Uitspraak Geschillencommissie Financiële Dienstverlening nr. 2022-0141
(mr. dr. D.P.C.M. Hellegers, voorzitter, mr. J. van der Groen, mr. F.H.E. Boerma, leden en mr. M.A. Kleijer, secretaris)

Klacht ontvangen op	: 10 november 2020
Ingediend door	: De consument
Tegen	: Coöperatieve Rabobank U.A., gevestigd te Amsterdam, verder te noemen de bank
Datum uitspraak	: 23 februari 2022
Aard uitspraak	: Bindend advies
Uitkomst	: Vordering afgewezen
Bijlage	: Relevante bepalingen uit wet- en regelgeving / de algemene voorwaarden

Samenvatting

Bank. Fraude. De consument heeft gesteld slachtoffer te zijn geworden van (identiteits)fraude en daardoor schade te hebben geleden. De consument heeft de bank gevraagd hem daarin tegemoet te komen. De bank heeft dit verzoek afgewezen. De commissie is van oordeel dat voor een dergelijke tegemoetkoming geen aanleiding is. De klacht wordt ongegrond geacht en de daarop gebaseerde vordering wordt afgewezen.

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) de aanvullende stukken van de consument; 3) het verweerschrift van de bank 4) de repliek van de consument en 5) 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 (verder: rekening) voorzien van bankpas en pincode bij de bank aan. De consument maakt gebruik van de mobielbankieren app van de bank. Op deze contractuele relatie zijn toepasselijk de Algemene Voorwaarden betalen en online diensten van de Rabobank 2019 (verder: AV 2019) en de Algemene Bankvoorwaarden 2017 (verder: ABV). De relevante bepalingen zijn als bijlage bij deze uitspraak opgenomen.

2.2 Op 15 mei 2020 heeft de consument een roodstand van € 1.000,- voor zijn rekening ingeregeld en heeft hij voor de periode 15 mei 2020 tot en met 21 mei 2020 de pinlimiet van zijn bankpas verhoogd. Op 16 mei 2020 is € 1.140,- bij een geldautomaat gepind.

2.3 Op 18 mei 2020 is via de persoonlijke internetbankomgeving van de consument een aanvraag voor een persoonlijke lening (verder: eerste PL) van € 5.000,- ingediend. De overige communicatie over deze aanvraag is via de persoonlijke internetomgeving van de consument verlopen. Zo heeft de consument op verzoek van de bank zijn meest recente en ondertekende arbeidsovereenkomst toegestuurd en op de vraag van de bank zijn woonsituatie toe te lichten, geantwoord. Uit de aanvraag volgde namelijk dat de consument huur betaalde terwijl uit de betaalrekening bleek dat de consument hypotheeklasten voldeed. De consument heeft geantwoord dat hij de vraag over zijn woonsituatie *'per ongeluk verkeerd* [heeft] *ingevuld en over het hoofd* [heeft] *gezien*'. De bank heeft vervolgens de eerste PL (20 mei 2020) verstrekt. Deze overeenkomst is door middel van een Raboscanner, de bankpas van de consument en de daarbij behorende pincode ondertekend.

2.4 Over het op 20 mei 2020 tussen de consument en de bank gevoerde telefoongesprek is in de administratie van de bank vermeld: *"(…)dhr wil 5000 opnemen bij automaat maar bij gea wordt pas geweigerd. Is vanwege aankoop auto vandaag. Oplossing: GEAlimiet is al verhoogd, pas actief. Dhr geadviseerd bij andere Rabo GEA te proberen en ook in kleinere hoeveelheden geld op te nemen. Nieuwe pas aanvragen duurt te lang omdat dhr geld vandaag nodig heeft."*

2.5 Over het op 23 mei 2020 tussen de consument en de bank gevoerde telefoongesprek is in de administratie van de bank vermeld: *"(…) Gesproken met* [naam consument, toevoeging commissie] *Klantvraag: klant geeft aan dat hij geld heeft overgemaakt naar vriendin (2170 euro), hierna is haar rekening geblokkeerd geraakt (Ze is klant bij XXX* [naam bank, toevoeging commissie]. *Meneer belt om door te geven dat XXX de rabobank gaat bellen hierover. Oplossing: Gezegd dat ik dit ga noteren."*

2.6 Op 25 mei 2020 is via de beveiligde internetomgeving van de consument een tweede persoonlijke lening (verder: tweede PL) van € 5.000,- aangevraagd. De bank heeft naar aanleiding van deze aanvraag telefonisch contact opgenomen met de consument en daarover in haar administratie vermeld: *"Dhr gesproken. Nu inboedel, recent auto. Geeft aan verder geen bijzonderheden. Alleenstaand is niet veranderd."* De bank heeft de aanvraag geaccordeerd. De vervolgens door de bank toegestuurde overeenkomst is door middel van de Raboscanner, de bankpas met de pincode van de consument ondertekend.

