

Conditions particulières pour la banque en ligne et la communication électronique

Version 1.0

Version datée : 05.10.2026

A. Conditions particulières pour la banque en ligne

Pour l'utilisation des services de banque en ligne proposés par CA Consumer Finance S.A.¹ (ci-après dénommée « Banque »), les conditions particulières suivantes s'appliquent en complément des règles énoncées dans la demande d'ouverture de compte correspondante ainsi que des conditions générales et des Conditions particulières pour l'épargne.

1. OFFRE DE SERVICES

1.1 Le Participant et ses représentants autorisés (ci-après dénommés « Participants ») peuvent effectuer certaines opérations bancaires à l'aide de la banque en ligne dans le cadre prévu par la Banque. En outre, ils peuvent obtenir des informations auprès de la Banque via la banque en ligne.

1.2 En outre, pour l'utilisation du Compte cash, le Participant est habilité à utiliser des services d'initiation de paiement et des services d'information sur les comptes tels que définis à l'article 2, 5° et 6° de la loi belge du 11 mars 2018 sur le statut et la surveillance des établissements de paiement et des établissements de monnaie électronique. En outre, il peut utiliser d'autres services auprès de prestataires tiers qu'il a sélectionnés.

1.3 L'espace personnel de banque en ligne sert principalement au

Participant pour gérer ses comptes. Parmi les fonctionnalités offertes par la banque en ligne figurent le blocage d'accès ou les restrictions relatives au numéro de téléphone mobile, la modification des données personnelles (telles que l'adresse et les coordonnées de contact), ainsi que la réception et la soumission de messages et informations via la Banque. En outre, la gamme de services comprend la possibilité pour le Participant de soumettre en ligne d'autres demandes d'ouverture de compte.

1.4 Dans l'espace de banque en ligne, le Participant peut consulter la situation financière actuelle. La situation financière affiche une liste de tous les comptes du Participant, ainsi que le numéro de compte correspondant, l'état et le solde en ligne du produit concerné. À partir de cette vue, il est possible de passer à la vue des opérations pour chaque compte.

1.5 Dans la vue d'ensemble des comptes de dépôt, des détails supplémentaires tels que la date d'ouverture du compte, l'échéance finale, la durée du terme et le taux d'intérêt annuel sont affichés.

2. CONDITIONS PREALABLES A L'UTILISATION DE LA BANQUE EN LIGNE

2.1 Le Participant peut utiliser la banque en ligne si la Banque les a authentifiés.

2.2 L'authentification est la procédure convenue séparément avec la Banque, grâce à laquelle la Banque

¹ Ces conditions particulières sont un document de CA Consumer Finance S.A., qui propose les produits et services décrits dans ce document sous la marque Crédit Agricole Savings. Sauf

indication contraire, toutes les informations et descriptions se réfèrent exclusivement à l'offre fournie par Crédit Agricole Savings.

peut vérifier l'identité du Participant ou l'utilisation autorisée d'un instrument personnalisé ou d'une méthode convenue, y compris l'utilisation du dispositif de sécurité personnalisé du Participant. Avec les éléments d'authentification convenus à cette fin, le Participant peut s'identifier comme Participant autorisé auprès de la Banque, accéder aux messages et informations (voir section 3 des présentes conditions), et donner des instructions (voir section 4 des présentes conditions).

2.3 Les éléments d'authentification sont

- Des éléments d'identification, c'est-à-dire des informations que seul le Participant connaît (par exemple, numéro d'identification personnel (PIN) ou mot de passe), et
- Des éléments de possession, c'est-à-dire des éléments que seul le Participant possède (par exemple, un appareil pour recevoir des numéros de transaction à usage unique (TAN) qui confirment la possession par le Participant comme l'appareil mobile).
- Des éléments biométriques, c'est-à-dire des éléments du Participant lui-même (inhérence, par exemple, empreinte digitale en tant que caractéristique biométrique du Participant).

