Uitspraak Geschillencommissie Kifid nr. 2025-0113

(mr. dr. ing. A.J. Verdaas, voorzitter en mr. Y.A. Gottenbos, secretaris)

Datum uitspraak	12 februari 2025
Klacht van	De consument
Tegen	International Card Services B.V., gevestigd te Amsterdam, verder te noemen ICS
Aard uitspraak	Bindend advies
Uitkomst	Vorderingen afgewezen
Bijlage	Relevante bepalingen uit wet- en regelgeving en uit de algemene voorwaarden

Samenvatting

Niet-toegestane betalingstransacties. De consument is slachtoffer geworden van oplichting. Een oplichter heeft zijn creditcard toegevoegd aan een Apple Pay-Wallet en heeft betalingen verricht ten laste van zijn rekening. De consument vordert vergoeding van de schade. De commissie overweegt dat de consument onvoldoende inzicht heeft gegeven in de wijze waarop een oplichter betalingen ten laste van zijn rekening heeft kunnen doen. Dit leidt ertoe dat ICS de schade niet hoeft te vergoeden. De vordering wordt afgewezen.

1. Procedure

1.1 De behandelend commissie, verder te noemen de commissie, beslist op basis van het 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 ICS; 3) de repliek van de consument en 4) de dupliek van ICS.

1.2 ICS is in deze zaak vertegenwoordigd door ABN AMRO Bank N.V.

1.3 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.

1.4 De consument en ICS 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 heeft een creditcardrekening bij ICS. Op de overeenkomst tussen de consument en ICS zijn de Algemene Card-voorwaarden ABN AMRO en ABN AMRO MeesPierson (hierna: de algemene voorwaarden) van toepassing. De relevante bepalingen uit de algemene voorwaarden zijn opgenomen in de bijlage bij deze uitspraak.

2.2 Op 6 december 2023 heeft de consument zijn creditcard toegevoegd aan de Apple Pay-Wallet op zijn telefoon.

2.3 Op diezelfde dag heeft een derde (hierna: de oplichter) de creditcard van de consument toegevoegd aan een Apple Pay-Wallet, waarbij de oplichter het nummer, de vervaldatum en de CVC-code van de creditcard van de consument heeft ingevuld. Daarbij heeft de oplichter een verificatiecode ingevuld, die per sms-bericht was verzonden naar het telefoonnummer van de consument.

2.4 Op 14 december 2023 zijn meerdere transacties verricht ten laste van de creditcardrekening van de consument via Apple Pay. In totaal is een bedrag van € 19.792,67 afgeschreven.

2.5 Op 22 december 2023 heeft de consument aangifte van fraude gedaan bij de politie.

De klacht en vordering

2.6 De consument vordert een schadevergoeding van € 19.792,67, te vermeerderen met de wettelijke rente vanaf 5 juni 2024. Ook vordert de consument dat ICS het proces om een creditcard in een Apple Pay-Wallet op te nemen aanpast en degelijker maakt. Aan deze vorderingen legt de consument – kort weergegeven – het volgende ten grondslag.

2.7 Het proces om een creditcard in een Apple Pay-Wallet op te nemen is onveilig. De gegevens van de creditcard moeten worden ingevuld in de Wallet waarna een verificatie-code bij ICS moet worden aangevraagd. ICS verstuurt deze verificatiecode per sms. Dit is onveilig. Het is namelijk kinderlijk eenvoudig om sms-berichten te onderscheppen.

2.8 In het geval van de consument heeft de oplichter de creditcardgegevens kunnen bemachtigen doordat de consument die gegevens heeft ingevuld op een website die waarschijnlijk frauduleus was. Daarnaast heeft de oplichter de via sms verstuurde verificatiecode blijkbaar onderschept. De consument kan niet aangeven hoe oplichters dit in zijn geval precies hebben gedaan. De consument heeft de verificatiecode niet zelf gedeeld met de oplichter.

