Uitspraak Geschillencommissie Financiële Dienstverlening nr. 2019-600
(mr. R.J. Paris, voorzitter en mr. T.A. Tang, secretaris)

Klacht ontvangen op	: 29 oktober 2018
Ingediend door	: Consument 1 en Consument 2, verder samen te noemen Consumenten
Tegen	: ABN AMRO Bank N.V., gevestigd te Amsterdam, verder te noemen de Bank
Datum uitspraak	: 20 augustus 2019
Aard uitspraak	: Bindend advies

Samenvatting

Ten laste van de en/of-rekening en de zakelijke rekening van Consumenten hebben acht betwiste transacties plaatsgevonden. Volgens Consumenten zijn wachtwoorden, pincodes, responsecodes en andere persoonlijke codes te allen tijde geheim gehouden. Daarnaast is de bankpas altijd in het bezit van Consumenten geweest. Voor zover de klacht betrekking heeft op de zakelijke rekening, oordeelt de Commissie dat deze niet behandelbaar is. Wat betreft de en/of- rekening overweegt de Commissie dat de Bank voldoende aannemelijk heeft gemaakt dat een onbevoegde derde met behulp van bankpas 1, de bijbehorende pincode en de met de e.dentifier verkregen responsecode een ander toestel aan het rekeningencomplex van Consument 1 heeft kunnen koppelen. Zodoende was het hierdoor voor een onbevoegde derde mogelijk om de transacties te authenticeren. De Commissie komt daarom tot het oordeel dat Consumenten kennelijk, ervan uitgaande dat zij niet zelf (bewust) de koppeling hebben verricht, zodanig hebben gehandeld dat de koppeling heeft kunnen plaatsvinden. Dit leidt ertoe dat de betwiste transacties op grond van artikel 7:529 lid 2 (oud) BW voor rekening en risico van Consumenten dienen te blijven.

1. Procesverloop

De Commissie beslist met inachtneming van haar Reglement en op basis van de volgende stukken:

- het door Consumenten ingediende klachtformulier met bijlagen;
- het verweerschrift van de Bank;
- de aanvulling op het verweerschrift van de Bank.

De Commissie stelt vast dat partijen hebben gekozen voor bindend advies.

Partijen zijn opgeroepen voor een hoorzitting op 24 juni 2019 en zijn aldaar verschenen.

2. Feiten

De Commissie gaat uit van de volgende feiten.

2.1 Consumenten houden meerdere bankrekeningen bij de Bank aan, waaronder een gezamenlijke en/of- rekening (hierna: bankrekening 1) en een zakelijke rekening (hierna: bankrekening 2). Hiervoor beschikken Consumenten over meerdere bankpassen. Aan bankrekening 1 is bankpas met nummer [nummer] (hierna: bankpas 1) gekoppeld. Verder maken Consumenten gebruik van de mogelijkheid om transacties te verrichten via Mobiel Bankieren met de ABN AMRO App, die op de mobiele telefoon van Consumenten is geïnstalleerd.

2.2 De Algemene Voorwaarden Bankvoorwaarden, de Voorwaarden Cliëntrelatie, de Voorwaarden Betaaldiensten Particulieren en het Informatieblad Betaaldiensten Particulieren (hierna: de voorwaarden) zijn van toepassing op de rechtsverhouding tussen partijen.

2.3 In artikel 15 van de Voorwaarden Cliëntrelatie is, voor zover relevant, bepaald:

> **"15. Risicoverdeling**
> Schade die ontstaat doordat de bank afgaat op een opdracht of andere Communicatie op naam van de cliënt die onjuist of buiten de wil van de cliënt aan de bank wordt overgebracht, wordt behoudens dwingend recht - volgens de volgende regels verdeeld:
>
> I. Indien de bank tegenover de cliënt in een (veiligheids)verplichting is tekortgeschoten, komt de schade voor rekening en risico van de bank voor zover deze als gevolg daarvan aan de bank kan worden toegerekend.
>
> II. Indien de cliënt tegenover de bank in een (veiligheids)verplichting is tekortgeschoten, komt de schade voor rekening en risico van de cliënt voor zover deze als gevolg daarvan
> aan de cliënt kan worden toegerekend.
>
> III. De schade komt voorts, op voorwaarde dat de bank aan haar desbetreffende (veiligheids)verplichtingen heeft voldaan, in ieder geval voor rekening en risico van de cliënt indien:
> - bij de Communicatie (onbevoegd) gebruik is gemaakt van een door de bank aan de cliënt (of zijn vertegenwoordiger) verstrekt Klantherkenningsmiddel; op naam gesteld papieren Formulier en/of het Elektronisch Klantdomein; en/of
> - de bank erop mocht vertrouwen dat de Communicatie juist en overeenkomstig de wil van de cliënt aan haar is overgebracht."