2.4 L'authentification du Participant a lieu en transmettant l'élément de connaissance conformément aux exigences de la Banque, ainsi que l'élément de preuve de possession et/ou l'élément de preuve d'inhérence à la Banque, si nécessaire dans des cas individuels.

3. ACCES A LA BANQUE EN LIGNE

3.1 Le Participant obtient l'accès à la banque en ligne de la Banque, lorsque

- ils fournissent leur identifiant individuel du Participant (p. ex., numéro de compte, identifiant de connexion) et
- ils s'identifient au moyen des éléments d'authentification demandés par la Banque et
- il n'y a pas de blocage d'accès (voir sections 8.1 et 9 de ces conditions) présent.

Après avoir accordé l'accès à banque en ligne, des informations peuvent être consultées ou des ordres conformément à la section 4 de ces conditions peuvent être émis.

3.2 Pour l'accès aux données de paiement sensibles au sens de l'article 2, 46° de la loi belge du 11 mars 2018 relative au statut et la surveillance des établissements de paiement et des établissements de monnaie électronique (par ex., aux fins de modifier l'adresse du client) ainsi que pour certaines fonctionnalités (par ex., modification du NIP), la Banque demande au Participant de s'identifier à l'aide d'un élément d'authentification supplémentaire si un seul élément d'authentification a été demandé lors de l'accès à la banque en ligne. Le nom du titulaire du compte et le numéro de compte ne sont pas des données de paiement sensibles pour le service d'initiation de paiement et le service d'information sur les comptes utilisés par le Participant.

3.3 Après la cessation de la relation d'affaires respective entre le Participant et la Banque, les fonctionnalités de banque en ligne resteront disponibles pendant

30 jours calendaires supplémentaires. Après cette période, la Banque est en droit de bloquer l'accès à toutes les fonctionnalités de banque en ligne.

4. ORDRES

4.1 Passation des ordres

Le Participant doit consentir à un ordre (par exemple, un virement) pour qu'il soit effectif (autorisation). Sur demande, il doit utiliser des éléments d'authentification (tels que la saisie d'un NIP ou l'utilisation de caractéristiques biométriques).

La Banque confirme la réception de l'ordre via la banque en ligne.

4.2 Révocation des ordres

La possibilité de révoquer un ordre est régie par les conditions particulières applicables au type d'ordre concerné (par exemple, les Conditions relatives aux virements).

La révocation des ordres ne peut avoir lieu qu'en dehors de la banque en ligne, sauf si la Banque offre expressément une possibilité de révocation via la banque en ligne.

5. TRAITEMENT DES ORDRES PAR LA BANQUE

5.1 Le traitement des ordres a lieu les jours ouvrables spécifiés pour le traitement du type d'ordre concerné (par exemple, des virements) sur la page de banque en ligne de la Banque ou dans la « Liste des prix et des services » dans le cadre du processus régulier. Si l'ordre est reçu après l'heure limite (période d'acceptation) indiquée sur la page de banque en ligne de la Banque ou dans la « Liste des prix et des services » ou si le moment de la réception ne tombe pas un jour ouvrable selon la page de banque en ligne de la Banque ou la « Liste des

prix et des services », l'ordre est considéré comme reçu le jour ouvrable suivant. Le traitement ne commence que ce jour ouvrable.

5.2 La Banque exécutera l'ordre si les conditions d'exécution suivantes sont remplies :

- Le Participant a autorisé l'ordre (cf. section 4.1 des présentes conditions).
- L'autorisation du Participant pour le type d'ordre concerné est présente.
- Le format de données de la banque en ligne est respecté.
- Les autres conditions d'exécution conformément aux conditions particulières applicables au type d'ordre respectif (par exemple, une provision suffisante sur le compte conformément aux conditions pour les virements) sont remplies.

Si les conditions d'exécution selon la phrase 1 sont remplies, la Banque exécute les ordres conformément aux dispositions des conditions particulières applicables au type d'ordre respectif (par exemple, Conditions particulières pour les virements).

