

**Tussenuitspraak Geschillencommissie Financiële Dienstverlening nr. 2021-0761A  
(mr. F.H.E. Boerma, voorzitter, mr. dr. D.P.C.M. Hellegers, A.E. Tevel, leden en  
mr. J. Hadziosmanovic, secretaris)**

Klacht ontvangen op : 7 januari 2021  
Ingediend door : De consument  
Tegen : ABN AMRO Bank N.V., gevestigd te Amsterdam, verder te noemen de bank  
Datum uitspraak : 27 augustus 2021  
Aard uitspraak : Bindend advies  
Uitkomst : Tussenuitspraak  
Bijlage : Relevante wetgeving

## **Samenvatting**

Tussenuitspraak. Niet-toegestane betalingstransactie. De niet van de consument is gemachtigd tot de betaalrekening van de consument bij de bank. Hiertoe beschikte zij over een betaalkas met pincode. Tijdens de vakantie van de niet is in haar woning ingebroken en hebben derden de betaalkas en pincode behorende bij de betaalrekening van de consument onttrokken en gelden opgenomen van de rekening tot een bedrag van € 11.907,-. De bank heeft het verzoek van de consument tot vergoeding van de schade afgewezen waarna de consument een klacht bij Kifid heeft ingediend. De commissie is van oordeel dat sprake is van 'grof nalatig' handelen in de zin van de wet en de contractuele voorwaarden waardoor de schade in beginsel voor rekening van de consument komt. Daarnaast is in geschil of de bank de op haar rustende (zorg)verplichtingen om de betaalkas tijdig te blokkeren na het detecteren van ongebruikelijke transacties heeft geschonden. De commissie verzoekt de bank nader inzicht te geven in hoe zij deze op haar rustende verplichting heeft ingevuld en houdt iedere verdere beslissing aan.

## **1. De procedure**

- 1.1 De commissie beslist op basis van haar reglement en op basis van de door partijen aan Kifid ingestuurde documenten inclusief bijlagen. Het gaat om: 1) het klachtformulier van de consument; 2) het verweerschrift van de bank; 3) de repliek van de consument en 4) de dupliek van de bank.
- 1.2 De commissie is van oordeel dat het niet nodig is de zaak mondeling te behandelen. De zaak wordt daarom op grond van de stukken beslist.
- 1.3 De consument en de bank hebben gekozen voor een bindend advies. Dit betekent dat partijen elkaar aan de uitspraak kunnen houden.

## 2. Het geschil

*Wat is er gebeurd?*

- 2.1 De consument houdt een betaalrekening aan bij de bank en de nicht van de consument is gemachtigde tot deze betaalrekening. Hiertoe beschikt de nicht over een betaalpas met pincode behorende bij de rekening. De paslimieten van de betaalpas waren ingesteld op € 1.000,- per dag voor opnames bij een geldautomaat en € 5.000,- per dag voor transacties bij een betaalautomaat.
- 2.2 Op de overeenkomst tussen de bank en de consument ter zake de betaalrekening zijn de Algemene Bankvoorwaarden, de Voorwaarden Betaaldiensten Particulieren en het Informatieblad Betaaldiensten Particulieren van toepassing.

In de Algemene Bankvoorwaarden staat:

### **Artikel 9 Vertegenwoordiging en volmacht**

*(...)*

*3. Uw vertegenwoordiger houdt zich aan dezelfde regels als u. U informeert elkaar. Alle regels die voor u gelden in uw relatie met ons, gelden ook voor uw vertegenwoordiger. U bent ervoor verantwoordelijk dat uw vertegenwoordiger zich daaraan houdt. Ook moeten u en uw vertegenwoordiger elkaar steeds goed blijven informeren over alles wat er in uw relatie met ons van belang kan zijn.*

*Een voorbeeld:*

*Uw vertegenwoordiger heeft een bankpas waarvan hij of zij namens u gebruik kan maken. Die vertegenwoordiger moet zich dan aan dezelfde veiligheidsvoorschriften houden als u. Als wij deze voorschriften aan u bekendmaken, geeft u deze meteen aan uw vertegenwoordiger door.*