2.9 Daarbij heeft ICS binnen één minuut twee verificatiecodes verstuurd naar het telefoon-nummer van de consument die allebei een half uur geldig waren. Dit lijkt onjuist. De consument heeft de tweede verificatiecode gebruikt om de creditcard in de Wallet op zijn eigen telefoon op te nemen. Als ICS had geregeld dat met het verstrekken van de tweede verificatiecode de eerder verstuurde verificatiecode onbruikbaar was geworden, dan was er mogelijk niets gebeurd.

2.10 Ook heeft ICS de consument geen instructies, waarschuwingen en attentiepunten gestuurd over het proces om een creditcard in de Apple Pay-Wallet op te nemen. Het proces is niet beschreven. Daardoor is het proces voor de consument niet te monitoren. Dat hij na het opnemen van de creditcard een bevestigingsmail zou ontvangen met “Gelukt! Uw Card staat in uw Apple Wallet” was voor de consument onbekend.

De twee bevestigingsmails die ICS heeft gestuurd nadat de consument en de oplichter de creditcard hadden opgenomen in de Apple Pay-Wallets, zijn in de spambox van de e-mail van de consument gekomen. Als de consument had geweten dat er een bevestigingsmail zou komen, dan zou hij alerter zijn geweest en zijn spambox in de gaten hebben gehouden. Dan zou hij hebben gereageerd op de twee bevestigingsmails en ICS hebben gebeld.

2.11 Verder komt de oplichting zoals in het geval van de consument exact overeen met een vorm van oplichting die is sinds mei 2022 is beschreven op een website. De consument begrijpt niet waarom ICS bij het mogelijk maken van het opnemen van creditcards in een Apple Pay-Wallet in december 2023 geen extra maatregelen heeft genomen om deze vorm van oplichting, die anderhalf jaar eerder al is opgetreden, te voorkomen.

2.12 Verder begrijpt de consument niet waarom de creditcardrekening niet na enkele transacties door ICS is geblokkeerd. De consument woont in Nederland. Bij een in Nederland wonende rekeninghouder die in Brazilië binnen korte tijd voor duizenden euro's aan transacties doet zouden bij het monitoringssysteem de alarmbellen moeten afgaan.

2.13 Ook heeft ICS een verzoek van de consument in 2016 om zijn limiet te verlagen niet uitgevoerd. De consument wist dit en heeft dat niet erg gevonden, want het was een heel gedoe geweest om de limiet op € 20.000,- te krijgen en te houden. Maar ICS heeft de consument niet gewezen op de hoge limiet en niet gevraagd of die niet wat naar beneden kon.

2.14 De consument voert verder een juridische analyse van een door hem ingeschakelde advocaat aan. De consument vat de conclusies van de advocaat als volgt samen:
- De betalingstransacties moeten worden aangemerkt als niet-toegestane betalings-transacties.
- ICS heeft geen bewijs geleverd van enig frauduleus handelen of opzettelijk dan wel met grove nalatigheid niet nakomen van veiligheidsvoorschriften.
- Een voor de consument geldende verzwaarde stelplicht kan niet verder strekken dan de informatie waarover de consument beschikt en heeft nooit betrekking op gegevens waarover de consument niet beschikt of kan beschikken.
- Een verzwaarde stelplicht is in dit soort zaken strijdig met de Europese Payments Services Directive (hierna: PSD2 richtlijn).[1]
- De consument heeft ruimschoots voldaan aan de verzwaarde stelplicht.
- Het bewijsrisico blijft bij ICS.
- ICS dient het bedrag van de betalingstransacties aan de consument te vergoeden, te vermeerderen met de wettelijke rente daarover vanaf 5 juni 2024.

[1] Richtlijn (EU) 2015/2366 van het Europees Parlement en de Raad van 25 november 2015.

Het verweer

2.15 ICS voert verweer tegen de stellingen van de consument. Voor zover relevant zal de commissie bij de beoordeling daarop ingaan.

3. De beoordeling

Waar het om gaat

3.1 De commissie merkt op dat zij het betreurt dat de consument slachtoffer is geworden van oplichting en dat hij daardoor schade heeft geleden. Dit staat evenwel los van de taak van de commissie om te onderzoeken of ICS juridisch gezien verplicht is de schade die hij heeft geleden te vergoeden. De commissie komt tot het oordeel dat ICS de schade niet hoeft te vergoeden en licht dat hieronder toe.

