Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2014–2015

34 033 Initiatiefnota van het lid Nijboer over veilig en betrouwbaar bankieren in de 21e eeuw

Nr. 2

INITIATIEFNOTA

1. Voorstellen

1.1. Beslispunten:

Veilig online bankieren

1) *Bij fraude, phishing en malware blijven banken verantwoordelijk voor vergoeding van schade. De verantwoordelijkheid wordt niet verschoven naar de consument.*
2) *ZZP-ers en het midden-en kleinbedrijf verdienen dezelfde bescherming tegen online criminelen als consumenten. Ook hun geld moet altijd veilig zijn.*
3) *De bewijslast moet worden omgedraaid: de consument hoeft niet te bewijzen dat hij of zij niet met grove opzet of nalatig handelde. Als een bank denkt dat sprake is van grove opzet of nalatigheid, moet de bank dat bewijzen. Bovendien moet schade binnen een maand worden vergoed.*
4) *In de wet staat dat bij schade consumenten een eigen risico hebben van 150 euro. In de praktijk is dit een dode letter. Ik stel voor dit eigen risico uit de wet te schrappen.*

Beschikbaarheid

5) *Er moet een storings- en beschikbaarheidsnorm komen voor online bankieren. Deze moet gehandhaafd worden door De Nederlandsche Bank.*
6) *Transacties moeten door banken veel sneller worden afgewikkeld. Nu is dat alleen op werkdagen tijdens kantooruren. Ook 's avonds en in het weekend bijschrijven biedt rente en liquiditeit voor consumenten en ondernemers.*

kst-34033-2
ISSN 0921 - 7371
's-Gravenhage 2014

7) *Banken beschikken over veel informatie. Deze hebben zij verkregen vanuit hun nutsfunctie. Deze informatie mag niet worden verkocht of voor commerciële doeleinden worden gebruikt.*
8) *Data zijn van klanten, niet van banken. Consumenten moeten hun bankrekeninggegevens makkelijk kunnen gebruiken voor online rekentools.*
9) *Afschrijvingen zijn veelal niet voorzien van duidelijke informatie. Banken moeten er in samenwerking met bedrijven zorg voor dragen dat je op je afschrift kunt zien wie de ontvanger is. Dan zijn afschriften ook beter te controleren.*

De Tweede Kamer vraagt het kabinet in te gaan op de beslispunten en bijbehorende nota.

1.2. Financiële consequenties:

Er zijn geen financiële consequenties voorzien van de beslispunten en de bijbehorende nota.

2. Inleiding

2.1. Het betalingsverkeer behoort tot de essentiële infrastructuur, net als het energienetwerk en onze dijken. De vorm van geld en de wijze van betalen is constant in ontwikkeling. Was geld in het verleden nog inwisselbaar voor goud, tegenwoordig is de waarde ervan gebaseerd op de waarde die de samenleving er aan toekent. De relatie tussen muntstuk en werkelijke waarde is al lang geleden losgelaten, de volgende stap is dat een steeds groter deel van het betalingsverkeer online en digitaal plaatsvindt. Dat is een goede zaak. Door innovaties wordt ons betalingsverkeer goedkoper, efficiënter en veiliger. Denk maar aan overvallen in het verleden en ramkraken tegenwoordig die leiden tot veel schade en slachtoffers. De modernisering stopt niet: proeven met mobiel en contactloos betalen zijn inmiddels gestart, waarbij een simpele beweging met een smartphone of contactloze pas voor betaling volstaat. Als gevolg van deze overgang naar het digitale betalingsverkeer gaat bijna een derde van de Nederlanders inmiddels regelmatig zonder contant geld op pad.[1]

2.2. Deze ontwikkelingen hebben echter ook keerzijden. Technologische vooruitgang brengt nieuwe kwetsbaarheden met zich mee, zoals een consument die te maken krijgt met phishing of een ondernemer die de dupe wordt van storingen in het betalingsverkeer. De DDoS-aanvallen op de systemen van banken in 2013 leidden tot de nodige onrust en maakten die kwetsbaarheid goed zichtbaar.[2]