### **Artikel 21 - Bewaar- en geheimhoudingsplicht**

*U gaat zorgvuldig om met codes, formulieren en passen. Als misbruik aannemelijk is, meldt u dit meteen.*

*1. U moet zorgvuldig en veilig omgaan met codes, formulieren, (bank)passen of andere hulpmiddelen. Zo helpt u voorkomen dat deze in verkeerde handen raken of dat iemand ervan misbruik kan maken.*

*2. Het kan gebeuren dat een code, formulier, (bank)pas, of ander hulpmiddel in verkeerde handen komt of dat iemand daarvan misbruik maakt of kan maken. Als u dit weet of redelijkerwijs kan vermoeden, meldt u dit meteen aan ons. Door uw melding kunnen wij proberen (verder) misbruik te voorkomen.*

*3. Houdt u er rekening mee dat wij nog andere veiligheidsregels stellen (zoals de Uniforme Veiligheidsregels Particulieren).*

In de Voorwaarden Betaaldiensten Particulieren van de bank staat:

### **6.3. Wie draagt het risico van misbruik?**

*Wanneer de bank zonder geldige opdracht een betaaltransactie uitvoert en van uw betaalrekening afschrijft geldt het volgende. Het afgeschreven bedrag komt dan voor rekening van de bank. Uitzondering hierop zijn de gevallen die hieronder worden beschreven.*

▢ Als u met opzet of op grove wijze nalatig bent geweest in de strikte naleving van de veiligheidsregels van de bank zijn de betaaltransacties volledig voor uw rekening en risico. Dit geldt tot het moment waarop u aan de bank meldt dat iemand onbevoegd uw klantherkenningsmiddelen kan gebruiken. De veiligheidsregels vindt u in het Informatieblad Betaaldiensten en in de Voorwaarden Cliëntrelatie.

▢ Als u frauduleus handelt zijn de betaaltransacties volledig voor uw rekening en risico. Hiermee wijkt de bank af van de risicoverdeling zoals die in de Voorwaarden Cliëntrelatie staat.

In artikel 1A het Informatieblad Betaaldiensten Particulieren van de bank staat:

#### **Toelichting veiligheidsregels**

*I Houd uw beveiligingscodes geheim Denk hierbij aan het volgende:*

*> Zorg ervoor dat beveiligingscodes nooit aan een ander bekend kunnen worden. Beveiligingscodes zijn niet alleen de pincode die u in combinatie met de betaalpas gebruikt. Het zijn ook alle andere codes die u moet gebruiken om elektronische betalingen te doen en gebruik te maken van Internet Bankieren en mobiele bankapps. Dat kunnen bijvoorbeeld de codes zijn die een door de bank verstrekte codecalculator aangeeft (zoals de e.dentifier), codes die u via een mobiele bankapp en/of die u per SMS van uw bank ontvangt.*

*> U mag deze beveiligingscodes alleen zelf gebruiken. U moet dat doen op de manier die de bank aangeeft. In onderdeel 1B van dit hoofdstuk staat welk gebruik van beveiligingscodes is toegestaan.*

*> Schrijf of sla de codes niet op. Of, als het echt niet anders kan, alleen in een voor anderen onherkenbare vorm die alleen door uzelf te ontcijferen is. Bewaar in dit geval de versleutelde informatie niet bij uw betaalpas of bij apparatuur waarmee u uw bankzaken regelt*

- 2.3 Op 10 augustus 2020 is ingebroken in de woning van de nicht en zijn de betaalpas en pincode gestolen, waarna de daders in de periode van 10 augustus 2020 tot en met 13 augustus 2020 door gebruikmaking van de betaalpas en het invoeren van de juiste pincode in 12 transacties een bedrag van € 11.907,- van de rekening hebben afgeboekt.