Niet-toegestane betalingstransacties

3.2 Tussen partijen is niet in geschil dat de consument niet heeft ingestemd met de betalingstransacties. Een transactie waarmee de consument niet heeft ingestemd, wordt volgens artikel 7:522 lid 2 van het Burgerlijk Wetboek (hierna: BW) als niet-toegestaan aangemerkt. Op grond van artikel 7:528 lid 1 BW moet een betaaldienstverlener in geval van een niet-toegestane betalingstransactie de consument onmiddellijk het bedrag van de niet-toegestane betalingstransactie terugbetalen. Op die regel bestaat een uitzondering. Volgens artikel 7:529 lid 1 BW hoeft ICS de niet-toegestane betalingstransacties niet terug te betalen als de consument frauduleus heeft gehandeld of in juridische zin opzettelijk of met grove nalatigheid één of meer verplichtingen uit hoofde van artikel 7:524 BW niet is nagekomen.[2] Volgens artikel 7:524 lid 1 BW moet de consument een betaalinstrument gebruiken overeenkomstig de voorwaarden die op het gebruik daarvan van toepassing zijn.

3.3 In artikel 5 van de algemene voorwaarden zijn bepalingen opgenomen die betrekking hebben op de veiligheid van de rekening. Daarin is onder meer opgenomen dat persoonlijke beveiligingscodes met betrekking tot de creditcard, niet alleen de pincode maar ook andere codes zoals een sms-code, alleen door de consument mogen worden gebruikt en dat hij persoonlijke beveiligingscodes moet geheimhouden. De commissie moet beoordelen of de consument – in juridische zin – grof nalatig heeft gehandeld met betrekking tot het naleven van deze veiligheidsvoorschriften.

Grove nalatigheid

3.4 Hoewel het aan ICS is om te bewijzen dat de consument grof nalatig heeft gehandeld, rust volgens de vaste lijn van de commissie op de consument een verzwaarde stelplicht.[3]

---

[2] Commissie van Beroep, nr. 2020-027.
[3] Geschillencommissie Kifid, nrs. 2024-0124, 2019-308 en 2019-733.

Deze verzwaarde stelplicht hangt samen met de omstandigheid dat de door ICS te stellen feiten zich afspelen in het domein van de consument. Dat betekent dat de consument enig inzicht moet geven in de wijze waarop zijn creditcardgegevens en de aan hem via sms verstrekte verificatiecode bij de oplichter zijn terechtgekomen. De consument kan niet volstaan met een onvoldoende onderbouwde betwisting dat hij niet weet hoe de oplichter de beschikking heeft verkregen over zijn gegevens. Een andere regel zou betaaldienst-verleners voor onaanvaardbare risico's van misbruik plaatsen.

3.5 De consument heeft zich onder verwijzing naar de door hem aangevoerde juridische analyse van de advocaat op het standpunt gesteld dat het aannemen van een verzwaarde stelplicht in strijd is met de PSD2 richtlijn. De advocaat heeft in die analyse onder meer gewezen op overweging 72 van de preambule van de PSD2 richtlijn[4] en heeft geschreven dat het aannemen van een verzwaarde stelplicht in specifieke situaties, zoals bij online-betalingen, afbreuk zou doen aan de bewijslast van ICS. De commissie volgt het standpunt niet aangezien de bewijslast bij ICS blijft bij het aannemen van een verzwaarde stelplicht voor de consument.

3.6 ICS heeft toegelicht dat voor het koppelen van een creditcard aan Apple Pay het nummer van de creditcard, de vervaldatum van de creditcard en de veiligheidscode van de creditcard moeten worden opgegeven in de Apple Pay-Wallet. Daarnaast wordt per sms een verificatiecode gestuurd naar het bij ICS bekende telefoonnummer van de consument. Die moet worden ingevoerd in de Wallet op de telefoon waar de creditcard aan wordt toegevoegd. In de sms wordt erop gewezen fraude te voorkomen en de verificatiecode alleen in de eigen Apple Pay-Wallet te gebruiken. ICS stelt dat de consument zich niet aan de voorwaarden heeft gehouden door de verificatiecode, die ICS enkel en alleen aan de consument heeft gestuurd, kenbaar te maken aan de oplichter. Volgens ICS heeft de consument grof nalatig gehandeld. Er is immers geen andere mogelijkheid denkbaar dan dat door toedoen van de consument de strikt persoonlijke verificatiecode bij een oplichter terecht is gekomen, aldus ICS.

