

Bijzondere Voorwaarden voor Internetbankieren en Elektronische Communicatie (België)

Versie 1.0

Versie datum: 05.10.2026

A. Bijzondere voorwaarden voor Internetbankieren

Voor het gebruik van de diensten voor internetbankieren die worden aangeboden door CA Consumer Finance S.A.¹ (hierna te noemen "Bank") gelden de volgende bijzondere voorwaarden, naast de bepalingen in het desbetreffende aanvraagformulier voor het openen van een rekening alsmede de Algemene Voorwaarden en de Bijzondere Voorwaarden voor Sparen.

1. DIENSTENAANBOD

- 1.1 De deelnemer en zijn gemachtigde vertegenwoordigers (hierna te noemen "Deelnemers") kunnen bepaalde banktransacties uitvoeren via internetbankieren binnen het door de Bank geboden kader. Daarnaast kunnen zij via internetbankieren informatie bij de Bank opvragen.
- 1.2 Voorts is de Deelnemer voor het gebruik van de Betaalrekening gerechtigd gebruik te maken van betalingsinitiatiediensten en rekeninginformatiediensten te gebruiken zoals gedefinieerd in artikel 2, 5° en 6° van de Wet van 11 maart 2018 betreffende het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen. Daarnaast kan

hij gebruikmaken van andere diensten van de door hem geselecteerde externe aanbieders.

- 1.3 De persoonlijke internetbankierenomgeving dient de Deelnemer primair voor het beheer van zijn rekeningen. Tot de functionaliteiten die via internetbankieren worden aangeboden behoren onder meer het blokkeren van de toegang of het beperken van het mobiele telefoonnummer, het wijzigen van persoonlijke gegevens (zoals adres- en contactgegevens), alsmede het ontvangen en indienen van berichten en informatie via de Bank. Daarnaast omvat het dienstenaanbod de mogelijkheid voor de Deelnemer om online verdere aanvragen voor het openen van rekeningen in te dienen.
- 1.4 In de internetbankierenomgeving kan de Deelnemer de actuele financiële status inzien. De financiële status toont een overzicht van alle rekeningen van de Deelnemer, met het bijbehorende rekeningnummer, de status en het online saldo van het desbetreffende product. Vanuit dit overzicht kan worden doorgeschakeld naar het transactieoverzicht van elke rekening.
- 1.5 In het overzicht voor depositorekeningen worden aanvullende gegevens getoond, zoals de dag van rekeningopening, het einde van de looptijd, de looptijdduur en het jaarlijkse rentetarief.

¹ Deze bijzondere bepalingen zijn een document van CA Consumer Finance S.A., die de in dit document beschreven producten en diensten aanbiedt onder het merk Crédit Agricole Savings.

Tenzij anders vermeld, verwijzen alle informatie en beschrijvingen uitsluitend naar het aanbod van Crédit Agricole Savings.

2. VOORWAARDEN VOOR HET GEBRUIK VAN INTERNETBANKIEREN

2.1 De Deelnemer kan gebruikmaken van internetbankieren indien de Bank hem heeft geauthenticeerd.

2.2 Authenticatie is de afzonderlijk met de Bank overeengekomen procedure waarmee de Bank de identiteit van de Deelnemer of het geautoriseerde gebruik van een overeengekomen gepersonaliseerd instrument of methode kan verifiëren, met inbegrip van het gebruik van het gepersonaliseerde beveiligingskenmerk van de Deelnemer. Met de daartoe overeengekomen authenticatie-factoren kan de Deelnemer zich bij de Bank identificeren als geautoriseerd Deelnemer, informatie raadplegen (zie artikel 3 van deze voorwaarden) en opdrachten verstrekken (zie artikel 4 van deze voorwaarden).

2.3 Authenticatie-factoren zijn

- kennisfactoren, dat wil zeggen iets dat alleen de Deelnemer weet (bijvoorbeeld een persoonlijk identificatienummer (PIN) of wachtwoord);
- bezitsfactoren, dat wil zeggen iets dat alleen de Deelnemer bezit (bijvoorbeeld een apparaat voor het ontvangen van eenmalige transactienummers (TAN) die het bezit door de Deelnemer bevestigen, zoals het mobiele apparaat); en
- Biometrische factoren, dat wil zeggen iets dat de Deelnemer is (inherentie, bijvoorbeeld een vingerafdruk als biometrisch kenmerk van de Deelnemer).

2.4 De authenticatie van de Deelnemer vindt plaats door het doorgeven van de kennisfactor overeenkomstig de vereisten van de Bank, tezamen met het bewijs van de bezitsfactor en/of het bewijs van de biometrische factor aan de Bank, voor zover in individuele gevallen vereist.