2.4 Consumenten beschikken over een prepaid creditcard (hierna: de creditcard) die door een creditcardmaatschappij aan hen is verstrekt.

2.5 Op 27 juli 2018 om 16.42 uur ontvangt Consument 1 een e-mail met als onderwerp [domeinnaam] Act now (hierna: de e-mail). Daarnaast bevat de e-mail een link met de benaming 'secure online payment'. Verder staat in de e-mail vermeld dat de prijs $ 84,00 is.

2.6 Op 28 juli 2018 heeft Consument 1 op de link in de e-mail geklikt waarna zij is doorgeleid naar een site. Op die site heeft Consument 1 het creditcardnummer van haar creditcard ingevuld.

2.7 Vervolgens hebben Consumenten op maandag 30 juli 2018 ontdekt dat de volgende bedragen van bankrekening 1 zijn afgeschreven:

29 juli 2018	€ 1.499,-
28 juli 2018	€ 732,01
28 juli 2018	€ 721,71
28 juli 2018	€ 562,62
28 juli 2018	€ 344,48
28 juli 2018	€ 338,31
28 juli 2018	€ 329,26

Daarnaast hebben Consumenten ontdekt dat er op 29 juli 2018 een bedrag van € 1.499,00 van bankrekening 2 is afgeschreven. Op 30 juli 2018 heeft Consument 1 contact met de Bank opgenomen om melding te doen van de onbevoegde transacties. Tussen 10.07 uur en 10.09 uur heeft Consument 1 de pincodes van de bankpassen gewijzigd. Vervolgens heeft de Bank op dezelfde dag een brief aan Consumenten gestuurd met daarin instructies.

2.8 Op 3 augustus 2018 heeft Consument 1 op het politiebureau te [plaats] aangifte gedaan. In het proces-verbaal staat voor zover relevant:

"(…)
Ik heb dit domein in oktober 2017 geclaimd bij het bedrijf [naam bedrijf]. Het is gebruikelijk dat er 1 keer per jaar een rekening wordt gestuurd voor een domeinnaam, derhalve vond ik het niet raar dat ik een rekening kreeg voor het domein.
(…)
Ik drukte (handgeschreven aantekening: ->za/28-7) op de link die in de e-mail stond. Die link bracht mij bij een site waar ik mijn creditcard gegevens moest invullen. Ik heb dit toen gedaan. Ik heb het bedrag van 84 dollar proberen te voldoen middels mijn creditcardrekening met nummer [nummer]. De bank heeft deze transactie echter geblokkeerd omdat de bank het een verdachte transactie vond. De bank zei dat de ontvanger uit [naam land] kwam.
(…)
Maandag 30 juli 2018 omstreeks 08.00 uur in de ochtend kwam ik erachter dat er er betalingen met mijn rekeningen waren gedaan.

(…)
Alleen ik heb toegang tot deze rekeningen en ik heb niemand toestemming geven om dergelijke handelingen uit te voeren.
(…)
Ik vermoed dat mijn laptop geïnfecteerd is geraakt door de link die ik in de email heb ingedrukt. Op aanraden van de bank is mijn laptop geschoond. Dit is gedaan door een specialist werkzaam bij [naam bedrijf]. De specialist zei dat de e-mail- er professioneel uitzag.
(…)"

2.9 Bij brief van 9 augustus 2018 heeft de Bank aan Consumenten geschreven:

"(…)
Waarom gaan wij de schade niet uitkeren?
Uit ons onderzoek is gebleken dat de schade is ontstaan doordat u op een phishing e-mail heeft gereageerd. Nadat u op de link in deze e-mail heeft geklikt kwam u op een onbekende website terecht. U geeft aan dat u op deze website de gegevens van uw (prepaid) creditcard, die gekoppeld is aan uw zakelijke rekening, heeft ingevuld. De omgeving waarin u aan het bankieren was, kwam u niet bekend voor. Daarbij heeft u zich niet gehouden aan de 5 veiligheidsregels die door de Betaalvereniging Nederland voor veilig bankieren zijn opgesteld. (…)"