Het gaat om de volgende transacties in binnen- en buitenland:

| boekdatum  | omschrijving                                                                                                                           | bedrag af     |
|------------|----------------------------------------------------------------------------------------------------------------------------------------|---------------|
| 13-08-2020 | BEA NR:2X8101 13.08.20/13.23<br>FC Hoorn,PAS331<br>HOORN NH<br>BEA BINNENLAND (mut. code:426)                                          | -300,00 EUR   |
| 13-08-2020 | BEA NR:2X8101 13.08.20/13.23<br>FC Hoorn,PAS331<br>HOORN NH<br>BEA BINNENLAND (mut. code:426)                                          | -300,00 EUR   |
| 13-08-2020 | BEA NR:2X8101 13.08.20/13.22<br>FC Hoorn,PAS331<br>HOORN NH<br>BEA BINNENLAND (mut. code:426)                                          | -300,00 EUR   |
| 13-08-2020 | GEA NR:00001621 13.08.20/00.30<br>Volksbank Emmerich-Ree,PAS331<br>BAG_621,Land: DE<br>GEA ACTIEF GASTGEBRUIK BUITENL. (mut. code:446) | -1.000,00 EUR |
| 12-08-2020 | BEA NR:65021304 12.08.20/13.43<br>Diamond Prinss,PAS331<br>Antwerpen,Land: BE<br>BEA BUITENLAND (mut. code:369)                        | -350,00 EUR   |
| 12-08-2020 | BEA NR:65021304 12.08.20/13.37<br>Diamond Prinss,PAS331<br>Antwerpen,Land: BE<br>BEA BUITENLAND (mut. code:369)                        | -3.650,00 EUR |
| 12-08-2020 | BEA NR:23012703 12.08.20/13.54<br>Insaff,PAS331<br>Antwerpen,Land: BE<br>BEA BUITENLAND (mut. code:369)                                | -7,00 EUR     |
| 12-08-2020 | GEA NR:00001621 12.08.20/00.02<br>Volksbank Emmerich-Ree,PAS331<br>BAG_621,Land: DE<br>GEA ACTIEF GASTGEBRUIK BUITENL. (mut. code:446) | -1.000,00 EUR |
| 11-08-2020 | BEA NR:WK003710 11.08.20/15.37<br>EUROPE GOLD,PAS331<br>ANTWERPEN,Land: BE<br>BEA BUITENLAND (mut. code:369)                           | -3.000,00 EUR |
| 11-08-2020 | GEA NR:00001621 11.08.20/01.37<br>Volksbank Emmerich-Ree,PAS331<br>BAG_621,Land: DE<br>GEA ACTIEF GASTGEBRUIK BUITENL. (mut. code:446) | -1.000,00 EUR |
| 10-08-2020 | GEA NR:S10228 10.08.20/15.16<br>2E HOGEWEG 38,PAS331<br>ZEIST<br>GELDAUTOMAAT OPNAME (mut. code:361)                                   | -900,00 EUR   |
| 10-08-2020 | GEA NR:006135 10.08.20/15.10<br>ING,PAS331<br>ZEIST<br>GEA ACTIEF GASTGEBRUIK BINNENL. (mut. code:445)                                 | -100,00 EUR   |

- 2.4 De bank heeft de betaalpas op 13 augustus 2020 om 13.25 uur geblokkeerd nadat het fraudesysteem een mogelijk ongebruikelijke transactie detecteerde.

#### *De klacht en vordering*

- 2.5 De consument vordert terugbetaling van het gestolen tegoed van € 11.907,- van de bank en stelt dat de bank dit dient te vergoeden.

De nicht van de consument heeft haar betaalpas opgeborgen in een map in een kast in de studeerkamer van haar woning en de pincode was opgeborgen in een map in een lade in een andere kamer.

Zij stelt dat er geen sprake is van opzettelijk of grof nalatig handelen waardoor de criminelen zich toegang hebben verschaft tot het tegoed op haar rekening. Zij verwijt de bank dat deze niet eerder dan op 13 augustus 2020 heeft ingegrepen nadat er al grote bedragen van de rekening waren opgenomen omdat het gaat om ongebruikelijke transacties in verschillende landen terwijl niet eerder gebruik was gemaakt van deze betaalpas.