3. TOEGANG TOT INTERNETBANKIEREN

3.1 De Deelnemers krijgt toegang tot het internetbankieren van de Bank, wanneer

- hij zijn individuele Deelnemersidentificatie verstrekt (bijvoorbeeld rekeningnummer, inlognaam);
- hij zich identificeert met de door de Bank gevraagde authenticatie-factoren; en
- 8.19er geen toegangsblokkering aanwezig is (zie artikelen 8.1 en 9 van deze voorwaarden).

Na het verlenen van toegang tot internetbankieren kan informatie worden geraadpleegd of kunnen opdrachten overeenkomstig artikel 4 van deze voorwaarden worden verstrekt. 4

3.2 Voor toegang tot gevoelige betaalgegevens in de zin van artikel 2, 46° van de Wet van 11 maart 2018 betreffende het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot betalingssystemen (bijvoorbeeld ten behoeve van het wijzigen van het adres van de klant) alsmede voor bepaalde functionaliteiten (bijvoorbeeld het wijzigen van de PIN), verzoekt de Bank de

Deelnemer zich te identificeren met een aanvullend authenticatie-factor indien bij de toegang tot internetbankieren slechts één authenticatie-factor was gevraagd. De naam van de rekeninghouder en het rekeningnummer zijn geen gevoelige betaalgegevens voor de door de Deelnemer gebruikte betalingsinitiatiedienst en rekeninginformatiedienst.

- 3.3 Na beëindiging van de desbetreffende zakelijke relatie tussen de Deelnemer en de Bank blijven de functionaliteiten van internetbankieren gedurende een aanvullende periode van 30 kalenderdagen beschikbaar. Na deze periode is de Bank gerechtigd de toegang tot alle functionaliteiten van internetbankieren te blokkeren.

4. OPDRACHTEN

4.1 Opdrachtverstrekking

De Deelnemer dient in te stemmen met een opdracht (bijvoorbeeld een overboeking) opdat deze geldig is (autorisatie). Op verzoek dient hij authenticatie-factoren te gebruiken (zoals het invoeren van een PIN of het gebruik van biometrische kenmerken).

De Bank bevestigt de ontvangst van de opdracht via internetbankieren.

4.2 Herroeping van opdrachten

De herroepbaarheid van een opdracht wordt bepaald door de bijzondere voorwaarden die van toepassing zijn op het desbetreffende type opdracht (bijvoorbeeld de Voorwaarden voor Overboeking). De herroeping van opdrachten kan uitsluitend buiten internetbankieren plaatsvinden, tenzij de Bank uitdrukkelijk een herroepingsmogelijkheid in internetbankieren biedt.

5. VERWERKING VAN OPDRACHTEN DOOR DE BANK

- 5.1 De verwerking van opdrachten vindt plaats op de werkdagen die voor de verwerking van het desbetreffende type opdracht (bijvoorbeeld overboeking) zijn aangewezen op de internetbankierenpagina van de Bank of in de “Lijst van Tarieven en Diensten”, in het kader van de reguliere werkwijze. Indien de opdracht wordt ontvangen na het uiterste tijdstip (acceptatieperiode) dat op de internetbankierenpagina van de Bank of in de “Lijst van Tarieven en Diensten” is vermeld, of indien het tijdstip van ontvangst niet op een werkdag valt volgens de internetbankierenpagina van de Bank of de “Lijst van Tarieven en Diensten”, wordt de opdracht geacht op de eerstvolgende werkdag te zijn ontvangen. De verwerking vangt pas op die werkdag aan.

- 5.2 De Bank zal de opdracht uitvoeren indien aan de volgende uitvoeringsvoorwaarden is voldaan:

- 4.1 De Deelnemer heeft de opdracht geautoriseerd (vgl. artikel 4.1 van deze voorwaarden).
- De autorisatie van de Deelnemer voor het desbetreffende opdrachttype is aanwezig.
- Het gegevensformaat voor internetbankieren is in acht genomen.
- 2 Aan de overige uitvoeringsvoorwaarden overeenkomstig de bijzondere voorwaarden die van toepassing zijn op het desbetreffende opdrachttype (bijvoorbeeld toereikend rekeningsaldo overeenkomstig de

voorwaarden voor
(overboekingen) is voldaan.

Indien aan de
uitvoeringsvoorwaarden
overeenkomstig de eerste zin is
voldaan, voert de Bank de
opdrachten uit overeenkomstig de
bepalingen van de bijzondere
voorwaarden die van toepassing zijn
op het desbetreffende opdrachttype
(bijvoorbeeld de Bijzondere
Voorwaarden Overboekingen).