2.7 Over het door de consument met de bank op 25 mei 2020 gevoerde telefoongesprek is in de administratie van de bank vastgelegd: *"Gesproken met:* [naam consument] *Klantvraag: Klant geeft aan dat hij op 22-5 € 2170,- heeft overgemaakt naar een vriendin naar XXX* [naam bank, toevoeging commissie]. *Hij geeft aan dat de transactie in onderzoek is bij XXX en dat het bedrag daar niet is bijgeschreven Oplossing: Gesproken met een collega van transactiemonitoring. Klant aangegeven dat de rekeninghouder zelf met XXX contact dient op te nemen".*

2.8 Over het op 28 mei 2020 door de bank met de consument over mogelijke phishing gevoerde telefoongesprek heeft de bank in haar de administratie vermeld:
" Klant gebeld. hij geeft aan dat hij zaterdag al had gebeld omdat zijn vriendin niet bij haar geld kon. Ik zie nu dat er allemaal storno;s zijn. [naam consument] *geeft* [aan] *dat hij van niets weet en dat waarschijnlijk misschien zijn vader gedaan heeft. Hij heeft zijn pas bij zijn ouders laten liggen. Voor nu zijn rekening vrijgegeven. Ik belde voor betaling naar de XXX. Reden van de navraag: mogelijk phishing Opdrachtgever:* [rekeningnummer consument] [naam consument]: [rekeningnummer ontvanger]: *bedrag: 1.000,00 EUR 1.000,00 EUR 170,00 EUR Datum + tijdstip overboeking: <Datum +tijdstip. 22-05-2020".*

2.9 Tussen 16 mei 2020 en 1 juni 2020 werd de pinlimiet van de bankpas van de consument verschillende keren verhoogd.

2.10 Op 2 juni 2020 heeft de consument de bank verteld zijn bankpas te zijn kwijtgeraakt. De bank heeft hierop die bankpas ingetrokken, de rekening geblokkeerd en voor de consument een nieuwe bankpas met pincode aangevraagd. Op 5 juni 2020 hebben de consument en de bank elkaar over de kwijtgeraakte bankpas, de aangevraagde leningen, de betalingen aan een derde (zie hiervoor onder 2.8: "rekeningnummer ontvanger") en diverse opnames, waaronder de door de consument betwiste opnames, gesproken. De consument heeft over het verlies van zijn bankpas bij de politie aangifte gedaan en de bank het opgemaakte proces-verbaal toegestuurd.

2.11 Op 18 juni 2020 heeft de consument de bank telefonisch laten weten slachtoffer te zijn geworden van identiteitsfraude. In de administratie van de bank is hierover vermeld:
"Klant belt op met verhaal dat zijn slachtoffer is geworden van identiteitsfraude. Klant heeft onder bedreiging al zn gegevens, pas en pincode moeten afstaan. Het gaat om 2 persoonlijke rekeningen (beide 5000 euro) die niet met zijn medeweten/goedkeuring zijn afgesloten en een bedrag van in totaal 3900 euro bij GEA's in [plaats]. Inmiddels is alles geblokkeerd verwijderd en ontkoppeld. Oplossing: Klant komt morgen langs bij Lokale bank om dit verder af te handelen. Er is inmiddels aangifte gedaan.(…)" De consument heeft dit proces-verbaal ook aan de bank gegeven.

2.12 De consument heeft van de bank herinneringen ontvangen over de achterstand in de betaling van de maandbedragen van de twee persoonlijke leningen.

2.13 Nadat de bank het verzoek van de consument om compensatie van zijn schade heeft afgewezen, heeft de consument zijn klacht bij Kifid ingediend.