5.3 Si les conditions d'exécution prévues à l'article 5.2 ne sont pas remplies, la Banque n'exécutera pas l'ordre de banque en ligne et communiquera au Participant des informations concernant la non-exécution et, dans la mesure du possible, les motifs de celle-ci ainsi que les possibilités de

corriger les erreurs ayant conduit au rejet via la banque en ligne.

6. **INFORMATIONS POUR LE PARTICIPANT SUR LES OPERATIONS DE BANQUE EN LIGNE**

La Banque informe le Participant au moins une fois par mois des opérations effectuées via la banque en ligne selon les modalités convenues pour les informations sur le compte, à condition qu'aucune dérogation ne soit prévue dans les conditions particulières convenues séparément (par exemple Conditions particulières pour l'épargne rien de dérogatoire n'est prévu.

7. **OBLIGATIONS DE DILIGENCE DU CLIENT**

7.1 **Protection des éléments d'authentification**

7.1.1. Le Participant doit prendre toutes les précautions raisonnables pour protéger ses éléments d'authentification (voir article 2 de ces conditions) contre tout accès non autorisé. Sinon, il existe un risque que la banque en ligne soit utilisée de manière abusive ou fasse autrement l'objet d'un accès non autorisé (voir articles 3 et 4 de ces conditions).

7.1.2. Pour protéger les éléments d'authentification individuels, le Participant doit particulièrement observer ce qui suit :

(i) Les éléments de connaissance, tels que par exemple le NIP, doivent être gardés secrets ; ils doivent particulièrement

- ne doivent pas être divulgués oralement (par exemple par téléphone ou en personne),
- pas au-delà banque en ligne sous forme de texte (par exemple via email ou service de messagerie),

- non stocké électroniquement sans protection (par exemple, stocker le NIP en texte en clair sur un ordinateur ou un appareil mobile) et

- non enregistré sur un appareil ni conservé sous forme de transcription avec un appareil servant d'élément de possession (par exemple, un appareil mobile) ou pour vérifier l'élément d'inhérence (par exemple, un appareil mobile avec une application de banque en ligne et un capteur d'empreintes digitales).

(ii) Les éléments de possession, tels que par exemple l'appareil mobile, doivent être protégés contre une utilisation abusive, en particulier

- veiller à ce que des personnes non autorisées ne puissent pas accéder à l'appareil mobile du Participant (par exemple, téléphone mobile), et
- veiller à ce que d'autres personnes ne puissent pas utiliser l'application de banque en ligne située sur l'appareil mobile (par exemple, application de banque en ligne, application d'authentification),
- l'application de banque en ligne (par exemple Application de banque en ligne, Application d'authentification) sur l'appareil mobile du Participant doit être désactivée avant que le Participant ne cède la propriété de cet appareil

mobile (par exemple par la vente ou l'élimination du téléphone mobile),

- preuve de l'élément de possession (par exemple TAN) ne doit pas être communiquée en dehors de la banque en ligne oralement (par exemple par téléphone) ou par écrit (par exemple par courriel, service de messagerie) et.
 - le Participant qui a reçu un code de la Banque pour activer l'élément de possession (par exemple un téléphone mobile avec l'application pour la banque en ligne) doit le conserver en toute sécurité afin d'empêcher tout accès non autorisé par d'autres personnes ; sinon, il existe un risque que d'autres personnes activent leur appareil en tant qu'élément de possession pour la banque en ligne du Participant.
- (iii) Les éléments personnels, tels que l'empreinte digitale du Participant, ne peuvent être utilisés comme élément d'authentification pour la banque en ligne sur l'appareil mobile du Participant que si aucun élément personnel d'autres personnes n'est stocké sur l'appareil mobile. Si des éléments personnels d'autres personnes sont stockés sur l'appareil mobile utilisé pour la banque en ligne, l'élément de connaissance délivré par la Banque (par exemple NIP) doit être utilisé pour la banque en ligne et non l'élément personnel stocké sur l'appareil mobile.