5.3 Indien niet aan de
uitvoeringsvoorwaarden
overeenkomstig artikel 5.2 is
voldaan, voert de Bank de
internetbankierenopdracht niet uit en
stelt zij de Deelnemer via
internetbankieren in kennis van de
niet-uitvoering en – voor zover
mogelijk – van de redenen daarvoor
en de mogelijkheden om fouten die
tot de afwijzing hebben geleid te
corrigeren.

6. INFORMATIE VOOR DE DEELNEMER OVER INTERNETBANKIEREN TRANSACTIES

De Bank informeert de Deelnemer
ten minste eenmaal per maand over
de via internetbankieren verrichte
transacties op de voor
rekeninginformatie overeengekomen
wijze, voor zover in de afzonderlijk
overeengekomen bijzondere
voorwaarden (bijvoorbeeld de
Bijzondere Voorwaarden voor
Sparen) geen afwijkende regeling is
opgenomen.

7. ZORGPLICHTEN VAN DE KLANT

7.1 Bescherming van authenticatie- factoren

7.1.1. De Deelnemer dient alle redelijke
voorzorgsmaatregelen te nemen om
zijn authenticatie-factoren (zie artikel
2 van deze voorwaarden) tegen
onbevoegde toegang te
beschermen. Anders bestaat het

risico dat internetbankieren wordt
misbruikt of anderszins onbevoegd
wordt benaderd (vergelijk de
artikelen 3 en 4 van deze
voorwaarden).

7.1.2. Ter bescherming van de
afzonderlijke authenticatie-factoren
dient de Deelnemer met name het
volgende in acht te nemen:

(i) Kennisfactoren, zoals
bijvoorbeeld de PIN, dienen
geheim te worden gehouden; zij
moeten met name

- niet mondeling worden
bekendgemaakt
(bijvoorbeeld via telefoon of
in persoon);
- niet buiten
internetbankieren in
tekstvorm worden gedeeld
(bijvoorbeeld via e-mail of
berichtendienst);
- niet onbeveiligd
elektronisch worden
opgeslagen (bijvoorbeeld
het opslaan van de PIN in
platte tekst op een computer
of mobiel apparaat); en
- niet worden vastgelegd op
een apparaat of als afschrift
worden bewaard tezamen
met een apparaat dat als
bezitsfactor dient
(bijvoorbeeld een mobiel
apparaat) of voor verificatie
van de biometrische
factoren (bijvoorbeeld een
mobiel apparaat met een
applicatie voor
internetbankieren en
vingerafdruksensor).

(ii) Bezitsfactoren, zoals
bijvoorbeeld het mobiele
apparaat, dienen tegen misbruik
te worden beschermd, met name
dient de Deelnemer:

- ervoor te zorgen dat onbevoegde personen geen toegang hebben tot het mobiele apparaat van de Deelnemer (bijvoorbeeld de mobiele telefoon);
- ervoor te zorgen dat andere personen de applicatie voor internetbankieren op het mobiele apparaat niet kunnen gebruiken (bijvoorbeeld de internetbankieren-app, de authenticatie-app);
- de applicatie voor internetbankieren (bijvoorbeeld de internetbankieren-app, de authenticatie-app) op het mobiele apparaat van de Deelnemer te deactiveren voordat de Deelnemer het eigendom van dit mobiele apparaat overdraagt (bijvoorbeeld door verkoop of verwijdering van de mobiele telefoon);
- het bewijs van de bezitsfactor (bijvoorbeeld TAN) niet buiten internetbankieren mondeling (bijvoorbeeld via de telefoon) of schriftelijk (bijvoorbeeld via e-mail, berichtendienst) door te geven; en
- de Deelnemer die van de Bank een code heeft ontvangen ter activering van de bezitsfactor (bijvoorbeeld een mobiele telefoon met de applicatie voor internetbankieren) deze veilig op te bergen om onbevoegde toegang door andere personen te voorkomen; anders bestaat het risico dat andere personen hun apparaat als

bezitsfactor voor het internetbankieren van de Deelnemer activeren.

- (iii) Biometrische factoren, zoals de vingerafdruk van de Deelnemer, mogen slechts als authenticatiefactor voor internetbankieren op het mobiele apparaat van de Deelnemer worden gebruikt indien op het mobiele apparaat geen persoonlijke factoren van andere personen zijn opgeslagen. Indien op het voor internetbankieren gebruikte mobiele apparaat persoonlijke factoren van andere personen zijn opgeslagen, dient voor internetbankieren het door de Bank verstrekte kennisfactor (bijvoorbeeld PIN) te worden gebruikt en niet het op het mobiele apparaat opgeslagen persoonlijke factor.