2.3. Geld draait om vertrouwen. Geld moet veilig en beschikbaar zijn. En dan is het belangrijk dat wetgeving, beveiliging en toezicht voldoen aan de eisen van deze tijd. Ook dient de samenleving voorbereid te zijn op nieuwe ontwikkelingen en innovaties in het betalingsverkeer. Dat is momenteel helaas niet altijd het geval. In het bijzonder het belang van de consument verdient daarbij aandacht. Voor mij staat voorop dat iedere burger, jong en oud, met vertrouwen moet kunnen deelnemen aan het betalingsverkeer. De beschikbaarheid, de veiligheid en privacy staan daarbij centraal.

2.4. In deze nota zal een aanzet gegeven worden tot een discussie die zal moeten leiden tot versterkt vertrouwen in het systeem en verbeterde toekomstbestendigheid van het betalingsverkeer. Voornoemde drie

[1] Betaalvereniging Nederland, okt. 2012
[2] http://www.nvb.nl/nieuws/2013/1828/ddos-aanval-websites-banken.html

centrale punten zullen in respectievelijke volgorde behandeld worden.

3. Beschikbaarheid

3.1. De beschikbaarheid van het elektronisch betalingsverkeer wordt gemonitord door drie organisaties. Het toezicht op het betalingsverkeer ligt bij De Nederlandsche Bank (DNB). Daarnaast is er regulier overleg over het betalingsverkeer binnen het Maatschappelijk Overleg Betalingsverkeer (MOB). In het MOB is een brede groep belanghebbenden vertegenwoordigd, waaronder banken, consumenten en winkeliers. Naast DNB en het MOB is het Nationaal Cyber Security Centrum door belanghebbenden in het leven geroepen ter bestrijding van internetcriminaliteit en aanvallen op het systeem via digitale weg.

3.2. Een betrouwbaar elektronisch betalingsverkeer is essentieel voor onze economie, en wint nog steeds aan belang. Uit cijfers van het MOB blijkt dat in 2013 het aantal pintransacties met 7,5% is gestegen. Nog maar 1/3 van de totale uitgaven aan de toonbank worden contant voldaan.[3] Het aantal geldautomaten en bankkantoren neemt al jaren af. Elektronisch betalen, waaronder PIN, creditcard, maar ook innovatievere oplossingen zoals betalen met de mobiele telefoon, zijn goedkoper, efficiënter en daarnaast veel veiliger.

3.3. Ondanks de grote voordelen van elektronisch betalingsverkeer, zijn er ook risico's verbonden aan deze nieuwe technologieën. De systemen die aan het elektronisch betalingsverkeer ten grondslag liggen worden steeds complexer, en er zijn verschillende partijen betrokken bij een transactie. Deze keten is zo sterk als zijn zwakste schakel, als het systeem bij één van deze partijen niet functioneert komt er geen transactie tot stand. Zo zijn bij een PIN-transactie drie belangrijke schakels te identificeren: 1) banknetwerken en processoren, 2) de openbare datacominfrastructuur en 3) de winkelomgeving.

3.4. Het systeem functioneert behoorlijk goed onder de huidige omstandigheden. Het MOB heeft onderzoek gedaan naar de beschikbaarheid van de verschillende schakels.[4] Het functioneren van het online betaalsysteem in Nederland komt aardig in de buurt van een beschikbaarheid van 100%. In de bank- en processoromgeving is de beschikbaarheid het hoogst, rond de 99,99%. In het segment van datacominfrastructuur is de beschikbaarheid iets lager, namelijk 99,80%. Om ondernemers duidelijkheid te verschaffen over deze kwaliteit, publiceert Betaalvereniging Nederland op haar website sinds eind 2012 beschikbaarheidscijfers van verschillende datacomdiensten. Die variëren van 99,60% tot 99,95%.