3.7 De commissie is van oordeel dat de consument, gelet op de verzwaarde stelplicht, onvoldoende tegenover de toelichting van ICS heeft gesteld. De consument heeft verklaard dat de oplichter zijn creditcardgegevens heeft kunnen bemachtigen doordat de consument die gegevens heeft ingevuld op een website die waarschijnlijk frauduleus was. De consument heeft echter onvoldoende inzicht gegeven in de wijze waarop de verificatiecode bij een oplichter bekend is geworden.

3.8 De consument heeft aangevoerd dat de via sms verstuurde verificatiecode is onderschept door de oplichter. Volgens de consument is het eenvoudig om een sms te onderscheppen. Hij heeft dit onderbouwd met artikelen op diverse websites.

[4] De tekst van overweging 72 van de preambule van de PSD2 richtlijn is opgenomen in de bijlage bij deze uitspraak.

ICS heeft hiertegen ingebracht dat bij het lezen van die artikelen blijkt dat het helemaal niet zo simpel en eenvoudig is om een sms-bericht te onderscheppen. Dit is namelijk enkel mogelijk in het geval dat de consument op enige wijze zogenoemde malwarebots heeft binnengehaald of wanneer op de mobiele telefoon van de consument een app is geïnstalleerd om sms-berichten te onderscheppen, zo stelt ICS.

3.9 Naar het oordeel van de commissie blijkt uit de tekst van de artikelen niet dat een sms-bericht zonder enige handeling van de consument kan worden onderschept. In de artikelen worden mogelijkheden genoemd waarop een sms-bericht kan worden onderschept, maar de consument heeft niet toegelicht op welke wijze het bericht in dit geval zou zijn onderschept. De stelling van de consument dat hij niet kan aangeven hoe in zijn geval de verificatiecode is onderschept en dat hij alle feiten waarover hij beschikt of kan beschikken heeft verstrekt, maakt niet dat de consument heeft voldaan aan de verzwaarde stelplicht. Een andere oorzaak dan dat de verificatiecode door een handeling van de consument in handen van de oplichter kon komen, is niet aannemelijk. Het is dan ook aan de consument om enig inzicht te geven in de wijze waarop de aan de consument verstuurde verificatie-code in handen van de oplichter is gekomen.

3.10 Hoe een oplichter de verificatiecode heeft kunnen bemachtigen en de creditcard aan een Apple Pay-Wallet kon toevoegen is onduidelijk gebleven. Zoals hiervoor is overwogen is het aan de consument om hier enig inzicht in te geven. Nu de consument dit niet heeft gedaan, heeft hij niet voldaan aan zijn verzwaarde stelplicht. Het gevolg hiervan is dat de commissie concludeert dat de consument onvoldoende zorgvuldigheid heeft betracht waardoor een oplichter de verificatiecode heeft bemachtigd en in de gelegenheid is geweest om de creditcard aan een Apple Pay-Wallet toe te voegen. Dit leidt tot het oordeel dat moet worden aangenomen dat de consument de verplichtingen voor het veilige gebruik van de rekening zoals opgenomen in de voorwaarden niet is nagekomen. Derhalve concludeert de commissie dat de consument in juridische zin grof nalatig heeft gehandeld en dat ICS de geleden schade op grond van artikel 7:529 lid 1 BW niet aan de consument hoeft te vergoeden.

3.11 Op grond van artikel 7:529 lid 2 BW kan de aansprakelijkheid van de consument worden beperkt als de omstandigheden van het geval daartoe aanleiding geven. De commissie ziet in dit geval geen aanleiding om van die mogelijkheid gebruik te maken.