7.1.3. Bij de mobiele TAN-procedure mag het mobiele apparaat dat wordt gebruikt voor het ontvangen van de TAN (bijvoorbeeld mobiele telefoon) niet gelijktijdig voor internetbankieren worden gebruikt.

7.1.4. Het voor de mobiele TAN-procedure opgeslagen referentie-mobiele telefoonnummer dient te worden verwijderd of gewijzigd indien de Deelnemer dit telefoonnummer niet langer voor internetbankieren gebruikt.

7.1.5. Onverminderd de beschermingsverplichtingen uit hoofde van de artikelen 7.1.1 tot en met 7.1.3, mag de Deelnemer zijn authenticatie-factoren gebruiken bij een door hem geselecteerde betalingsinitiatiedienst en rekeninginformatiedienst alsmede bij een andere dienst van derden (zie artikel 1.2, tweede en derde zin van deze voorwaarden). De Deelnemer dient bij de selectie van diensten van

derden de in het verkeer vereiste zorgvuldigheid in acht te nemen.

7.2 Veiligheidsmededelingen van de Bank

De Deelnemer dient de veiligheidsmededelingen van de Bank met betrekking tot internetbankieren na te leven, met name de maatregelen ter bescherming van de gebruikte hardware en software (klantensysteem).

7.3 Verificatie van opdrachtgegevens met de door de Bank weergegeven gegevens

De Bank toont de Deelnemer de door haar ontvangen opdrachtgegevens (bijvoorbeeld bedrag, rekeningnummer van de begunstigde) via het afzonderlijk overeengekomen apparaat van de Deelnemer (bijvoorbeeld door middel van een mobiel apparaat).

De Deelnemer is verplicht de overeenstemming van de weergegeven gegevens met de voor de opdracht beoogde gegevens te controleren alvorens te bevestigen. Indien afwijkingen worden vastgesteld, dient de transactie te worden afgebroken.

8. INFORMATIE- EN MELDINGSPLICHTEN

8.1 Blokkeringsmelding

8.1.1. Indien de Deelnemer vaststelt

- dat de referentie-mobiele telefoon verloren is gegaan of is gestolen, of
- dat er sprake is van misbruik of ander onbevoegd gebruik van een authenticatie-factor,

dient de Deelnemer de Bank hiervan onverwijld in kennis te stellen (blokkeringsmelding). De Deelnemer

kan een dergelijke blokkeringsmelding te allen tijde indienen bij de Bank via de afzonderlijk medegedeelde communicatiekanalen.

8.1.2. De Deelnemer dient elke diefstal of elk misbruik van een authenticatie-factor onmiddellijk bij de politie te melden.

8.1.3. Indien de Deelnemer onbevoegd of frauduleus gebruik van een van zijn authenticatie-factoren vermoedt, dient hij eveneens een blokkeringsmelding in te dienen.

8.2 Melding van niet-geautoriseerde of onjuist uitgevoerde transacties

De Deelnemer dient de Bank onverwijld in kennis te stellen zodra hij een niet-geautoriseerde of onjuist uitgevoerde transactie ontdekt.

9. GEBRUIKSBEPERKING

9.1 Door de Deelnemer geïnitieerde beperking

De Bank beperkt op instructie van de Deelnemer, met name in geval van een blokkeringsmelding overeenkomstig artikel 8.1 van deze voorwaarden,

- de toegang tot internetbankieren voor hem of alle Deelnemers; of
- zijn authenticatie-factoren voor het gebruik van internetbankieren.

9.2 Blokkering op verzoek van de Bank

9.2.1 De Bank kan de toegang tot internetbankieren voor een Deelnemer blokkeren indien

- zij gerechtigd is de internetbankierenovereenko

mst om gewichtige redenen op te zeggen;

- objectieve redenen in verband met de veiligheid van de authenticatie-factoren van de Deelnemer dit rechtvaardigen; of
- objectieve redenen met betrekking tot de beveiliging van de authenticatiemiddelen van Deelnemer dit rechtvaardigen, of
- er een vermoeden bestaat van onbevoegd of frauduleus gebruik van een authenticatie-factor.

9.2.2 De Bank stelt de Deelnemer, onder vermelding van de relevante redenen, zo spoedig mogelijk, doch uiterlijk onmiddellijk na de blokkering, hiervan in kennis. Het vermelden van redenen mag achterwege blijven indien dit in strijd zou zijn met wettelijke verplichtingen.

9.3 **Opheffing van de blokkering**

De Bank heft een blokkering op of vervangt de betrokken authenticatie-factoren indien de redenen voor de blokkering niet langer van toepassing zijn. Zij stelt de Deelnemer hiervan onverwijld in kennis.