7.1.3. Avec la procédure TAN mobile, l'appareil mobile utilisé pour recevoir la TAN (par exemple téléphone mobile) ne doit pas être utilisé simultanément pour la banque en ligne.

7.1.4. Le numéro de téléphone mobile de référence enregistré pour la procédure TAN mobile doit être supprimé ou modifié si le Participant n'utilise plus ce numéro de téléphone pour la banque en ligne.

7.1.5. Nonobstant les obligations de protection en vertu de l'article 7.1.1 à 7.1.3, le Participant peut utiliser ses éléments d'authentification avec un service d'initiation de paiement et un service d'information sur les comptes qu'il a sélectionnés, ainsi qu'avec un autre service tiers (voir l'article 1.2 phrases 2 et 3 des présentes conditions). Le Participant doit sélectionner d'autres services tiers avec la diligence requise dans les transactions.

7.2 **Consignes de sécurité de la Banque**

Le Participant doit se conformer aux consignes de sécurité de la Banque concernant la banque en ligne, en particulier aux mesures de protection du matériel et des logiciels utilisés (système du client).

7.3 **Vérification des données de l'ordre avec celles affichées par la Banque**

La Banque affiche au Participant les données de l'ordre qu'elle a reçues (par exemple, montant, numéro de compte du bénéficiaire) via l'appareil convenu séparément du Participant (par exemple, au moyen d'un appareil mobile).

Le Participant est tenu de vérifier la conformité des données affichées avec les données envisagées pour l'ordre avant la confirmation. En cas

de divergences, l'opération doit être interrompue.

8. OBLIGATIONS D’AFFICHAGE ET DE NOTIFICATION

8.1 Avis de blocage

8.1.1. Constat par le Participant

- la perte ou le vol du téléphone mobile de référence, ou
- l’usage abusif ou toute autre utilisation non autorisée d’un élément d’authentification,

le doit Participant informer la Banque de cela sans délai (notification de blocage). Le Participant peut également soumettre une telle notification de blocage à la Banque à tout moment par les canaux de communication communiqués séparément.

8.1.2. Le Participant doit immédiatement déclarer tout vol ou usage abusif d’un élément d’authentification à la police.

8.1.3. Si le Participant soupçonne une utilisation non autorisée ou une utilisation frauduleuse de l’un de ses éléments d’authentification, il doit également soumettre une notification de blocage.

8.2 Notification d’opérations non autorisées ou mal exécutées

Le Participant doit notifier la Banque immédiatement dès la découverte d’une opération non autorisée ou mal exécutée.

9. RESTRICTION D’UTILISATION

9.1 Restriction initiée par le Participant

La Banque restreint sur instruction du Participant, notamment en cas de notification de restriction

conformément à article 8.1 des présentes conditions,

- l’accès à la banque en ligne pour lui ou tous les Participants ou
- ses éléments d’authentification pour l’utilisation de la banque en ligne.

9.2 Blocage à la demande de la Banque

9.2.1 La Banque peut bloquer l’accès à la banque en ligne à l’égard d’un Participant si

- elle est en droit de résilier la convention de banque en ligne pour motif légitime,
- des raisons objectives liées à la sécurité des éléments d’authentification du Participant le justifient ou
- un soupçon d’utilisation non autorisée ou frauduleuse d’un élément d’authentification existe.

9.2.2 la Banque informera le Participant, en précisant les motifs pertinents dès que possible, mais au plus tard immédiatement après le blocage. La fourniture des motifs peut être omise si cela contreviendrait aux obligations légales.

9.3 Levée du blocage

la Banque procédera à la levée du blocage ou remplacera les éléments d’authentification concernés si les raisons du blocage ne s’appliquent plus. Elle informera immédiatement le Participant.