De klacht en vordering

2.14 De klacht van de consument valt uiteen in drie onderdelen. Ten eerste verwijt de consument dat de bank niet gemerkt heeft dat *"er iets niet klopte";* er werden namelijk storneringen uitgevoerd, diverse hoge bedragen gepind, betaald en overgemaakt. Ten tweede verwijt de consument de bank twee leningen te hebben afgesloten zonder daarvoor van hem een handtekening en legitimatiebewijs te vragen. Ten onrechte stelt de bank dat voor het afsluiten van een lening met een pincode of een telefoontje kan worden volstaan. Ten derde heeft de consument kritiek geuit over de bejegening door de bank nadat hij over de fraude openheid van zaken had gegeven.

2.15 De consument heeft verklaard over de manier waarop hij door de derde is bedreigd. De consument heeft toegelicht onder dwang zijn bankpas en pincode en overige persoonlijke bankgegevens te hebben afgegeven omdat, als hij niet zou meewerken, hem of zijn naasten iets zou worden aangedaan. De consument heeft hiervoor een flinke reis moeten ondernemen, omdat hij op 15 mei 2020 via Snapchat werd benaderd met de mededeling dat hij op 16 mei 2020 zijn pas en pincode in Utrecht moest inleveren. De consument heeft weliswaar zelf op 15 mei 2020 de roodstand voor zijn rekening ingeregeld en de pinlimiet van zijn bankpas verhoogd maar ook dat was in opdracht van de derde. De consument heeft verder uitgelegd dat het telefonisch contact met de bank verliep volgens de door de derde gegeven instructies. Zo heeft de consument bijvoorbeeld de vragen van de bank over de kredietaanvragen overeenkomstig de door de derde gegeven instructies beantwoord. De consument heeft vanuit angst voor mogelijke gevolgen bij de bank en de politie een valse verklaring afgelegd. Nadat de consument vanwege de door de derde uitgevoerde storneringen betalingsherinneringen bleef ontvangen, heeft hij uiteindelijk aan zijn familie alles opgebiecht en daarna de bank en de politie over de werkelijke gang van zaken geïnformeerd.

2.16 Wat de bejegening door de bank betreft heeft de consument opgemerkt dat de afhandeling van de fraude veel tijd heeft gekost. Dat de bank alleen na legitimatie informatie met hem wilde delen, heeft de consument zeer verbaasd omdat zonder legitimatie leningen zijn afgesloten. De consument heeft hieraan toegevoegd dat hem tijdens een bezoek aan de bank door een medewerker is verteld dat een lening alleen na het tonen van een legitimatiebewijs wordt verstrekt. Een procedure die, aldus de consument, ook op de website van de bank staat vermeld.

2.17 De consument vordert dat de bank zijn schade zal vergoeden.

Deze schade heeft de consument begroot op € 17.000,- , bestaande uit twee leningen ad € 5.000,-, de daarvoor verschuldigde rente begroot op € 2.000,-, de roodstand ad € 1.000,- en de door de derde(n) verrichte geldopnames.

Het verweer

2.18 De bank heeft verweer gevoerd tegen de stellingen van de consument. Voor zover relevant zal de commissie bij de beoordeling daarop ingaan.

3. De beoordeling

Inleiding

3.1 De vraag die de commissie dient te beoordelen is, kort gezegd, of de bank als betaaldienstverlener de door de consument geleden schade moet vergoeden. De commissie is van oordeel dat de bank hiertoe niet verplicht kan worden. Dit oordeel wordt hieronder toegelicht. De in dit verband relevante wet- en regelgeving is in de bijlage opgenomen.

Niet-toegestane transacties/grove nalatigheid

3.2 Vaststaat dat de consument zijn bankpas, pincode en overige persoonlijke bankgegevens aan een derde heeft afgegeven. De consument heeft aangevoerd dit onder bedreiging te hebben gedaan, maar heeft de bank daarover niet- terstond en dus tijdig- ingelicht. Een handelwijze die, zoals door de bank onweersproken is gesteld, in de zin van de wet als 'grof nalatig' moet worden gekwalificeerd (zie artikel 7:524 BW). In een dergelijke situatie is in de wet bepaald (zie artikel 7:529 lid 1 BW) dat de consument alle verliezen draagt die uit niet-toegestane transacties voortvloeien.