9.4 **Beperking van rekeningtoegang voor betaalinitiatiedienst en rekeninginformatiedienst**

De Bank kan aanbieders van rekeninginformatiediensten of betalingsinitiatiediensten de toegang tot een betaalrekening van een Deelnemer weigeren indien gemotiveerde en naar behoren aangetoonde redenen in verband met onbevoegde of frauduleuze toegang door de aanbieder van rekeninginformatiediensten of betalingsinitiatiediensten tot de

betaalrekening, met inbegrip van het onbevoegd of frauduleus initiëren van een betalingstransactie, een dergelijke weigering rechtvaardigen. De Bank stelt de Deelnemer in kennis van een dergelijke toegangsweigering. De kennisgeving geschiedt vóór, of uiterlijk onmiddellijk na, de weigering van toegang. Redenen mogen niet worden bekendgemaakt voor zover de Bank daarmee toepasselijke wettelijke verplichtingen zou schenden. Zodra de redenen voor de toegangsweigering niet langer bestaan, heft de Bank de toegangsbeperking op. De Deelnemer wordt hiervan onverwijld in kennis gesteld.

10. **AANSPRAKELIJKHEID**

10.1 **Aansprakelijkheid van de Bank voor onbevoegde of onjuiste wijzigingen van klantspecifieke informatie**

De Bank is aansprakelijk voor schade die voortvloeit uit een onbevoegde wijziging, of uit een wijziging van klantspecifieke informatie (zoals een wijziging van contactgegevens of PIN) die niet, onjuist of te laat wordt doorgevoerd.

10.2 **Aansprakelijkheid van de Bank voor de uitvoering van een niet-geautoriseerde transactie en een transactie die niet, onjuist of te laat uitgevoerd is**

De aansprakelijkheid van de Bank voor een niet-geautoriseerde opdracht en voor een opdracht die niet, onjuist of te laat is uitgevoerd, wordt beheerst door de bijzondere voorwaarden die voor het desbetreffende type opdracht zijn overeengekomen (bijvoorbeeld de Voorwaarden voor Overboekingen).

10.3 Aansprakelijkheid van de Deelnemer bij misbruik van hun authenticatie-factoren

waaraan activiteiten van de betalingsdienstaanbieder zijn uitbesteed.

10.3.1. Aansprakelijkheid van de Deelnemer bij onbevoegde toegang en wijziging van gebruikersspecifieke informatie vóór de blokkeringsmelding

- (i) Indien onbevoegde toegang en wijziging van gebruikersspecifieke informatie vóór de blokkeringsmelding berust op het gebruik van een verloren gegaan, gestolen of anderszins in het ongerede geraakt authenticatie-factor of op ander misbruik van een authenticatie-factor, is de Deelnemer aansprakelijk voor de daardoor aan de Bank veroorzaakte schade, mits het verlies, het in het ongerede raken of het ander misbruik van het authenticatie-factor te wijten is aan nalatig of verwijtbaar handelen van de Deelnemer.
- (ii) De Deelnemer is niet gehouden tot vergoeding van de schade op grond van lid (i) indien
- het voor hem niet mogelijk was het verlies, de diefstal, het in het ongerede raken of enig ander misbruik van het authenticatie-factor vóór de onbevoegde toegang en wijziging op te merken; of
 - het verlies van het authenticatie-factor is veroorzaakt door een medewerker, een vertegenwoordiger, een bijkantoor van een betalingsdienstaanbieder of een andere entiteit

10.3.2. Aansprakelijkheid van de Deelnemer voor niet-geautoriseerde betalingsdiensten vóór de blokkeringsmelding

- (i) Indien niet-geautoriseerde betalingstransacties vóór de blokkeringsmelding berusten op het gebruik van een verloren gegaan, gestolen of anderszins in het ongerede geraakte authenticatie-factor of op misbruik van een authenticatie-factor, is de Deelnemer aansprakelijk voor de daardoor aan de Bank veroorzaakte schade tot een bedrag van EUR 50, ongeacht of de Deelnemer schuld treft.
- (ii) De Deelnemer is niet gehouden tot vergoeding van de schade op grond van lid (i) indien
- (iii) De Deelnemer is niet aansprakelijk voor schadevergoeding onder paragraaf (i) indien
- het voor hem niet mogelijk was het verlies, de diefstal, het in het ongerede raken of enig ander onbevoegd gebruik van de authenticatie-factor vóór de niet-geautoriseerde betalingstransactie op te merken; of
 - het verlies van de authenticatie-factor is veroorzaakt door een medewerker, een vertegenwoordiger, een bijkantoor van een betalingsdienstaanbieder

of een andere entiteit waaraan de activiteiten van de betalingsdienstaanbieder zijn uitbesteed.