#### *Het verweer*

- 2.6 De bank heeft verweer gevoerd tegen de stellingen van de consument en aangevoerd dat de betaalpas en pincode niet goed opgeborgen waren en het voor de inbreker(s) mogelijk is geweest om de betaalpas van gemachtigde te bemachtigen en daarnaast ook de strikt vertrouwelijke pincode. Op 12 november 2020 heeft de nicht telefonisch aan de bank verklaard dat zij de betaalpas bewaarde in een lade in een kast in de slaapkamer samen met andere waardevolle eigendommen zoals vreemde valuta en identificatiedocumenten. Deze lade kon niet afgesloten worden. De pincode bewaarde zij in een envelop in een map in een kast in de studeerkamer. Deze kast kon wel worden afgesloten maar was ten tijde van de inbraak niet afgesloten met de bijbehorende sleutel.
- 2.7 Het was voor de onbevoegden mogelijk om de betaalpas en de pincode te vinden en deze aan elkaar te koppelen. Volgens de bank heeft de nicht zich niet gehouden aan de voorwaarden en veiligheidsregels van de bank zoals die zijn voorgeschreven in het Informatieblad Betaaldiensten Particulieren. De schade komt daardoor geheel voor rekening van de consument. De bank verwijst hiervoor ook naar artikel 6.3 van de Voorwaarden Betaaldiensten Particulieren.
- 2.8 De bank heeft de betaalpas op 13 augustus 2020 om 13.25 uur geblokkeerd nadat haar fraudedetectiesysteem enkele transacties als ongebruikelijk had gedetecteerd. Daarmee is verdere schade voor de consument voorkomen.

### **3. De beoordeling**

#### *Inleiding*

- 3.1 De commissie ziet zich voor de vraag gesteld of de bank ertoe gehouden kan worden de schade die consument heeft geleden, doordat onbevoegde derden gelden van haar rekening hebben opgenomen, te vergoeden. Alvorens in te gaan op de inhoudelijke behandeling van de klacht, hecht de commissie er waarde aan op te merken dat 'grof nalatig' een wettelijke term is, die is opgenomen in de toepasselijke wet- en regelgeving (zie bijlage).

Dit betekent dat de commissie bij haar beoordeling een juridisch oordeel – en dus geen moreel waardeoordeel – geeft over de handelwijze van de consument (ofwel haar nicht).

#### *Juridisch kader*

- 3.2 Het toetsingskader voor het onderhavige geval wordt geregeld in artikel 7:524 Burgerlijk Wetboek (BW) en verder (zie bijlage). Daarin is, en in navolging daarvan in de toepasselijke voorwaarden (zie overweging 2.2.) bepaald dat de betaaldienstgebruiker (een consument) alle redelijke maatregelen dient te nemen om de veiligheid van de gepersonaliseerde veiligheidskenmerken van zijn betaalpas te waarborgen. Artikel 7:529 BW bepaalt dat alle verliezen voor rekening en risico van de betaaldienstgebruiker komen, indien opzettelijk of met grove nalatigheid niet aan de voorwaarden van artikel 7:524 BW is voldaan. In artikel 7:529 lid 2 BW is de bevoegdheid tot matiging van de aansprakelijkheid van de consument neergelegd. Een bevoegdheid die alleen dan openstaat als een consument niet frauduleus of opzettelijk heeft gehandeld en de specifieke feiten en omstandigheden van het geval tot matiging aanleiding geven.