Veiligheidsmaatregelen

3.12 De consument heeft gesteld dat ICS onvoldoende veiligheidsmaatregelen heeft genomen om de oplichting te voorkomen.

3.13 ICS heeft toegelicht dat voor het koppelen van een creditcard aan Apple Pay het nummer, de vervaldatum en de CVC-code van de creditcard moeten worden opgegeven. Daarnaast wordt per sms een verificatiecode gestuurd naar het telefoonnummer van de consument die moet worden ingevoerd op de iPhone waar de creditcard aan wordt toegevoegd.

Naar het oordeel van de commissie heeft ICS hiermee voldoende veiligheidsmaatregelen genomen om te voorkomen dat een oplichter de creditcard kon toevoegen aan een Apple Pay-Wallet. Zoals hiervoor ook al is overwogen, is het de commissie niet gebleken dat het zonder handeling van de consument mogelijk is om een sms-bericht te onderscheppen. Dat het versturen van de verificatiecode per sms onveilig zou zijn is niet gebleken.

3.14 De consument heeft aangevoerd dat de vorm van oplichting waarvan hij slachtoffer is geworden in mei 2022 al op een website is beschreven. De commissie overweegt dat onduidelijk is gebleven hoe de oplichter de creditcard aan een Apple Pay-Wallet kon toevoegen. Daarom kan de commissie, nog los van de vraag of ICS hiertegen extra maatregelen had kunnen en moeten nemen, niet vaststellen dat in het geval van de consument sprake was van dezelfde vorm van oplichting zoals die op de website van mei 2022 waarnaar de consument verwijst staat beschreven.

3.15 De consument heeft verder nog naar voren gebracht dat ICS binnen één minuut twee verificatiecodes heeft gestuurd die beiden een half uur geldig waren. ICS heeft gesteld dat een aantal minuten zat tussen het versturen van de eerste verificatiecode en de tweede verificatiecode. Naar het oordeel van de commissie maakt de stelling van de consument dat ICS binnen één minuut twee verificatiecodes heeft gestuurd niet dat ICS onvoldoende veiligheidsmaatregelen heeft genomen. De verificatiecodes moeten immers volgens de algemene voorwaarden worden geheimgehouden en alleen door de consument in de eigen Apple Pay-Wallet worden gebruikt. Ook de stelling van de consument dat hij niet is geïnformeerd over het proces voorafgaand en tijdens het proces, leidt niet tot de conclusie dat ICS in dit geval onvoldoende veiligheidsmaatregelen heeft genomen.

3.16 De commissie concludeert dat niet is komen vast te staan dat ICS in dit geval onvoldoende veiligheidsmaatregelen heeft genomen om de oplichting te voorkomen.

Monitoringsplicht

3.17 De consument heeft verder gesteld dat de alarmbellen hadden moeten afgaan bij ICS op het moment dat de transacties werden verricht. Daarvoor geldt het volgende. Op ICS rust geen algemene monitoringsplicht. Op ICS rust wel een zorgplicht, die kort gezegd inhoudt dat zij rekening dient te houden met de gerechtvaardigde belangen van de rekeninghouder. De reikwijdte van deze zorgplicht hangt af van de omstandigheden van het geval.

3.18 Volgens de vaste lijn van de commissie mag van ICS worden verwacht dat zij zich inspant om fraude en misbruik van het betalingsverkeer te voorkomen.[5] Deze zorgplicht strekt echter niet zover dat ICS gehouden is om in het algemeen betalingstransacties te monitoren. Een algemene monitoringsverplichting zou het proces van geautomatiseerde gegevensverwerking en het maatschappelijk belang dat daarmee gediend is, kunnen schaden.

[5] GC Kifid 2016-602.