10.3.3. Indien niet-geautoriseerde betalingstransacties of onbevoegde toegang en wijziging van klantspecifieke informatie zich voordoen vóór de blokkeringsmelding, en de Deelnemer met frauduleus opzet heeft gehandeld of zijn meldingsverplichtingen en zorgplichten uit hoofde van deze voorwaarden opzettelijk of met grove nalatigheid heeft geschonden, draagt de Deelnemer, in afwijking van lid (ii) van de artikelen 10.3.1 en 10.3.2, de ontstane schade volledig. Van grove nalatigheid van de Deelnemer kan met name sprake zijn indien hij een van zijn zorgplichten uit hoofde van

- **Erreur ! Source du renvoi introuvable.**artikel 7.1.2;
- 7.1.3artikel 7.1.3, tweede zin;
- 7.3artikel 7.3; of
- **Erreur ! Source du renvoi introuvable.**artikel 8.1.1;

van deze voorwaarden heeft geschonden.

10.3.4. Onverminderd lid (i) van de artikelen 10.3.1 en 10.3.2 en artikel 10.3.3, is de Deelnemer niet gehouden tot schadevergoeding indien de Bank van de Deelnemer geen sterke cliëntauthenticatie overeenkomstig artikel 2, 45° van de Wet van 11 maart 2018 betreffende het statuut van en het toezicht op de betalingsinstellingen en de instellingen voor elektronisch geld, de toegang tot het bedrijf van betalingsdienstaanbieder en tot de activiteit van uitgifte van elektronisch geld, en de toegang tot

betalingssystemen heeft verlangd. Sterke cliëntauthenticatie vereist met name het gebruik van twee onafhankelijk geclassificeerde authenticatie-factoren uit de categorieën kennis, bezit of biometrisch (zie artikel 2.3 van deze voorwaarden).

10.3.5. **10.3.1Erreur ! Source du renvoi introuvable.Erreur ! Source du renvoi introuvable.**2.3De

aansprakelijkheid voor schade die is ontstaan gedurende de periode waarvoor het beschikkingslimiet geldt, is beperkt tot het overeengekomen beschikkingslimiet.

10.3.6. De Deelnemer is niet gehouden tot schadevergoeding op grond van lid (i) van de artikelen 10.3.1 en 10.3.2 en artikel 10.3.3 indien de Deelnemer niet in staat was de blokkeringsmelding overeenkomstig artikel 8.1 van deze voorwaarden te doen omdat de Bank niet heeft zorggedragen voor de mogelijkheid om de blokkeringsmelding te ontvangen.

10.3.7. Lid (ii) van de artikelen 10.3.1 en 10.3.2 en de artikelen 10.3.4 tot en met 10.3.6 zijn niet van toepassing indien de Deelnemer met frauduleus opzet heeft gehandeld.

10.4 **Aansprakelijkheid van de klant voor onbevoegde beschikkingen buiten betalingsdiensten vóór de blokkeringsmelding**

Indien onbevoegde beschikkingen buiten betalingsdiensten (bijvoorbeeld beschikkingen over deposito's) vóór de blokkeringsmelding berusten op het gebruik van een verloren gegaan of gestolen authenticatie-factor of op ander misbruik van de authenticatie-factor en dit schade aan de Bank heeft veroorzaakt, zijn de Deelnemer en de Bank aansprakelijk

overeenkomstig de wettelijke beginselen van eigen schuld.

10.5 Aansprakelijkheid van de Bank vanaf de blokkeringsmelding

Zodra de Bank een blokkeringsmelding van een Deelnemer heeft ontvangen, draagt zij de verantwoordelijkheid voor alle daarna ontstane schade als gevolg van niet-geautoriseerde internetbankierentransacties of -wijzigingen. Dit geldt niet indien de Deelnemer met frauduleus opzet heeft gehandeld.

10.6 Uitsluiting van aansprakelijkheid

Aansprakelijkheidsclaims zijn uitgesloten indien de omstandigheden die aan de claim ten grondslag liggen berusten op een uitzonderlijke en onvoorzienbare gebeurtenis waarop de partij die zich op deze gebeurtenis beroept geen invloed had en waarvan de gevolgen ook bij betrachting van de nodige zorgvuldigheid niet hadden kunnen worden vermeden.

B. Bijzondere Voorwaarden voor Elektronische Communicatie

1. Inleiding

1.1 De communicatie tussen de Bank en de klant vindt in beginsel elektronisch plaats via internetbankieren. De Bank en de klant komen overeen dat de Bank de internetbankierenfunctie mag gebruiken voor de communicatie met de klant en met name voor het ter beschikking stellen van documenten en informatie aan de klant (bijvoorbeeld rekeningafschriften).