3.5. De impact van voorkomende storingen is echter groot. De grootschalige DDoS-aanvallen op Nederlandse banken in 2013 legden de onderliggende kwetsbaarheid treffend bloot. Internetbankieren en Ideal waren dagdelen lang niet bereikbaar. Meer recent in juli 2014 kampte de Rabobank met grote storingen na updates van de computersystemen.[5] De systemen zijn inmiddels dermate complex dat een oplossing niet snel gevonden was. Niet alleen zorgde dit voor ongemak en economische schade, ook leidde het tot twijfel over de robuustheid van het systeem. Voor sommigen voelt het alsof er ieder moment zich een fatale fout kan voordoen waarbij de bank niet meer kan terugvinden wie hoeveel geld bij de bank heeft gestald.

---

[3] Rapportage MOB 2013

[4] Analyse robuustheid van het elektronisch betalingsverkeer

[5] http://www.telegraaf.nl/overgeld/consument/22891941/__Ook_vandaag_weer_storing_Rabobank_internetbankieren__.html

3.6. Er zijn alternatieven voor het elektronisch betaalverkeer. In geval van storing bij een of meer banken kan worden teruggevallen op bijvoorbeeld chartaal geld, creditcards en zo meer. Deze alternatieven hebben zo hun nadelen. Chartaal geld is duurder, steeds meer winkels accepteren slechts PIN en bovendien functioneren geldautomaten niet altijd tijdens een storing. Het gebruik van een creditcard dwingt consumenten om een, weliswaar kortlopende, schuld aan te gaan waarvan de rente bij verlate terugbetaling stevig in de papieren kan lopen.

3.7. Het moderne betalingsverkeer is inmiddels onderdeel van onze essentiële infrastructuur, vergelijkbaar met bijvoorbeeld het elektriciteitsnetwerk. Waar het elektriciteitsnetwerk onderworpen is aan een norm voor de betrouwbaarheid van de levering van energie bestaat er nog geen vergelijkbare norm voor het elektronisch betaalverkeer. Ik heb bij motie[6] de Minister gevraagd helderheid te verschaffen over een norm voor het vereiste veiligheidsniveau en beschikbaarheid van het online betalingsverkeer. Tot op heden is hier geen concreet voorstel toe gedaan. Wel heeft de Minister in de Wijzigingswet Financiële Markten 2015[7] voorgesteld een delegatiebepaling op te nemen. Wat mij betreft zou een dergelijke norm kunnen bestaan uit vereisten ten aanzien van de bereikbaarheid, beschikbaarheid en communicatie. Hierbij kan onderscheid gemaakt worden tussen de verschillende vormen van elektronisch en online betalingsverkeer.

3.8. Ik vind dat er naast betrouwbaarheid ook aandacht moet zijn voor een snelle afwikkeling van transacties. Een modern betalingssysteem dient immers een katalysator te zijn voor de economie, geen beperkende factor. Waar mensen inmiddels ook 's avonds en in de weekenden hun facturen overmaken en online bankieren, vinden transacties tussen banken slechts plaats op werkdagen en binnen kantooruren. Soms duurt het dagen voordat geld is overgeschreven en wordt rente gemist. Voor ondernemers geldt dat zij niet bij hun geld kunnen en dan niet over liquiditeit kunnen beschikken. Dit is niet meer van deze tijd. De PvdA-fractie heeft hierover Kamervragen gesteld.[8] Het onderliggende Target2-systeem is een Europees project dat de Nederlandse partijen niet eenzijdig kunnen aanpassen. In antwoord op de Kamervragen gaf de Minister echter aan dat er wellicht mogelijkheden bestaan om nationaal tot een snellere verwerking van transacties te komen. DNB, het MOB en de banken zijn een onderzoek gestart en komen naar verwachting in november 2014 met een voorstel om tot snellere betaaltransacties buiten kantooruren te komen, primair met betrekking tot PIN, Ideal en elektronische overschrijvingen. Met de PvdA kijk ik uit naar de uitkomsten van het onderzoek, en roep ik met de PvdA partijen op ook op Europees niveau te zoeken naar verbeteringen, zodat consumenten en bedrijven in de nabije toekomst 24 uur per dag, 7 dagen per week gebruik kunnen maken van elektronisch bankieren.