Monitoringsplicht in relatie tot de aard van de transacties

3.3 De consument is het hiermee niet eens en is van mening dat de bank hem moet compenseren omdat de bank haar monitoringsplicht jegens hem niet is nagekomen. De bank heeft deze stelling gemotiveerd betwist en aangevoerd dat een dergelijke monitoringsplicht alleen dan opgaat als de bank zich daadwerkelijk bewust was van het ongebruikelijke betalingsverkeer en het daaraan verbonden gevaar [1] en daarbij verwezen naar eerdere uitspraken van de commissie[2]. De commissie oordeelt als volgt.

3.4 De transactiemonitoringsplicht geldt wanneer de bank wist van het ongebruikelijk betalingsverkeer. [3] Bij een dergelijke subjectieve wetenschap zou een bank verplicht kunnen worden te waarschuwen voor de transacties. De verplichting om transacties in zijn algemeenheid te controleren bestaat echter niet.

---

[1] Zie Hoge Raad 27 november 2015 ECLI:NL:HR:2015:3399.
[2] Zie Geschillencommissie Kifid nrs. 2020-940, 2019-882 en 2019-759.
[3] Zie Hoge Raad 27 november 2015 ECLI:NL:HR:2015:3399.

Dat de bank wist dat er iets niet in de haak was, is niet gebleken. De bank wist niet dat de consument zijn pas en pincode aan een derde had afgestaan. Daarbij komt dat het de consument is geweest die met de bank telefonisch contact heeft opgenomen over bepaalde transacties, zie hetgeen daarover onder 2.4 (geldopname GEA), 2.5 (geblokkeerde rekening begunstigde), 2.7 (overboeking waarbij rekening begunstigde in onderzoek is) en 2.8 (contact vanwege mogelijke phishing en vraag over storno's) is vermeld. Zoals door de bank is aangevoerd dient indachtig de vaste lijn in de uitspraken van de commissie[4] dit verwijt van de consument te worden afgewezen. Dat de consument daarbij op instructie van de derde handelde kan in dit geval niet tot een ander oordeel leiden.

Persoonlijke leningen

3.5 De bank heeft toegelicht dat de twee leningen tot stand zijn gekomen overeenkomstig de tussen partijen gemaakte afspraken over de elektronische handtekening en daarbij verwezen naar artikel 8 van de ABV en artikel 13 lid 2 van de AV 2019. De commissie stelt vast dat de consument deze gemaakte afspraken niet heeft bestreden. Dit betekent dat de consument zijn uit de leningen voortvloeiende verplichtingen jegens de bank dient na te komen. Hierbij wordt van belang geacht dat de bank gedurende de aanvraagprocedures van de beide leningen contact met de consument heeft opgenomen en daaruit niet kon afleiden dat de consument die leningen onder dwang afsloot. Daarbij wist de bank niet en kon dit ook niet weten dat de consument zijn bankpas en de pincode had afgegeven aan de derde. Dat er 'iets niet klopte', kon dan ook niet door de bank worden opgemerkt. De commissie is met de bank van oordeel dat hetgeen door de consument over diens legitimatie in de bankhal (zie hiervoor onder 2.16) heeft aangevoerd niet tot een andere conclusie kan leiden. Dat voor het afsluiten van een lening in de bankhal een consument zich vooraf dient te legitimeren, maakt dit eveneens niet anders.

Bejegening

3.6 De commissie stelt vast dat de bank haar excuses heeft aangeboden enerzijds voor het feit dat de consument lang heeft moeten wachten voordat de bank zijn vragen beantwoordde en anderzijds voor het feit dat de klacht in eerste instantie intern niet goed is doorgeleid. Ook al kan de commissie zich het door de consument ervaren ongemak voorstellen, de bank kan niet tot meer worden verplicht en het onervaren ongemak kan niet tot toewijzing van de vorderingen leiden.

[4] Zie Geschillencommissie Kifid nrs. 2020-940, 2019-882 en 2019-759.

Conclusie

3.7 Alhoewel de commissie betreurt dat de consument slachtoffer is geworden van fraude en daardoor geld is kwijtgeraakt, luidt de conclusie dat de vorderingen van de consument moet worden afgewezen.

4. De beslissing

De commissie acht de klacht ongegrond en wijst de daarop gebaseerde vorderingen af.