1.2 De klant kan de internetbankierenfunctie met name gebruiken om de door de Bank ter beschikking gestelde documenten op te halen, online in te zien, te downloaden, af te drukken en te archiveren.

2. Inrichting en gebruiksmogelijkheden

2.1 De Bank richt in de internetbankierenomgeving een speciaal onderdeel in dat is bestemd voor elektronische communicatie met de klant (de "Online Communicatie Omgeving"). De Bank kan de Online Communicatie Omgeving te allen tijde hernoemen of technisch wijzigen zonder dat dit afbreuk doet aan de functie ervan als het overeengekomen kanaal voor elektronische communicatie.

2.2 Zodra de functie beschikbaar is, kan de klant de berichtenfunctie binnen de Online Communicatie Omgeving gebruiken om berichten aan de Bank te verzenden (zoals vragen over de rekening, terugbelverzoeken of wijzigingen van contactgegevens). Het verzenden van documenten of afbeeldingen door de klant aan de Bank via de Online Communicatie Omgeving is uitgesloten, tenzij dit door de Bank uitdrukkelijk is ingeschakeld.

2.3 Indien de zakelijke relatie niet tot stand komt of nadien wordt beëindigd (bijvoorbeeld door het uitoefenen van een wettelijk herroepingsrecht), kan de Bank de internetbankierenfunctie, met inbegrip van de Online Communicatie Omgeving, onmiddellijk deactiveren en zo nodig de inhoud verwijderen.

2.4 De Bank is te allen tijde gerechtigd de toegang tot de internetbankierenfunctie, met inbegrip van de Online Communicatie Omgeving, geheel of gedeeltelijk te blokkeren of te beperken, indien omstandigheden het vermoeden rechtvaardigen dat de veiligheid van de toegang is aangetast, onbevoegde of frauduleuze toegang mogelijk is, of de Bank gerechtigd is de zakelijke relatie met de klant om gewichtige redenen te beëindigen.

3. Terbeschikkingstelling van documenten en afstand door de klant van andere bezorgingswijzen

3.1 De klant verklaart zich ermee in te stemmen dat de Bank alle documenten met betrekking tot de zakelijke relatie tussen de klant en de Bank versleuteld en rechtsgeldig ter beschikking stelt in de Online Communicatie Omgeving, tenzij uitdrukkelijk schriftelijk met de klant anders is overeengekomen of de wet anders vereist.

3.2 De klant erkent en verklaart zich ermee in te stemmen dat dergelijke documenten niet op enige andere wijze aan hem ter beschikking hoeven te worden gesteld. De klant doet met name afstand van de postale bezorging van deze documenten.

3.3 De Bank blijft evenwel gerechtigd de klant op andere geschikte wijze van

- informatie en documenten te voorzien indien de wet dit vereist of indien dit redelijk is vanwege andere omstandigheden (bijvoorbeeld bij een tijdelijke storing van de internetbankierenfunctie).
- 3.4 Onverminderd het voorgaande is de Bank gerechtigd afzonderlijke of alle documenten per post of anderszins aan de klant toe te zenden in geval van technische problemen, indien zij dit in het licht van de belangen van de klant passend acht.
4. **Tijdstip van ontvangst**
- 4.1 De door de Bank in de Online Communicatie Omgeving geplaatste documenten worden geacht te zijn ontvangen wanneer de klant door de Bank is geïnformeerd over de plaatsing en de mogelijkheid van ophaling via de internetbankierenomgeving, en gebruikelijke kennisgeving door de klant kan worden aangenomen, dat wil zeggen uiterlijk op de werkdag volgend op de informatie door de Bank. Indien de klant de documenten reeds eerder heeft opgehaald, worden zij geacht op dat eerdere tijdstip te zijn ontvangen. Deze fictieve ontvangstbepaling laat de aanvang van een dwingendrechtelijke wettelijke herroepingstermijn onverlet; deze termijn vangt aan op de datum waarop de klant daadwerkelijk de relevante precontractuele informatie heeft ontvangen, zoals vereist op grond van toepasselijk dwingend recht.
- 4.2 Vanaf het tijdstip van ontvangst van het desbetreffende document overeenkomstig artikel 4.1 vangt de aan deze ontvangst gekoppelde termijnen aan (bijvoorbeeld een herroepingstermijn).
5. **Integriteit van documenten binnen de internetbankierenomgeving**
- 5.1 De Bank waarborgt de onveranderlijkheid van documenten binnen de Online Communicatie Omgeving.
- 5.2 Deze verplichting geldt niet indien de documenten buiten de Online Communicatie Omgeving worden opgeslagen of bewaard. Zodra deze documenten door de klant buiten de Online Communicatie Omgeving worden opgeslagen of gebruikt (bijvoorbeeld na downloaden), aanvaardt de Bank geen verantwoordelijkheid voor de integriteit van de documenten of hun inhoud.
- 5.3 Door individuele hardware- of software-instellingen komt een afdruk niet altijd visueel overeen met de weergave op het scherm.
6. **Kennisgeving**
- 6.1 Wanneer een nieuw document in de Online Communicatie Omgeving wordt geplaatst, stuurt de Bank een kennisgeving per e-mail naar het door de klant opgegeven e-mailadres. De klant controleert regelmatig zijn persoonlijke e-mailapplicatie en de spammappen van de door hem gebruikte e-mailapplicatie. De klant stemt ermee in dergelijke kennisgevingen onversleuteld per e-mail te ontvangen.
- 6.2 De klant is verplicht ervoor te zorgen dat het e-mailadres dat bij het aangaan van de zakelijke relatie met de Bank is opgegeven voor het ontvangen van e-mails, gereed is voor gebruik. De klant is verplicht de Bank onverwijld in kennis te stellen van elke wijziging van het e-mailadres.
7. **Medewerkingsplicht van de klant**
- 7.1 De klant is verplicht de Online Communicatie Omgeving met regelmatige, redelijke tussenpozen,