4. Veiligheid

4.1. Geld is gebaseerd op vertrouwen. Geld moet derhalve veilig zijn. De nieuwste innovaties op betalingsgebied bieden naast efficiëntie en gemak helaas ook veel uitdagingen op het gebied van veiligheid. Op gewiekste wijze ontfutselen criminelen mensen geld door middel van skimming, phishing of malware. En waar een antwoord lijkt gevonden te worden op de ene vorm, duikt er weer een nieuwe vorm op. 100% veiligheid is dan ook een illusie. Omdat ons betalingsverkeer

---

[6] Motie van het lid Nijboer c.s., Kamerstuk 27 863, nr. 48 (3 juli 2013)
[7] Kamerstukken 2013–2014, nr. 33 918 / art. 3:17, lid 2 Wft
[8] Kamervragen 15 april 2014, nr. 1870

een cruciaal onderdeel van onze economie is moeten we er alles aan doen om het zo veilig mogelijk te maken.

4.2. Er gebeurt al veel op het gebied van veiligheid, zoals de samenwerking tussen banken, het OM en de politie in het Electronic Crimes Task Force om internetcriminelen aan te pakken, maar ook uitgebreidere voorlichting door banken. De cijfers laten over 2013 gelukkig een aanzienlijke daling (72%) zien van de schade door fraude met internetbankieren tot EUR 9,6 miljoen. Ook de schade door skimming daalde in 2013 fors (76%) tot EUR 6,8 miljoen. De totale fraude in het betalingsverkeer in 2013 bedroeg EUR 33 miljoen.[9] Het MOB concludeert dat cybercriminelen, ondanks de dalingen bij skimming en internetbankieren, een grote bedreiging zullen blijven vormen.[10] En waar vroeger in een gestolen portemonnee misschien honderd gulden zat, kan nu je gehele bankrekening worden geplunderd. De risico's zijn dus fors opgelopen: van een overzichtelijk bedrag naar je gehele spaarrekening. Deze vormt het pensioen, het bedrag dat is gespaard voor kinderen die ervan kunnen studeren of de middelen die de ZZP-er nodig heeft om zijn facturen te voldoen. Mensen moeten erop kunnen vertrouwen dat het geld dat op de bank staat te allen tijde veilig is.

4.3. Het betalingsverkeer heeft een nutsfunctie, daarom is het erg belangrijk dat consumenten en ondernemers met vertrouwen kunnen deelnemen en zich beschermd weten tegen criminelen. Op het gebied van online fraude dient de positie van deelnemers aan het betalingsverkeer te worden verbeterd. Uit de artikelen 7:524, 7:528 en 7:529 BW volgt dat in beginsel de bank verplicht is om de geleden schade aan consumenten te vergoeden. Dat is alleen dan niet het geval wanneer de klant frauduleus heeft gehandeld of opzettelijk of met grove nalatigheid een of meerdere verplichtingen uit de voorwaarden van artikel 7:524 BW niet nakomt (artikel 7:529, tweede lid, BW). Niettemin waren voorheen klanten bij online fraude in de praktijk afhankelijk van het beleid van de bank of zij gecompenseerd werden voor het geld dat van hen werd gestolen. De mate waarin dat werd gedaan verschilde tussen banken en zelfs tussen filialen van dezelfde bank. Dat geldt temeer voor ZZP-ers en het MKB, waarvoor deze wettelijke bescherming niet geldt. Ik vind dat zij eenzelfde beschermingsniveau moeten krijgen.

4.4. Er bestaat geen definitie voor het wettelijke begrip «grove nalatigheid». Of hier in een concreet geval sprake van is wordt nog altijd per geval bepaald. Zoals hierboven vermeld wordt een consument in ieder geval niet grof nalatig geacht als zij voldoet aan bepaalde regels zoals opgenomen in de algemene voorwaarden van de aanbieders. Deze regels verplichten consumenten onder andere minstens tweewekelijks hun rekeningoverzicht te controleren en om beveiligingssoftware up to date te houden. Indien één of meer regels niet zijn nageleefd kan de bank alsnog beslissen de consument te compenseren. Indien compensatie wordt afgewezen heeft de consument toegang tot geschillenbeslechting door het onafhankelijk klachteninstituut Kifid of de rechter.