9.4 Restriction d’accès au compte pour le service d’initiation de

**paiement et le service
d'information sur les comptes**

La Banque peut refuser au prestataire de services d'information sur les comptes ou au prestataire de services d'initiation de paiement l'accès au compte de paiement d'un Participant si des motifs fondés et dûment prouvés, liés à un accès non autorisé ou frauduleux du prestataire de services d'information sur les comptes ou du prestataire de services d'initiation de paiement au compte de paiement, y compris le lancement non autorisé ou frauduleux d'une opération de paiement, justifient ce refus. La Banque informera le Participant de ce refus d'accès. La notification sera effectuée avant, ou au plus tard immédiatement après, le refus d'accès. Les motifs ne pourront être divulgués dans la mesure où cela entraînerait une violation par la Banque des obligations légales applicables. Dès que les motifs du refus d'accès auront cessé d'exister, la Banque lèvera la restriction d'accès au compte. Le Participant en sera immédiatement informé.

10. RESPONSABILITE**10.1 Responsabilité de la Banque pour les modifications incorrectes ou non autorisées des informations spécifiques au client**

la Banque est responsable de tout dommage résultant d'une modification non autorisée, ou d'une modification des informations spécifiques au client (telles qu'un changement des coordonnées de contact ou du NIP) qui n'est pas effectuée, est incorrecte, ou est retardée.

10.2 Responsabilité de la Banque pour l'exécution d'une opération non autorisée et d'une opération**incorrecte, défectueuse ou exécutée tardivement**

La Responsabilité de la Banque pour un ordre non autorisé et pour un ordre non exécuté, exécuté de manière incorrecte ou exécuté tardivement est régie par les conditions particulières convenues pour le type d'ordre respectif (par exemple, conditions pour les virements).

10.3 Responsabilité du Participant en cas d'usage abusif de leurs éléments d'authentification**10.3.1. Responsabilité du Participant en cas d'accès non autorisé et de modification d'informations propres à l'utilisateur avant la notification de blocage**

(i) Si un accès non autorisé et une modification d'informations propres à l'utilisateur avant la notification de blocage sont fondés sur l'utilisation d'un élément d'authentification perdu, volé ou autrement égaré, ou sur un autre usage abusif d'un élément d'authentification, le Participant est responsable du dommage causé à la Banque en conséquence, à condition que la perte, l'égarement ou un autre usage abusif de l'élément d'authentification soit dû à un acte fautif ou négligent du Participant.

(ii) Le Participant n'est pas tenu d'indemniser le dommage en vertu du paragraphe (i) si

- il ne lui a pas été possible de constater la perte, vol, égarement, ou tout autre usage abusif de l'élément d'authentification avant l'accès non autorisé accès

et modification constater,
ou

- la perte de l'élément d'authentification a été causée par un employé, un agent, une succursale d'un prestataire de services de paiement, ou une autre entité à laquelle les activités du prestataire de services de paiement ont été externalisées.

10.3.2. Responsabilité du Participant pour les services de paiement non autorisés avant la notification de blocage

- (i) Si des opérations de paiement non autorisées avant la notification de blocage sont fondées sur l'utilisation d'un élément d'authentification perdu, volé ou autrement égaré, ou sur l'usage abusif d'un élément d'authentification, le Participant est responsable du dommage causé à la Banque qui en résulte, jusqu'à concurrence de 50 euros, indépendamment du fait que le Participant soit en faute.
- (ii) Le Participant n'est pas responsable de l'indemnisation des dommages en vertu du paragraphe (i) si
- il n'était pas possible pour eux de détecter la perte, le vol, l'égarement ou toute autre utilisation non autorisée de l'élément d'authentification avant que l'opération de paiement non autorisée ne survienne, ou
 - la perte de l'élément d'authentification a été causée par un employé, un agent, une succursale

d'un prestataire de services de paiement, ou une autre entité à laquelle les activités du prestataire de services de paiement ont été externalisées.

10.3.3. Si des opérations de paiement non autorisées ou un accès non autorisé et une altération des informations spécifiques au client surviennent avant l'Avis de blocage, et que le Participant a agi avec intention frauduleuse ou a manqué à ses obligations de notification et de diligence au titre des présentes conditions soit intentionnellement, soit avec faute lourde, le Participant supporte, contrairement au paragraphe (ii) des sections 10.3.1 et 10.3.2, l'intégralité du dommage encouru. Une faute lourde du Participant peut notamment être présente s'il n'adhère pas à l'une quelconque de ses obligations de diligence en vertu

- section 7.1.2 ou
- section 7.1.3 phrase 2 ou
- section 7.3 ou
- section 8.1.1

a violé les présentes conditions.