doch ten minste eenmaal per maand, te controleren, alsmede onverwijld bij specifieke gelegenheden (bijvoorbeeld na opdrachten aan de Bank of na een kennisgevingse-mail overeenkomstig artikel 6.1 van deze voorwaarden) op inkomende berichten.

7.2 De klant verklaart hierbij dat de Bank aan haar verzend- en kennisgevingsverplichtingen heeft voldaan met de ontvangst van de documenten in de Online Communicatie Omgeving en de bijbehorende kennisgevingse-mail aan de klant.

7.3 De klant is verplicht de door de Bank in de Online Communicatie Omgeving geplaatste documenten op te halen en de inhoud ervan op juistheid en volledigheid te controleren.

7.4 Onverminderd artikel 6, lid 2, van de Algemene Voorwaarden van de Bank, dient de klant bezwaren onverwijld na ontvangst van de documenten, ten minste in tekstvorm (bijvoorbeeld per e-mail of via de Online Communicatie Omgeving), aan de Bank kenbaar te maken.

8. **Bewaartermijn**

De in de [Online Communicatie Omgeving] ter beschikking gestelde documenten zijn beschikbaar gedurende de gehele looptijd van de desbetreffende zakelijke relatie tussen de klant en de Bank. Na beëindiging van de desbetreffende zakelijke relatie tussen de klant en de Bank blijven de in de Online Communicatie Omgeving ter beschikking gestelde documenten gedurende een aanvullende periode van 30 kalenderdagen toegankelijk, totdat de gehele internetbankierenfunctie wordt opgeschort. De klant is verantwoordelijk voor de bewaring

van de documenten na beëindiging van de zakelijke relatie. Wettelijke bewaarverplichtingen van de Bank blijven onverlet.

9. **Erkenning van documenten**

De Bank garandeert niet dat de in de Online Communicatie Omgeving geplaatste documenten door derden, met name de bevoegde autoriteiten en instellingen (zoals belastingautoriteiten), worden geaccepteerd. De klant is verplicht zelfstandig bij de voor hem bevoegde autoriteit of instelling informatie in te winnen over de acceptatie van de documenten.

10. **Onderhoud en wijziging van de diensten**

10.1 De Bank kan de Online Communicatie Omgeving geheel of gedeeltelijk beperken, herontwerpen, doorontwikkelen of beëindigen, en/of voorwaarden verbinden aan het gebruik ervan door de klant.

10.2 De Bank stelt de klant met passende voorafgaande kennisgeving in kennis van dergelijke wijzigingen en/of beëindiging van de Online Communicatie Omgeving en wijst de klant, indien van toepassing, op een alternatieve communicatiemethode.

10.3 De Bank garandeert niet de constante, ononderbroken beschikbaarheid van de Online Communicatie Omgeving of de daarin opgenomen documenten. De Bank kan de toegang tot de Online Communicatie Omgeving met name onderbreken ten behoeve van onderhoudsvensters.

10.4 De toegang kan eveneens worden onderbroken door omstandigheden buiten de macht van de Bank (bijvoorbeeld een storing van de internetverbinding).

11. **Beëindiging van de
rechtsverhouding**

Na beëindiging van de desbetreffende zakelijke relatie tussen de klant en de Bank blijven de documenten gedurende een aanvullende periode van 30 kalenderdagen beschikbaar in de Online Communicatie Omgeving. Na deze periode is de Bank gerechtigd de toegang tot de Online Communicatie Omgeving te blokkeren.