2.10 Op 13 augustus 2018 dienen Consumenten een schriftelijke klacht in bij de Bank. In de brief staat:

"(…)

- We hebben de 5 veiligheidsregels in acht genomen - zoals we altijd doen:
  - Beveiligingscodes geheim houden
  - Bankpas is niet door derden gebruikt
  - Laptop was volgens ons (als niet IT-specialisten) beveiligd
  - We controleren bijna dagelijks onze bankrekeningen (anders hadden we ook niet meteen maandag-ochtend 30-7 kunnen reageren en met de bank gebeld)
  - Het incident is onmiddellijk aan de bank gemeld, op maandag 30-7-2018.

    De zelfde dag zijn de pincodes, identificatiecodes van alle bankpasjes gewijzigd en is ook de laptop geschoond (er was gelukkig geen virus oid op te vinden).

- Als een consument die te goeder trouw is, ben ik in een professioneel opgezette val gestapt, waarvan ik uiteraard achteraf spijt heb en een goede les is om voortaan nog attenter te zijn.

- Bovenstaande feiten in beschouwing genomen, zijn wij van mening dat U mij geen grove nalatigheid kunt verwijten, cq dat ik mij niet aan de veiligheidsregels heb gehouden.

(…)"

2.11 In haar brief van 18 september 2018 heeft de Bank aan Consumenten geschreven dat zij de schade niet vergoedt.

“(…)
Wat vinden wij?
Wij merken hierbij het volgende op. Door toedoen van 'phishing' of 'malware' is vertrouwelijke informatie - zoals één of meer persoonlijke code(s)- aan derden doorgegeven. Kennelijk is via de door u ontvangen nepmail en de geopende link, een infiltratie in de beveiliging van uw computer mogelijk gemaakt en het systeem als het ware 'overgenomen'.

Deze vorm van fraude komt voor wanneer sprake is van een geïnfecteerde computer voor Internet Bankieren.
(…)
Beide partijen zijn verplicht om zich aan de voorwaarden te houden, om misbruik tegen te gaan.
(…)
Wij benadrukken dat de bank niet verantwoordelijk is voor dergelijke oplichting van buitenaf. Bedragen worden nooit zomaar van een bankrekening afgeboekt. Daarvoor is altijd een pin- of responsecode voor nodig. De bank verwacht van u dat u uw persoonlijke code(s) zorgvuldig bewaart en tijdens het gebruik er zorgvuldig mee omgaat. Dit houdt in dat u een wachtwoord, een pincode, een reponsecode en (een) andere persoonlijke code(s) strikt geheim dient te houden. Ook zijn regels opgesteld hoe u op een veilige manier van de code in combinatie met de communicatiemiddelen van de bank gebruik kunt maken. Kortom, de bank ziet geen reden haar standpunt te wijzigen. De transacties zullen niet vergoed worden.
(…)”

2.12 Bij brief van 1 oktober 2018 schrijven Consumenten aan de Bank:
“(…)
U geeft aan dat „door toedoen van…..is vertrouwelijke informatie - zoals een of meer persoonlijke code(s)- aan derden doorgegeven" en dat „u uw bankgegevens en bijbehorende beveiligingscodes niet geheim heeft gehouden".
Dit is echter niet het geval en feitelijk onjuist - de enige informatie die is doorgegeven is het credit-card nummer van mijn ([naam consument 1]) pre-pay credit-card. Er zijn nooit persoonlijke code (s) of andere klantherkenningsmiddelen aan derden doorgegeven.

Tevens vermeldt u dat "deze vorm van fraude komt voor wanneer sprake is van een geïnfecteerde computer voor Internet Bankieren". Dit was niet het geval. Na vaststelling van de fraude hebben we onze computer onmiddellijk laten checken en schonen, er is geen infectie vastgesteld.

Samenvattend, uw argument is dat op basis van bovengenoemde suggesties, wij als klant tekort zijn geschoten in de veiligheids-verplichting doordat wij onze persoonlijke inlog- en responscodes hebben vrijgegeven. Zoals vermeld, dit is niet het geval - persoonlijke codes zijn nooit doorgegeven. Wachtwoord, pincode, responsecode en andere persoonlijke codes zijn ten allen tijde geheim gehouden.