#### *Is er sprake van grof nalatig handelen in juridische zin?*

- 3.3 De bank heeft gesteld dat de nicht 'grof nalatig', zoals bedoeld in de wet en in de voorwaarden heeft gehandeld en dat de bank daarom niet gehouden is de door de consument geleden verliezen te vergoeden. De bank heeft daarbij aangevoerd dat de nicht zich niet heeft gehouden aan de voorwaarden en veiligheidsregels van de bank zoals die zijn voorgeschreven in het Informatieblad Betaaldiensten Particulieren. De betaalpas en pincode waren blijkbaar niet goed genoeg verstopt, dan wel de lade en de kast waarin deze werden bewaard waren niet afgesloten tijdens haar vakantie. De pincode mag voorts niet worden opgeschreven of opgeslagen en indien niet anders mogelijk dan mag het alleen opgeschreven of opgeslagen worden op een manier dat deze voor anderen onherkenbaar is en alleen door de houder ervan kan worden ontcijferd. Dit was niet het geval. De schade had volgens de bank verder (geheel of gedeeltelijk) kunnen worden voorkomen door direct na bekend te zijn geworden met de inbraak op 10 augustus 2020, uit veiligheidsoverwegingen, de betaalpas te blokkeren door mogelijke diefstal direct te melden bij de bank.
- 3.4 De commissie is van oordeel dat de tot de betaalrekening bevoegde nicht van de consument de veiligheidsvoorschriften, zoals bedoeld in artikel 7:524 BW en de voorwaarden van de bank niet heeft nageleefd en in wettelijke zin grof nalatig is geweest. Hoewel de nicht van de consument de betaalpas en pincode niet naast elkaar heeft bewaard, heeft zij de pincode wel bewaard in een voor derden te herkennen formaat.

*Heeft de bank onzorgvuldig gehandeld door de betaalpas niet eerder te blokkeren?*

- 3.5 De consument heeft gesteld dat de bank de betaalpas eerder had moeten blokkeren dan 13 augustus 2020, omdat de transacties al vanaf 10 augustus 2020 door de bank als ongebruikelijk moesten worden aangemerkt nu deze zijn gedaan op verschillende plaatsen in binnen en buitenland. Daarnaast is de betaalpas in september 2017 aangevraagd en geactiveerd, maar is er tot aan het incident geen gebruik van gemaakt.
- 3.6 De commissie oordeelt als volgt. In artikel 2 van de Gedelegeerde Verordening (EU) 2018/389 van de Commissie van 27 november 2017 tot aanvulling van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad wat betreft technische reguleringsnormen voor sterke cliëntauthenticatie en gemeenschappelijke en veilige open communicatiestandaarden<sup>1</sup>, welke in september 2019 in werking is getreden, staat het volgende opgenomen:

#### *Artikel 1*

#### **Onderwerp**

*Door deze verordening worden de vereisten vastgesteld die betaaldienstverleners in acht moeten nemen ten behoeve van de uitvoering van beveiligingsmaatregelen die hen in staat stellen het volgende te doen:*

- a)toepassen van de procedure voor sterke cliëntauthenticatie in overeenstemming met artikel 97 van Richtlijn (EU) 2015/2366;*
- b)vrijstellen van de toepassing van de beveiligingsvereisten voor sterke cliëntauthenticatie, afhankelijk van nader omschreven en beperkte voorwaarden op basis van de omvang van het risico, het bedrag en de recurrentie van de betalingstransactie en het voor de uitvoering van de betalingstransactie gebruikte betalingskanaal;*
- c)beschermen van de vertrouwelijkheid en de integriteit van de persoonlijke beveiligingsgegevens (credentials) van de betaaldienstgebruiker;*
- d)vaststellen van gemeenschappelijke en veilige open standaarden voor de communicatie tussen rekeninghoudende betaaldienstverleners, betaalinitiatiedienstverleners, rekeninginformatiedienstverleners, betalers, betalingsbegunstigden en andere betaaldienstverleners met betrekking tot het verlenen en het gebruik van betaaldiensten uit hoofde van titel IV van Richtlijn (EU) 2015/2366.*

---

<sup>1</sup> Gedelegeerde Verordening (EU) 2018/389 van de Commissie van 27 november 2017 tot invulling van Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad wat betreft technische reguleringsnormen voor sterke cliëntauthenticatie en gemeenschappelijke en veilige open communicatiestandaarden, PbEU 2018 L 69/23, te vinden op [www.eur-lex.europa.eu](http://www.eur-lex.europa.eu).