4.5. Sinds januari 2014 zijn er uniforme veiligheidsregels voor elektronisch bankieren en betalen. Banken hebben met de consumentenbond uniforme regels opgesteld als het gaat om waar de consument zich aan moet houden, zodat deze in alle gevallen in aanmerking komt voor compensatie bij online fraude. Banken stellen dat indien een consument zich aan die regels houdt, deze altijd gecompenseerd wordt in geval van fraude. Dit is een verbetering ten opzichte van de situatie daarvoor, omdat er toen een wirwar aan algemene bepalin-

[9] http://www.nvb.nl/publicaties/108/jaarverslag.html

[10] Rapportage Maatschappelijk Overleg Betalingsverkeer 2013, pag. 24 e.v.

gen bestond. Niettemin is het niet zo dat als niet aan de voorwaarden wordt voldaan banken de schade niet zouden hoeven vergoeden.

4.6. De algemene voorwaarden van banken bestaan naast de wettelijke regels. De hoofdregel dat de bank de schade dient te vergoeden bij fraude blijft bestaan. De algemene voorwaarden kunnen slechts garanties aan consumenten geven in welke gevallen in ieder geval wordt vergoed. In de praktijk blijkt het Kifid echter sterk te leunen op de algemene voorwaarden en beperkt het zijn toetsingskader sterk tot het wel of niet hebben voldaan aan de regels zoals opgesteld door de banken zelf. Dit leidt tot ongewenste uitholling van de zware bewijslast die aan banken is toebedeeld. In de motie Nijboer-Merkies[11] werd het kabinet reeds opgeroepen er met de sector voor te zorgen dat de verantwoordelijkheid voor vergoeding van schade bij online fraude niet verder richting de consument wordt verschoven. Het niet controleren van je rekening of het net niet meer up-to-date hebben van je virusscanner kan geen reden zijn om in geval van schade deze niet te vergoeden. Uit de jurisprudentie van het Kifid blijkt dat hier nog veel valt te winnen. Ik wijs om die reden de Minister nogmaals op het bestaan van de motie Nijboer-Merkies en stel voor om het regelgevend kader aan te passen zodat de praktijk weer in lijn wordt gebracht met de bedoeling van de wet. Dit zou kunnen middels aanpassingen in het Burgerlijk Wetboek, maar ook in het kader van toezicht of zelfregulering. Ik vraag de Minister en de sector hiertoe met voorstellen te komen.

4.7. Voorts wordt in de huidige situatie pas tot compensatie overgegaan nadat vastgesteld is dat geen sprake is van fraude of grove nalatigheid door de klant. In voorkomende gevallen duurt dit erg lang. Een ondernemer die enkele maanden niet kan beschikken over een groot deel van zijn geld kan daardoor in grote problemen komen. Datzelfde geldt uiteraard voor consumenten. Ik stel voor dat de bank binnen een maand de consument/ondernemer schadeloos dient te stellen, tenzij er gerede twijfel is over de goede intenties van die klant (tegenbewijsregeling). De bewijslast hiertoe ligt wederom bij de bank. Dit is in lijn met de bedoeling van de wetgever, en geeft consumenten en ondernemers de gelegenheid sneller te herstellen van de schok die een dergelijke misdaad met zich brengt. Bovendien komen zo de machten van consumenten en banken meer in balans. Er zijn tal van individuele voorbeelden waarin schade niet door banken werd vergoed, terwijl nog geen enkele zaak bij de rechter is getoetst. De (financiële) armslag om een zaak tegen een bank aan te spannen is kennelijk te gering.

4.8. Tot slot is in de wet een eigen risico van EUR 150 voor de consument opgenomen in het geval van online fraude, ook in het geval er geen sprake is van fraude of grote nalatigheid door de consument. In de praktijk wordt dit eigen risico niet in rekening gebracht door banken. Ik vind een eigen risico onredelijk indien de consument niets te verwijten valt. Aangezien deze eigen risicobepaling in de praktijk toch al een dode letter blijkt te zijn, stel ik voor dit eigen risico te schrappen.