Overigens heeft de credit-card firma tijdig de overboeking weten te blokkeren, en de vraag rijst hoe het kan dat U als ABN-AMRO geen veiligheids-systemen in acht houdt waarmee deze ongeoorloofde betalingen vanaf onze ABN-AMRO rekening wel vermeden hadden kunnen worden?
(…)”

2.13 In haar e-mail van 22 oktober 2018 schrijft de Bank aan Consumenten:

> "(…)
> U heeft aangegeven dat mevrouw [naam Consument 1] alleen de creditcardgegevens heeft achtergelaten op de phishing mail die zij ontvangen had. Echter, de frauduleuze handelingen die daarna plaatsgevonden hebben, kunnen niet zijn uitgevoerd met alleen de creditcardgegevens. Er is dus geen direct verband tussen het achterlaten van de creditcardgegevens en frauduleuze transacties op 28 en 29 juli 2018.
>
> Wij verwijzen naar ons eerdere antwoord van 18 september 2018; Het betreft Artikel 15 van de Voorwaarden Cliëntrelatie. De bank valt niets aan te rekenen, als zij tegenover de klant niet in een veiligheidsverplichting is tekortgeschoten. Als de klant tekort is geschoten in de veiligheidsverplichting, dan is de schade voor rekening en risico van de klant. Dit is van toepassing wanneer onbevoegd gebruik is gemaakt met een door de bank aan de klant verstrekt klantherkenningsmiddel, in combinatie met de pincode en inlogcodes. Wij blijven van mening dat dit hier van toepassing is.
>
> Een onbevoegde heeft kans gezien om met uw hulp toegang te krijgen tot uw bankrekening via Internet Bankieren. Doordat u deze onbevoegde de mogelijkheid heeft geboden om uw PC te bedienen én u mogelijk onbewust uw persoonlijke inlog- en responscodes heeft vrijgegeven, heeft de onbevoegde kans gezien om over uw bankrekeningen te beschikken. De bank kan zich daar niet tegen wapenen. Hiervoor kunt u de bank niet aansprakelijk houden. De bank is niet verantwoordelijk voor dergelijke oplichting van buitenaf.
> (…)"

2.14 Op 29 oktober dienen Consumenten een klacht in bij Kifid.

3. Vordering, klacht en verweer

Vordering Consument

3.1 Nu Consumenten de transacties niet zelf hebben verricht vorderen zij dat de Bank wordt veroordeeld tot het betalen van een bedrag van € 6.026,39, zijnde het bedrag van de betwiste transacties.

Grondslagen en argumenten daarvoor

3.2 Aan de vordering leggen Consumenten ten grondslag dat zij niet grof nalatig zijn geweest. Wachtwoorden, pincodes, responsecodes en andere persoonlijke codes zijn te allen tijde geheim gehouden. Consumenten hebben zich altijd gehouden aan de vijf uniforme veiligheidsregels van banken in Nederland en de Consumentenbond. Daarnaast is de bankpas altijd in het bezit van Consumenten geweest. Volgens Consumenten is er ook geen sprake van een geïnfecteerde computer.

Verweer van de Bank

3.3 De Bank heeft de stellingen van Consumenten gemotiveerd weersproken. Voor zover nodig zal de Commissie bij de beoordeling daarop ingaan.

4. Beoordeling

Behandelbaarheid van de klacht

4.1 Voordat de vordering van Consumenten inhoudelijk kan worden beoordeeld, moet aan de hand van het Reglement worden nagegaan of deze klacht in aanmerking komt voor behandeling door de Commissie.

4.2 In dit kader stelt de Commissie vast dat deze klacht een zakelijk element heeft, namelijk bankrekening 2 betreft een zakelijke bankrekening waar een bedrag van € 1.499,00 van is afgeschreven. De Commissie dient daarom allereerst ambtshalve vast te stellen of zij volgens haar Reglement bevoegd is om deze klacht inhoudelijk te beoordelen.