Deze uitspraak is een bindend advies. Tegen deze uitspraak kunt u beroep instellen bij de Commissie van Beroep Financiële Dienstverlening als wordt voldaan aan de vereisten van artikel 2 van het Reglement van de Commissie van Beroep Financiële Dienstverlening. Voor het instellen van beroep geldt een termijn van zes weken na verzending van deze uitspraak. Het reglement van de commissie van beroep en meer informatie over het instellen van beroep kunt u vinden op de website www.kifid.nl/in-beroep-gaan-bij-kifid.

Binnen twee weken na de verzenddatum van deze uitspraak 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 uitspraak kan hiermee niet ter discussie worden gesteld. Binnen een maand na de verzenddatum van de uitspraak kunt u een schriftelijk verzoek indienen om de uitspraak aan te vullen als u vindt dat de geschillencommissie niet heeft beslist over alle onderdelen van uw vordering. Dit ziet niet op de situatie waarin u meent dat de geschillencommissie in haar uitspraak niet uitdrukkelijk al uw argumenten, ter onderbouwing van uw vordering, heeft behandeld. Meer informatie hierover staat in artikel 40 van het reglement van de geschillencommissie, te vinden op de website www.kifid.nl/reglementen-en-statuten.

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

Relevante wetsartikelen

Artikel 7:522 BW

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 7:524 BW

4. *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.*
5. *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.*
6. *De voorwaarden bedoeld in het eerste lid, onderdeel a, zijn objectief, niet-discriminerend en evenredig.*

Artikel 7:528 BW

1. Onverminderd artikel 526, betaalt de betaaldienstverlener van 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.
2. Op grond van het eerste lid herstelt de betaaldienstverlener van de betaler de betaalrekening die met dat bedrag is gedebiteerd in de toestand zoals die geweest zou zijn wanneer de niet-toegestane betalingstransactie niet had plaatsgevonden. De valutadatum van de creditering van de betaalrekening van de betaler is uiterlijk de datum waarop het bedrag was gedebiteerd.
3. Het eerste lid is niet van toepassing indien de betaaldienstverlener van de betaler redelijke gronden heeft om fraude te vermoeden en hij deze gronden schriftelijk aan de Autoriteit Financiële Markten meedeelt.

4. Indien de betalingstransactie via een betaalinitiatiedienstverlener wordt geïnitieerd, betaalt de rekeninghoudende betaaldienstverlener onmiddellijk, en in elk geval uiterlijk aan het einde van de eerstvolgende werkdag, het bedrag van de niet-toegestane betalingstransactie terug en herstelt hij, in voorkomend geval, de betaalrekening die met dat bedrag was gedebiteerd, in de toestand zoals die geweest zou zijn wanneer de niet-toegestane betalingstransactie niet had plaatsgevonden.
5. Ingeval de betaalinitiatiedienstverlener aansprakelijk is voor de niet-toegestane betalingstransactie, vergoedt hij de rekeninghoudende betaaldienstverlener op diens verzoek onmiddellijk de geleden verliezen of de aan de betaler terugbetaalde bedragen, waaronder het bedrag van de niet-toegestane betalingstransactie. Overeenkomstig artikel 527, tweede lid, is de betaalinitiatiedienstverlener gehouden te bewijzen dat, binnen zijn verantwoordelijkheid, de betalingstransactie is geauthenticeerd, juist is geregistreerd en niet door een technische storing of enig ander falen in verband met de betaaldienst waarmee hij is belast, is beïnvloed.
6. Aanvullende financiële compensatie kan worden vastgesteld overeenkomstig het recht dat van toepassing is op de tussen de betaler en zijn betaaldienstverlener gesloten overeenkomst of de tussen de betaler en de betaalinitiatiedienstverlener gesloten overeenkomst, indien van toepassing.

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 betaalinstrument voortvloeien, tenzij hij frauduleus heeft gehandeld.

Relevante bepalingen uit de Algemene Bankvoorwaarden 2017 (ABV)

***"Artikel 8** – Handtekening*
(…)

1. *Het kan nodig zijn dat u uw handtekening gebruikt om uw akkoord te geven aan een opdracht of een andere handeling die u met ons verricht. Er zijn handgeschreven handtekeningen en elektronische handtekeningen.*

(…)".