## Artikel 2

### Algemene authenticatievereisten

1. Betaaldienstverleners beschikken over mechanismen voor het monitoren van transacties waarmee zij ongeoorloofde of frauduleuze betalingstransacties voor de toepassing van de onder a) en b) van artikel 1 genoemde veiligheidsmaatregelen kunnen implementeren.

Die mechanismen zijn gebaseerd op de analyse van betalingstransacties, waarbij rekening wordt gehouden met elementen die typisch zijn voor de betaaldienstgebruiker in omstandigheden van normaal gebruik van de persoonlijke beveiligingsgegevens.

2. Betaaldienstverleners zorgen ervoor dat de mechanismen voor het monitoren van transacties ten minste met elk van de volgende risicofactoren rekening houden:

- a) lijsten van gecompromitteerde of gestolen authenticatie-elementen;
- b) het bedrag van elke betalingstransactie;
- c) bekende fraudescenario's bij het verlenen van betaaldiensten;
- d) tekenen van malwarebesmetting tijdens sessies van de authenticatieprocedure;
- e) ingeval de toegangsapparatuur of -software door de betaaldienstverlener wordt verstrekt, een gebruiksgelog van de aan de betalingsgebruiker verstrekte toegangsapparatuur of -software en het abnormale gebruik van de toegangsapparatuur of -software.

3.7 Hiermee is een directe monitoringsplicht opgelegd aan betaaldienstverleners (in dit geval de bank). De bank beschikt over informatie omtrent het gedrag van de specifieke betaaldienstgebruiker (de consument), het gedrag van de gemiddelde betaaldienstgebruiker en gevallen van ongeoorloofde betalingstransacties. Computerprogramma's stellen de bank in staat om die gegevens te analyseren en op basis van die analyse de kans dat een specifieke betalingstransactie ongeoorloofd is, te waarderen. De bank kan ingrijpen als die kans onaanvaardbaar groot is, bijvoorbeeld door uitvoering van een specifieke betaalopdracht op te schorten.<sup>2</sup>

3.8 Voor de commissie is niet duidelijk op welke wijze de bank invulling heeft gegeven aan deze verplichting. Op basis van welke criteria is het detectiesysteem van de bank op 13 augustus 2020 om 13.25 uur aangeslagen? Alvorens een eindoordeel te geven verzoekt de commissie de bank binnen vier weken na ontvangst van deze uitspraak een toelichting te geven op de op haar rustende monitoringsverplichting en hoe zij hier invulling aan heeft gegeven in het onderhavige geval.

---

<sup>2</sup> Zie ook R.E. Van Esch, Het innoverende karakter van PSD2 wat betreft zorgplichten van betaaldienstverleners jegens betaaldienstgebruikers, MvV 2018 nummer 7-8, p. 252.

De commissie verzoekt de bank daarbij nader in te gaan op de stelling van de consument dat met behulp van het fraudedetectiesysteem van de bank eerder dan op 13 augustus 2020 om 13.25 uur de rekening van de consument geblokkeerd had moeten worden door de bank gelet op de omstandigheden dat het ging om intensief gebruik van een niet eerder voor transacties gebruikte betaalkas, op verschillende locaties in binnen- en buitenland in een korte periode.

#### **4. De beslissing**

De commissie verzoekt de bank om binnen vier weken na ontvangst van deze tussenuitspraak een nadere toelichting te geven conform hetgeen is opgenomen in overweging 3.8. Daarna zal de consument in de gelegenheid worden gesteld hierop te reageren. De commissie houdt iedere verdere beslissing aan.