4.3 Het Reglement bepaalt, voor zover hier relevant, over de behandelbaarheid van klachten:

> "Artikel 1 Welke klachten behandelt de Geschillencommissie?
> De Geschillencommissie behandelt Klachten van Consumenten over Financiële diensten tegen Financiële dienstverleners of, bij nawerking, voormalig aangesloten Financiële dienstverleners. (…)
> Artikel 60 Begrippen
> In dit Reglement wordt verstaan onder:
> Consument:
> Iedere natuurlijke persoon die handelt voor doeleinden die buiten zijn handels-, bedrijfs-, ambachts- of beroepsactiviteit vallen. Wordt de overeenkomst evenwel gesloten voor doeleinden die deels binnen en deels buiten in de vorige volzin genoemde activiteit van de persoon liggen (gemengde overeenkomsten) en is het oogmerk van die activiteit zo beperkt dat het binnen de algehele context van de overeenkomst niet overheerst, dan dient die persoon eveneens als Consument te worden aangemerkt. (...)"

4.4 De Commissie heeft begrepen dat bankrekening 2 voor zakelijke doeleinden van het bedrijf van Consumenten bestemd was. Gelet op deze informatie zijn Consumenten met betrekking tot deze bankrekening niet te kwalificeren als 'Consument' in de zin van het Reglement. De Commissie is daarom van oordeel dat de klacht, voor zover deze betrekking heeft op de transactie die op bankrekening 2 heeft plaatsgevonden, niet behandelbaar is.

En/of-rekening

4.5 De klacht ziet verder op de zeven transacties die van bankrekening 1, de en/of- rekening van Consumenten, zijn afgeschreven.

Het totaalbedrag van deze transacties bedraagt € 4.527,39. Beoordeeld moet worden of deze transacties voor rekening en risico van Consumenten of de Bank dienen te komen.

4.6 Ten aanzien van betaaldiensten bevat het Burgerlijk Wetboek (BW) een regeling in artikel 7:522 en verder. De nummering van deze bepalingen is in februari 2019 gewijzigd; hierna zal worden verwezen naar de wettekst die van toepassing was ten tijde van de voor deze procedure relevante transacties. Het volgende is bepaald over de vraag voor wiens rekening en risico de schade komt als er sprake is van niet- toegestane transacties.

4.7 Op grond van artikel 7:529 lid 2 (oud) BW draagt de betaler alle verliezen die uit niet-toegestane betalingstransacties voortvloeien voor zover hij frauduleus heeft gehandeld of opzettelijk of met grove nalatigheid een of meer verplichtingen uit hoofde van artikel 7:524 (oud) BW niet is nagekomen. In artikel 7:524 (oud) BW is ook bepaald dat de betaler zich moet houden aan de veiligheidsregels die de Bank stelt.

4.8 In beginsel is het aan de Bank om te bewijzen dat er sprake is van grove nalatigheid in de nakoming van de verplichtingen uit de voorwaarden. Daar staat tegenover dat het aan Consumenten is om voldoende inzichtelijk te maken onder welke omstandig-heden een derde toegang zou kunnen hebben gehad tot de bankrekening en zodoende betalingsopdrachten heeft kunnen geven. Hierdoor zou de Bank zich in ieder geval een beeld kunnen vormen van de manier waarop Consumenten met de bankpas en de bankrekening zijn omgaan.

4.9 Consumenten stellen dat zij slachtoffer zijn geworden van frauduleuze handelingen van derden doordat zij het nummer van de prepaid creditcard hebben ingevuld op een site na ontvangst van de e-mail.

4.10 Volgens de Bank is het onmogelijk dat de transacties zijn uitgevoerd op basis van uitsluitend de gegevens van de prepaid creditcard van Consumenten. Zij voert aan dat uit technisch onderzoek is gebleken dat de transacties zijn uitgevoerd met behulp van responsecodes die met bankpas 1 zijn verkregen. Op 28 juli 2018 is een Iphone [type] (hierna: Iphone) aan het account van Consument 1 gekoppeld. Deze koppeling heeft plaatsgevonden met behulp van het rekeningnummer van bankrekening 1, het driecijferig volgnummer van bankpas 1 en de e.dentifier responsecode. De e.dentifier responsecode is gegenereerd met behulp van een e.dentifier, bankpas 1 en de pincode behorende bij bankpas 1. Hiermee is met de Iphone toegang verkregen tot het rekeningencomplex van Consument 1. Vervolgens zijn de transacties met de Iphone via iDEAL door middel van Mobiel Bankieren met de ABN AMRO app uitgevoerd. In dit kader heeft de Bank een uitdraai uit de administratie overgelegd.