5. Privacy

5.1. Naast beschikbaarheid en veiligheid is privacy een belangrijk aandachtspunt in het moderne betalingsverkeer. Internetbankieren, mobiel betalen, het zijn innovaties die het de consument makkelijker maken en dus worden verwelkomd. Maar ze maken persoonlijke informatie over diezelfde consument ook makkelijker beschikbaar,

[11] Kamerstuk 27 863, nr. 47, zie tevens antwoorden van 8 januari 2014 op vragen van het lid Nijboer, 2013–2014, nr. 890

doorzoekbaar en verhandelbaar. De wereldwijde strijd om online klantgegevens gaat zeker niet voorbij aan het betalingsverkeer. Waar de balans tussen privacy en consumentengemak breder wordt gezocht, verdient die in de wereld van het betalingsverkeer ook zeker aandacht.

5.2. ING kondigde in maart van dit jaar een proef aan waarbij betaalgegevens van de klant zouden worden gebruikt voor commerciële doeleinden. Dit zorgde begrijpelijkerwijs voor veel ophef. Naar aanleiding van die ophef legde ING toen uit dat het analyseren en bundelen van die betaalgegevens alleen met toestemming van de klant zou gebeuren. Het voordeel zou bij de klant liggen omdat deze dan kon profiteren van aanbiedingen op maat. Bovendien zou ING zelf de gegevens analyseren en bewerken, derde partijen zouden hier geen toegang toe hebben.

5.3. De principiële vraag is of betaalgegevens überhaupt gebruikt mogen worden voor commerciële doeleinden. Banken weten waar, wanneer en aan wie men welk bedrag heeft betaald voor diensten of producten. Banken beschikken over deze betaalgegevens omdat zij een nutsfunctie hebben, namelijk het veilig en goed laten verlopen van het betaalverkeer. Consumenten hebben niet de keuze geen betaalrekening aan te houden. Ook indien klantgegevens alleen met toestemming commercieel worden gebruikt vind ik dat de consument moet worden beschermd in zijn persoonlijke levenssfeer. Banken mogen deze gegevens niet commercieel gebruiken. Een soepeler beleid heeft een te groot risico op een hellend vlak te komen, en dat is uiteindelijk niet in het belang van de consument. Ik vind dat er richtlijnen op dit gebied dienen te komen, hetzij wettelijk, hetzij vanuit de sector.

5.4. Klanten dienen daarentegen te allen tijde kunnen beschikken over hun eigen betaalgegevens. Deze informatie is immers van de klant, niet van de bank. Ik vind dat banken hierin faciliterend dienen te opereren. Het exporteren van betaalgegevens naar klanten, inclusief naar computerprogramma's die klanten thuis gebruiken, dient zo eenvoudig mogelijk te zijn. Ook het NIBUD is van mening dat inzicht in het eigen betaalgedrag van groot belang is. Hierbij dient de veiligheid van de online-omgeving echter gewaarborgd te worden.

5.5. Op afschriften staat soms na bijvoorbeeld een pintransactie een onbekende of vage naam. Dat strookt niet met de wens van banken dat consumenten afschriften controleren. De Consumentenbond vroeg hier onlangs aandacht voor.[12] Bedrijven moeten duidelijker communiceren en geen bedrijfscodes of onduidelijke namen opgeven op afschriften. De naam van het café of de supermarkt is heel anders dan «Mooiweer BV» of «Zaandam filiaal 11» die sommige winkels gebruiken. Banken zouden bedrijven daartoe ook moeten stimuleren. Zij vragen van consumenten immers dat zij hun rekening regelmatig controleren. Dat kan alleen als er bruikbare informatie is.

Nijboer

[12] http://www.consumentenbond.nl/actueel/nieuws/2014/onbegrijpelijke-bankafschrijvingen-irriteren-consumenten/