***"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). "*

Relevante bepalingen uit de Algemene Voorwaarden betalen en online diensten van de Rabobank 2019 (AV 2019)

Hoofdstuk 1 Meldpunten bij verlies, diefstal en andere incidenten en mogelijkheden met uw betaalpakket en online diensten van Rabobank

"2 Meldpunt bij verlies, diefstal, vermoeden van fraude of andere incidenten

1. *Bij een incident moet u contact opnemen met het relevante meldpunt. Als u contact opgenomen heeft met een meldpunt, geeft het meldpunt u aanwijzingen.*
   (…)"

Hoofdstuk 3 Algemeen

"12 Niet toegestaan gebruik van de rekening, online diensten en betaaldiensten
U bent ervoor verantwoordelijk dat de rekening, online diensten en betaaldiensten niet worden gebruikt voor zaken die:
a. in strijd zijn met de wet
b. inbreuk maken op rechten van iemand anders
c. om andere redenen onrechtmatig zijn
d. de bancaire relatie tussen u en ons schade toebrengen
e. naar onze mening schade toebrengen of kunnen toebrengen aan onze reputatie of de integriteit van het bankwezen in gevaar brengen"

"13 Gebondenheid aan (rechts)handelingen
1. U bent gebonden aan alle (rechts)handelingen die met een betaalpas, creditcard of RaboMobielbetalen van u, een toestel van u, een beveiligingscode van u, een vingerafdruk van u of uw gezicht zijn verricht. Rechtshandelingen zijn bijvoorbeeld het sluiten van een overeenkomst of het geven van een betaalopdracht. U bent ook gebonden aan alle (rechts)handelingen die door een ander met een betaalpas, creditcard of Rabo Mobielbetalen, toestel, beveiligingscode, vingerafdruk of gezicht van u zijn verricht. Bijvoorbeeld als u die ander een volmacht heeft gegeven.
2. Als een elektronische handtekening gezet wordt heeft deze elektronische handtekening dezelfde rechtsgevolgen als een schriftelijke handtekening. U kunt een elektronische handtekening onder andere zetten met de signeercode, S-code, 5-cijferige code, uw vingerafdruk of uw gezicht. (…)"

"18 Terugbetaling bij betalingen zonder toestemming
1. U geeft uw toestemming voor betaalopdrachten. Hierna, in de hoofdstukken 9 en 10, leggen wij uit hoe u ons toestemming voor betaalopdrachten kunt geven.

2. Heeft er een betaling zonder toestemming plaatsgevonden? Dan heeft u recht op terugbetaling als:
- u ons tijdig en op de afgesproken manier heeft laten weten dat het een betaling was zonder uw toestemming of dat er een incident was of u één van deze zaken vermoedde
- u ook de andere veiligheidsregels uit hoofdstuk 4 heeft nageleefd, bijvoorbeeld over het veilig omgaan met uw 5-cijferige code en signeercode
3. U bent in ieder geval volledig aansprakelijk als een betaling zonder toestemming heeft kunnen plaatsvinden door het opzettelijk, met grove schuld of met grove nalatigheid niet naleven van de veiligheidsregels door u of door frauduleus handelen van u. U heeft dan geen recht op terugbetaling.
4. Onderzocht wordt voor wiens rekening en risico de betaling zonder toestemming komt. Blijkt dat u dat bent? Dan heeft u geen recht op terugbetaling en betaalt u het eventueel ontvangen bedrag weer aan ons terug. Wij mogen dit bedrag van uw rekening afboeken.
5. In artikel 2 van hoofdstuk 10 staat wat geldt bij betalingen zonder toestemming na verlies, diefstal of onrechtmatig gebruik van de betaalpas, creditcard of NFC-telefoon.
6. Als wij onderzoek doen naar een betaling zonder toestemming, moet u hieraan meewerken. Bijvoorbeeld door ons informatie te geven, aangifte te doen bij de politie of informatie op te vragen bij een betaalinitiatiedienstverlener, als deze betrokken is. Wij kunnen u hiervoor aanwijzingen geven."