4.11 Gelet op het hiervoor overwogene kan het niet anders zijn dan dat op 28 juli 2018 met behulp van bankpas 1, de bijbehorende pincode en de met de e.dentifier verkregen responsecode een ander toestel (in dit geval: de Iphone) aan het rekeningencomplex van Consument 1 is gekoppeld. Door deze koppeling konden derden met behulp van de gekoppelde Iphone toegang krijgen tot het rekeningencomplex van Consument 1. Zodoende was het hierdoor voor een onbevoegde derde mogelijk om de transacties te authenticeren.

4.12 Naar het oordeel van de Commissie is hiermee in voldoende mate komen vast te staan dat de betwiste transacties zijn verricht met behulp van de Iphone die op 28 juli 2018 aan het rekeningencomplex van Consument 1 is gekoppeld met behulp van bankpas 1, de bijbehorende pincode en de met de e.dentifier verkregen responsecode.

4.13 Consumenten kunnen niet verklaren hoe een ander toestel aan hun rekeningencomplex gekoppeld kon worden. De argumenten van Consumenten kunnen niet leiden tot een andere conclusie dan hiervoor vermeld. De Commissie komt daarom tot het oordeel dat Consumenten kennelijk, ervan uitgaande dat zij niet zelf (bewust) de koppeling hebben verricht, zodanig hebben gehandeld dat de koppeling aan een ander toestel heeft plaatsgevonden. Consumenten zijn zodoende grof nalatig geweest (in de zin van artikel 7:529 lid 2 (oud) BW). Dit leidt ertoe dat de betwiste transacties op grond van artikel 7:529 lid 2 (oud) BW voor rekening en risico van Consumenten dienen te blijven. Voor de volledigheid merkt de Commissie op dat 'grof nalatig' een wettelijke term is en dat de Commissie in de beoordeling van deze klacht zich heeft beperkt tot die juridische toets.

4.14 Daarnaast is het de Commissie niet gebleken dat er specifieke omstandigheden zijn die aanleiding geven om de aansprakelijkheid van Consumenten te beperken op grond van artikel 7:529 lid 3 (oud) BW.

4.15 Hiervoor is geconstateerd dat de transacties zijn geauthenticeerd met response-codes die met een gekoppelde Iphone zijn verkregen. De transacties op bank-rekening 1 zien op aankopen bij reguliere Nederlandse bedrijven. Naar het oordeel van de Commissie zijn er voor de Bank, gelet op de situatie, geen redenen om de transacties in twijfel te trekken. Een vergelijking met de transactie die door de creditcardmaatschappij is tegengehouden kan niet worden getrokken, nu het in die situatie gaat om een begunstigde in [naam land]. Ten overvloede merkt de Commissie op dat de Bank geen algemene signalerings- en monitoringsplicht heeft bij (afwijken-de) mutaties van het banksaldo van haar klanten.

4.16 Het voorgaande brengt met zich mee dat, hoewel Consumenten slachtoffers zijn geworden van een gewiekste handelwijze van criminelen, de schade als gevolg daarvan voor hun rekening dient te blijven. De vordering van Consumenten dient te worden afgewezen.

5. Beslissing

De Commissie wijst de vordering af.

In artikel 2 van het Reglement van de Commissie van Beroep Financiële Dienstverlening is bepaald in welke gevallen beroep openstaat van bindende beslissingen van de Geschillencommissie Financiële Dienstverlening bij de Commissie van Beroep Financiële Dienstverlening. Daarbij geldt een termijn van zes weken na verzending van deze uitspraak. Op de website van Kifid vindt u praktische informatie over het instellen van beroep. Zie hiervoor www.kifid.nl/in-beroep-gaan-bij-kifid.

U kunt, binnen twee weken na de verzenddatum van deze uitspraak, bij de Voorzitter van de Geschillencommissie Financiële Dienstverlening schriftelijk een verzoek indienen tot herstel van kennelijke vergissingen in de uitspraak. U moet daarbij met name denken aan correctie van reken- of schrijffouten en verbetering van namen en data. De volledige procedure met de termijnen die daarbij in acht moeten worden genomen staat beschreven in artikel 40 van het Reglement.