Wel kan van ICS worden verwacht dat zij tot onderzoek overgaat als zij weet van ongebruikelijk betalingsverkeer en het daaraan verbonden gevaar. Bepalend is datgene waarvan ICS zich daadwerkelijk bewust was.[6]

3.19 In dit geval is niet gesteld en ook niet gebleken dat ICS wist dat de consument werd opgelicht. Dat de transacties voor de consument mogelijk ongebruikelijk waren, maakt niet dat ICS wist dat de consument werd opgelicht. Omdat ICS zich niet bewust was van een gevaar en dat ook niet hoefde te zijn, was er voor ICS ook geen verplichting om de rekening te blokkeren of op andere wijze actie te ondernemen.

Limiet van de creditcard

3.20 De consument heeft verder nog gesteld dat ICS een in 2016 gedaan verzoek om de bestedingslimiet te verlagen niet heeft doorgevoerd. ICS heeft aangegeven dat dit verzoek inderdaad niet is doorgevoerd. De consument heeft aangegeven dat hij wist dat hij een limiet had met € 20.000,- en dat hij het niet erg vond dat ICS het verzoek niet had doorgevoerd. De commissie volgt het standpunt van ICS dat, als de consument een lagere limiet had gewild dan € 20.000,-, het op de weg van de consument had gelegen om hierover opnieuw contact op te nemen met ICS. Verder hoefde ICS de consument niet te vragen of de bestedingslimiet omlaag kon en ook niet te wijzen op het risico van een bestedingslimiet van € 20.000,-.

3.21 De consument heeft nog gesteld dat zijn Private Banker van ABN AMRO MeesPierson, onderdeel van ABN AMRO Bank N.V., hem niet heeft gewezen op het risico van de bestedingslimiet van € 20.000,-. De commissie overweegt dat deze klachtzaak tegen ICS, en niet tegen ABN AMRO Bank N.V. wordt gevoerd. Daarom zal de commissie in deze zaak niet oordelen over deze stelling.

Conclusie

3.22 De conclusie is dat de klacht van de consument ongegrond is. De vorderingen worden dan ook afgewezen.

Ambtshalve toetsing

3.23 Voor de beoordeling van de klacht is artikel 5 van de algemene voorwaarden van belang. Dit beding is door de commissie getoetst aan het Europese en Nederlandse (consumenten)-recht waarvoor ambtshalve toetsing geldt en de commissie acht het beding niet in strijd met deze regelgeving.

[6] Zie Hoge Raad 27 november 2015, ECLI:NL:HR:2015:3399.

4. De beslissing

De commissie wijst de vorderingen af.

Deze uitspraak is bindend. Of u tegen deze uitspraak beroep kunt instellen, kunt u nalezen in regel 7 van het Reglement Commissie van Beroep Kifid – vanaf 1 oktober 2023, te vinden op de website www.kifid.nl/reglementen-en-statuten. In regel 18.1 van dat reglement is bepaald dat beroep kan worden ingesteld tot 6 weken na de dag van deze uitspraak. Meer informatie over het instellen van beroep kunt u vinden op de website www.kifid.nl/in-beroep-gaan-bij-kifid.

Binnen 2 weken na verzending van de uitspraak kunt u schriftelijk verzoeken een overduidelijke vergissing in de uitspraak zoals een schrijffout, een verkeerde naam/datum of een rekenfout te herstellen. De beslissing in de uitspraak kan hiermee niet ter discussie worden gesteld. Ook kunt u binnen 2 weken na verzending van de uitspraak schriftelijk verzoeken de uitspraak aan te vullen als u vindt dat niet op alle onderdelen van uw vordering is beslist. Dit ziet niet op de situatie waarin u meent dat de Geschillencommissie Kifid niet op al uw argumenten is ingegaan. Meer informatie hierover staat onder vraag 58 en 59 van het Reglement Geschillencommissie Kifid – vanaf 1 april 2024, te vinden op de website www.kifid.nl/reglementen-en-statuten.