Hoofdstuk 4 Veiligheid

"3.1 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 en mPIN die u in combinatie met de betaalpas, creditcard of NFC-telefoon gebruikt. Het zijn ook alle andere codes die u moet gebruiken om elektronisch betaalopdrachten te geven en/of gebruik te maken van Rabo Online Bankieren, de Rabo Wallet en Rabofoon. Bijvoorbeeld de inlogcode/I-code en signeercode/Scode, die u aanmaakt met een Rabo Scanner of Random Reader. En de 5-cijferige code en de driecijferige code achterop uw creditcard (de CVC-code).
- U mag deze beveiligingscodes alleen zelf gebruiken. U moet dat doen op de manier die wij aangeven.
- 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 is te ontcijferen. Bewaar in dit geval de versleutelde informatie niet bij uw betaalpas, creditcard of NFC-telefoon of apparatuur waarmee u uw bankzaken regelt. (…)

- Geef nooit een beveiligingscode door per telefoon, e-mail, op een website of in een app anders dan die van de Rabobank of op een andere wijze dan wij u hebben voorgeschreven. Dat geldt ook als u telefonisch, per e-mail of persoonlijk door iemand wordt benaderd die aangeeft medewerker van de bank te zijn. Wij zullen u op deze wijze nooit om beveiligingscodes vragen. (…)"

"3.2 Zorg ervoor dat een ander uw betaalpas, creditcard en NFC-telefoon nooit gebruikt

Denk hierbij aan het volgende:

- Laat u niet afleiden als u uw betaalpas, creditcard of NFC-telefoon gebruikt en controleer of u uw eigen betaalpas, creditcard of NFC-telefoon daarna terugkrijgt.

- Berg de betaalpas, creditcard en NFC-telefoon altijd op een veilige plaats op en zorg ervoor dat u deze niet gemakkelijk kunt verliezen.

- Controleer regelmatig of u de betaalpas, creditcard en NFC-telefoon nog in uw bezit heeft."

"3.5 Meld incidenten direct aan ons en volg onze aanwijzingen op

Denk hierbij aan het volgende:

• Neem in de volgende gevallen in elk geval direct contact op met het in artikel 2 van hoofdstuk 1 vermelde meldpunt:

- u heeft uw betaalpas, creditcard of NFC-telefoon niet meer in uw bezit of weet niet waar deze is

- u weet of vermoedt dat iemand anders een beveiligingscode kent of heeft gebruikt - u weet of vermoedt dat iemand een vingerafdruk of gezicht toegevoegd heeft voor Rabo Online Bankieren

- u ziet dat er betalingen op uw rekening hebben plaatsgevonden, waarvoor u geen toestemming heeft gegeven

- u heeft uw mobiele apparaat met daarop één van onze apps waarmee u kunt betalen of bankieren niet meer, tenzij u dit apparaat aan een ander heeft overgedragen en eerst de apps heeft verwijderd.

- Neem ook direct contact op met het in artikel 2 van hoofdstuk 1 vermelde meldpunt bij iets dat u als vreemd of ongebruikelijk ervaart, zoals een andere manier van inloggen. Wij kunnen zorgen voor een blokkade om (verdere) schade te voorkomen. (…)"

Hoofdstuk 10 Regels voor betaalpassen, creditcards en Rabo Mobielbetalen

"2 Gebondenheid bij gebruik pas/regeling schade bij betaling met pas zonder toestemming

1. U bent gebonden aan alle (rechts)handelingen die met een pas van u zijn verricht. Ook als ze door een ander met uw pas zijn verricht.

2. Is uw betaalpas, creditcard of NFC-telefoon gestolen of verloren? Of is één van deze passen op een andere manier onrechtmatig gebruikt? En heeft er vervolgens een betaling zonder toestemming plaatsgevonden? Dan heeft u recht op terugbetaling als:
- ons tijdig en op de afgesproken manier heeft laten weten dat het een betaling was zonder uw toestemming, dat er een incident was of dat u één van deze zaken vermoedde en
- u ook de andere veiligheidsregels uit hoofdstuk 4 heeft nageleefd. Bijvoorbeeld over het veilig omgaan met uw pas en pincode. U bent niet aansprakelijk voor betaalopdrachten die zonder uw toestemming zijn gegeven na de melding.
3. U bent in ieder geval volledig aansprakelijk als een betaling zonder toestemming heeft kunnen plaatsvinden door het opzettelijk, met grove schuld of met grove nalatigheid niet naleven van de veiligheidsregels door u of door frauduleus handelen van u. U heeft dan geen recht op terugbetaling. (…)".

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.

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.

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 gebruikslog van de aan de betalingsgebruiker verstrekte toegangsapparatuur of -software en het abnormale gebruik van de toegangsapparatuur of -software.