*Binnen twee weken na de verzenddatum van deze tussenuitspraak kunt u een schriftelijk verzoek indienen tot herstel van vergissingen in de uitspraak zoals schrijffouten, een verkeerde naam/datum of rekenfouten. De beslissing van de geschillencommissie in de tussenuitspraak kan hiermee niet ter discussie worden gesteld. Meer informatie hierover staat in artikel 40 van het reglement van de geschillencommissie, te vinden op de website [www.kifid.nl/reglementen-en-statuten](http://www.kifid.nl/reglementen-en-statuten).*

## **Bijlage - Relevante bepalingen uit wet- en regelgeving.**

### Bepalingen uit het Burgerlijk Wetboek (BW)

#### **Artikel 7:524 BW**

1. De betaaldienstgebruiker die gemachtigd is om een betaalinstrument te gebruiken,
  - a) gebruikt het betaalinstrument overeenkomstig de voorwaarden die op de uitgifte en het gebruik van het betaalinstrument van toepassing zijn, en
  - b) stelt de betaaldienstverlener, of de door laatstgenoemde gespecificeerde entiteit, onverwijld in kennis van het verlies, de diefstal of onrechtmatig gebruik van het betaalinstrument of van het niet-toegestane gebruik ervan.
2. Voor de toepassing van het eerste lid, onder a, neemt de betaaldienstgebruiker, zodra hij een betaalinstrument ontvangt, in het bijzonder alle redelijke maatregelen om de veiligheid van de persoonlijke beveiligingsgegevens ervan te waarborgen.
3. De voorwaarden bedoeld in het eerste lid, onderdeel a, zijn objectief, niet-discriminerend en evenredig.

#### **Artikel 7:525 BW**

- 1) De betaaldienstverlener die een betaalinstrument uitgeeft,
  - a) zorgt ervoor dat de persoonlijke beveiligingsgegevens van een betaalinstrument niet toegankelijk zijn voor andere partijen dan de betaaldienstgebruiker die gerechtigd is het betaalinstrument te gebruiken, onverminderd artikel 524;(...)
- 2) De betaaldienstverlener draagt het risico van het zenden aan de betaler van een betaalinstrument en van de gepersonaliseerde veiligheidskenmerken daarvan.

#### **Artikel 7:529 BW**

1. De betaler draagt alle verliezen die uit niet-toegestane betalingstransacties voortvloeien, indien deze zich hebben voorgedaan doordat hij frauduleus heeft gehandeld of opzettelijk of met grove nalatigheid een of meer verplichtingen uit hoofde van artikel 524 niet is nagekomen.
2. In gevallen waarin de betaler, zonder frauduleus of opzettelijk te hebben gehandeld, zijn verplichtingen uit hoofde van artikel 524 niet is nagekomen, kan de rechter de in het eerste lid van dit artikel bedoelde aansprakelijkheid beperken, met name rekening houdend met de aard van de persoonlijke beveiligingsgegevens van het betaalinstrument en met de omstandigheden waarin het is verloren, gestolen of onrechtmatig gebruikt.
3. Indien de betaaldienstverlener van de betaler geen sterke cliëntauthenticatie verlangt, draagt de betaler geen financiële verliezen, tenzij de betaler frauduleus heeft gehandeld. Indien de sterke cliëntauthenticatie door de begunstigde of de betaaldienstverlener van de begunstigde niet wordt aanvaard, wordt de door de betaaldienstverlener van de betaler geleden financiële schade door hen vergoed.
4. Na de kennisgeving overeenkomstig artikel 524, eerste lid, onder b, heeft het gebruik van het betaalinstrument geen financiële gevolgen voor de betaler, tenzij deze frauduleus heeft gehandeld.

*5. Indien de betaaldienstverlener nalaat om overeenkomstig artikel 525, eerste lid, onder c, passende middelen beschikbaar te stellen waarmee te allen tijde een kennisgeving als bedoeld in artikel 524, eerste lid, onder b, kan worden gedaan, is de betaler niet aansprakelijk voor de financiële gevolgen die uit het gebruik van dat betaalinstrument voortvloeien, tenzij hij frauduleus heeft gehandeld.”*