige tijd ook geëvalueerd zullen worden. Daarnaast wordt regelmatig de suggestie gewekt dat de consument bij het niet naleven van de uniforme veiligheidsregels per definitie «grof nalatig» zou zijn, waarbij hij of zij aansprakelijk zou zijn voor de volledige schade. Dit zou echter niet in lijn zijn met het Nederlandse aansprakelijkheidsrecht. Van de NVB heb ik begrepen dat banken zich er goed van bewust zijn dat een gemiddelde consument zich niet 100% tegen internetcriminelen kan beveiligen. Het niet naleven van een beperkt onderdeel van de uniforme regels betekent daarom niet per definitie dat de consument aansprakelijk wordt gesteld voor de schade, zo benadrukt de NVB. Of sprake is van grove nalatigheid in een individueel geval, kan alleen door de rechter worden vastgesteld.

Vraag 11
Hoe verhoudt de verdeling van de bewijslast in artikel 7:529 Burgerlijk Wetboek, waarbij de bewijslast op de bank drukt, zich tot de situatie waarin de klant moet aantonen dat hij zich aan de nieuwe uniforme veiligheidsregels heeft gehouden? Wordt de klant nu niet gevraagd zijn eigen onschuld aan te tonen in plaats van dat de bank de grove nalatigheid dan wel opzet aan de kant van de klant moet aantonen?

Antwoord 11
Eerder heb ik uw Kamer toegelicht[9] dat ik het een wenselijk ontwikkeling vind dat banken samen met de Consumentenbond eenduidige, uniforme regels overeen zijn gekomen. Mede op mijn aandringen is in het MOB onderzocht in welke mate de verschillende veiligheidsnormen, waaraan de klant zich bij internet- (en mobiel-) bankieren dient te houden, qua inhoud en formulering beter op elkaar konden worden afgestemd. Als consumenten schade lijden, maar deze de uniforme veiligheidsregels hebben nageleefd, dan kunnen zij er in ieder geval op rekenen dat zij het bedrag dat zonder toestemming van de rekening is gehaald, vergoed krijgen.
Uit de artikelen 7:524, 7:528 en 7:529 BW volgt dat in beginsel de bank verplicht is om de geleden schade te vergoeden. Alleen wanneer sprake is van opzet of grove schuld aan de zijde van de klant kan dit anders zijn (artikel 7:529, tweede lid, BW). Onderlinge afspraken tussen de Consumentenbond en de NVB zijn niet van invloed op deze wettelijke bewijslastverdeling. De rechter heeft het laatste woord over de uitleg van de wet- en regelgeving. Als de bank het standpunt van de consument – volgens deze ten onrechte – afwijst, kan de consument het geschil voorleggen aan Kifid (Klachtinstituut Financiële Dienstverlening) of de rechter.

Vraag 12
Er is een aantal gevallen bekend waarbij klanten op verzoek van de bank eerlijk vertelden op welke wijze zij zijn bedonderd door internetcriminelen en zij door de vertelde feiten aan de bank de schade niet vergoed kregen, terwijl als zij niets zouden hebben gezegd de schade wel vergoed zou worden; deelt u de mening dat dit niet zou moeten gebeuren? Bent u bereid dit in gesprek met de Nederlandse Vereniging van Banken (NVB) aan de orde te stellen en banken te bewegen de schade voor deze gedupeerden alsnog te vergoeden?

[9] Beantwoording schriftelijke Kamervragen van het lid Nijboer (PvdA) aan de Minister van Financiën over de uniforme veiligheidsregels voor online bankieren, 8 januari 2014, FM/2013/2223

Antwoord 12
Op Europees niveau is besloten om, indien een klant opzettelijk heeft gefraudeerd of grof nalatig is geweest, de schade die daaruit ontstaan is door de klant zelf te laten dragen. Deze regel is in lijn met het Nederlandse aansprakelijkheidsrecht. komt mij niet onredelijk voor. Ook van een klant mag worden verwacht dat hij op een verantwoordelijke manier online zijn bankzaken regelt.
Of in een concrete situatie sprake is van grove nalatigheid of grove schuld aan de zijde van de gedupeerde, is niet aan mij om te bepalen maar aan de rechter. Indien sprake is van grove schuld aan de zijde van de gedupeerde zijn banken niet wettelijk verplicht om de schade van een gedupeerde te vergoeden. Vergoedt een bank desalniettemin (een deel van) de schade uit coulance, dan is dit een eigen en vrijwillige keuze van die bank.

Vraag 13
Kunt u een overzicht geven van het aantal rechtszaken dat loopt van gedupeerden van online fraude tegen banken? In hoeveel gevallen is al een uitspraak gedaan en hoe luidde deze?

Antwoord 13
Ik kan u niet voorzien van een overzicht van het aantal rechtszaken dat loopt rond online fraude, noch van het aantal gevallen waarin een uitspraak is gedaan. Van de NVB heb ik begrepen dat een inventarisatieronde langs de grootbanken leert dat het aantal lopende en afgeronde rechtszaken rond dit onderwerp zeer beperkt is.

Vraag 14
Uit onderzoek van de Universiteiten van Amsterdam en Leiden zou blijken dat slachtoffers van identiteitsfraude met een lage opleiding minder vaak geld terugkrijgen van de bank dan hoger opgeleiden; zijn deze gegevens juist?[10] Zo ja, wat zijn hiervan de oorzaken? Deelt u de mening dat het zeer onwenselijk is als het vergoeden van schade impliciet of expliciet afhankelijk is van de opleiding van mensen? Wat wilt u eraan doen om dit te voorkomen?

Antwoord 14
Het genoemde onderzoek[11] kijkt naar de opgetreden financiële schade van personen die te maken hebben gekregen met in hun ogen onterechte bankafschrijvingen. Het onderzoek laat hierbij in het midden wat de exacte oorzaken hiervan zijn. Deze kunnen variëren van fraude via internetbankieren door *phishing* of *malware*tot marktplaatsfraude, geschillen met (web)winkeliers, *family fraud*, babbeltrucs, diefstal/ verwisseling van betaalpassen waarbij pincode zijn afgekeken en zelfs – onterecht geachte – overheidsvorderingen.
Het is op basis van het aangehaalde onderzoek voor mij niet mogelijk om uitspraken te doen over de vraag of lager opgeleide mensen inderdaad minder snel hun schade vergoed krijgen dan hoger opgeleide mensen. Voor alle situaties geldt, dat bij een onterechte afschrijving, de bank in beginsel gehouden is de schade te vergoeden, tenzij sprake is van opzet of grove schuld.

Vraag 15
Bent u bereid deze vragen te beantwoorden voor het Algemeen overleg Betalingsverkeer op 30 januari 2014?

Antwoord 15
Ja

[10] «Laagopgeleide geld vaker kwijt», De Persdienst 17 januari 2014
[11] Tijdschrift voor Criminologie 2013(55) 4, p. 360–374.