Contactgegevens Klachteninstituut financiële dienstverlening

Telefoonnummer: 070 - 333 8 999
Website: www.kifid.nl

Bijlage - Relevante bepalingen uit wet- en regelgeving en uit de algemene voorwaarden

Algemene Card-voorwaarden ABN AMRO en ABN AMRO MeesPierson

Artikel 5. Pincode en geheimhouding

5.1. Uw Card heeft een pincode. Deze pincode heeft u zelf gekozen of is automatisch aan u toegekend. De pincode is net zoals uw Card persoonlijk en mag alleen door u worden gebruikt. Wij kunnen instructies geven over het kiezen van de pincode. Deze moet u opvolgen.
5.2. U mag het document waarmee de pincode aan u wordt toegestuurd niet bewaren. U mag de pincode niet noteren op uw Card of op een document dat u bij uw Card bewaart. Als u al een aantekening maakt van de pincode, dan moet u dit zo doen dat de pincode niet voor anderen herkenbaar is of dat duidelijk is waar de pincode voor is.
5.3. U moet de pincode geheimhouden voor iedereen, ook voor familieleden, huisgenoten en onze medewerkers. U moet ervoor zorgen dat anderen niet kunnen meekijken wanneer u de pincode intoetst.
5.4. Ook andere persoonlijke beveiligingscodes met betrekking tot uw Card, zoals een inlognaam, een wachtwoord, e-Code of SMS Code mogen alleen door u worden gebruikt en moet u geheimhouden.

Overweging 72 van de preambule bij richtlijn 2015/2366/EU

72. Om te kunnen beoordelen of er bij de betalingsdienstgebruiker sprake was van nalatigheid of grove nalatigheid moeten alle omstandigheden in aanmerking worden genomen. In de regel moeten het bewijs voor en de mate van de beweerde nalatigheid volgens het nationale recht worden beoordeeld. Terwijl het begrip nalatigheid een schending van de zorgplicht inhoudt, dient een grove nalatigheid echter meer dan louter nalatigheid in te houden, en dus gedrag dat een aanzienlijke mate van onvoorzichtigheid vertoont; bijvoorbeeld het bewaren van de voor het verlenen van toestemming voor een betalingstransactie gebruikte beveiligingsgegevens naast het betaalinstrument in een open en voor derden gemakkelijk op te sporen formaat. Contractuele clausules en voorwaarden met betrekking tot de verstrekking en het gebruik van een betaalinstrument die de bewijslast voor de consument vergroten of de bewijslast voor de uitgever verminderen, moeten als nietig worden beschouwd. In specifieke situaties en met name wanneer het betaalinstrument niet aanwezig is op het verkooppunt, zoals bij onlinebetalingen, is het voorts passend dat het bewijs van de beweerde nalatigheid door de betalingsdienstaanbieder moet worden geleverd, aangezien de betaler slechts zeer beperkte middelen heeft om in zulke gevallen het tegendeel te bewijzen.

Boek 7 van het Burgerlijk wetboek

Artikel 522

1. Een betaaldienstverlener voert een betalingstransactie slechts uit met instemming van de betaler met de uitvoering van de betaalopdracht.
2. De instemming met een betaalopdracht wordt verleend overeenkomstig de tussen de betaler en zijn relevante betaaldienstverlener(s) overeengekomen vorm en procedure. De instemming met de uitvoering van een betalingstransactie kan ook worden verleend via de begunstigde of de betaalinitiatiedienstverlener. Bij gebreke van een dergelijke instemming wordt een betalingstransactie als niet toegestaan aangemerkt.
3. De instemming kan te allen tijde, doch uiterlijk op het tijdstip van het onherroepelijk worden, krachtens artikel 534 van de betaalopdracht door de betaler worden ingetrokken. Hetzelfde geldt voor een instemming met de uitvoering van een betaalopdracht betreffende een reeks betalingstransacties, die kan worden ingetrokken met als gevolg dat iedere toekomstige betalingstransactie als niet-toegestaan wordt aangemerkt.

Artikel 524

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, onder a, zijn objectief, niet-discriminerend en evenredig.

Artikel 528

1. Onverminderd artikel 526, betaalt de betaaldienstverlener de betaler, in geval van een niet-toegestane betalingstransactie, de betaler onmiddellijk het bedrag van de niet-toegestane betalingstransactie terug en in elk geval uiterlijk aan het einde van de eerstvolgende werkdag, nadat hij bekend is geworden met de transactie of daarvan in kennis is gesteld.
   (...)

Artikel 529

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.
(...)