10.3.4. Nonobstant les paragraphes (i) des sections 10.3.1 et 10.3.2 et de la section 10.3.3, le Participant n'est pas tenu de payer une indemnisation si la Banque n'a pas demandé une authentification forte du client au Participant conformément à l'article 2, 45° de la loi belge du 11 mars 2018 relative au statut et au contrôle des établissements de paiement et des établissements de monnaie électronique. L'authentification forte du client exige notamment l'utilisation de deux éléments d'authentification classés indépendamment parmi les

catégories connaissance, possession ou inhérence (voir section 2.3 des présentes conditions).

10.3.5. La Responsabilité pour les dommages causés pendant la période pour laquelle le plafond de disposition s'applique est limitée au plafond de disposition convenu.

10.3.6. Le Participant n'est pas obligé d'indemniser les dommages au titre de l'article (i) des articles 10.3.1 et 10.3.2 et de l'article 10.3.3 si le Participant n'a pas pu fournir l'Avis de blocage conformément à l'article 8.1 des présentes conditions parce que la Banque n'a pas garanti la possibilité de recevoir l'Avis de blocage.

10.3.7. paragraphes (ii) des articles 10.3.1 et 10.3.2 et l'article 10.3.4 à 10.3.6 ne s'appliquent pas si le Participant a agi avec intention frauduleuse.

10.4 **Responsabilité du client pour les opérations non autorisées en dehors des services de paiement avant l'Avis de blocage**

Si des opérations non autorisées en dehors des services de paiement (par exemple, des opérations sur dépôts) avant l'Avis de blocage sont fondées

sur l'utilisation d'un élément d'authentification perdu ou volé ou sur un autre usage abusif de l'élément d'authentification et que cela a causé un dommage à la Banque, le Participant et la Banque sont responsables conformément aux principes juridiques de la faute partagée.

10.5 **Responsabilité de la Banque à partir de l'Avis de blocage**

Dès que la Banque a reçu un Avis de blocage d'un Participant, elle assume la responsabilité de tous les dommages en résultant par la suite dus à des opérations de banque en ligne non autorisées ou modifications. Ceci ne s'applique pas si le Participant a agi avec une intention frauduleuse.

10.6 **Clause de non-responsabilité**

Les Actions en responsabilité sont exclues si les circonstances à l'origine de la réclamation reposent sur un événement inhabituel et imprévisible sur lequel la partie invoquant cet événement n'a exercé aucune influence et dont les conséquences n'auraient pas pu être évitées malgré l'exercice de la diligence requise.

B. Conditions particulières pour la Communication électronique

1. Introduction

1.0 La Communication entre la Banque et le client se déroulera généralement par voie électronique via la banque en ligne. La Banque et le client conviennent que la Banque peut utiliser la fonctionnalité de banque en ligne pour la communication avec le client et, en particulier, pour la fourniture de documents et d'informations au client (par exemple, des relevés de compte).

1.1 Le client peut utiliser la fonctionnalité de banque en ligne notamment pour récupérer, consulter en ligne, télécharger, imprimer et archiver les documents fournis par la Banque.

2. Configuration et options d'utilisation

2.0 la Banque crée une section dédiée dans l'espace de banque en ligne destinée à la communication électronique pour le client l'«Espace de communication en ligne». La Banque peut renommer ou modifier techniquement l'Espace de communication en ligne sans affecter sa fonction en tant que canal convenu pour la communication électronique à tout moment.

2.1 Dès que la fonctionnalité est disponible, le client peut utiliser la fonction de messagerie au sein de l'Espace de communication en ligne pour envoyer des messages à la Banque (tels que des questions sur le compte, des demandes de rappel ou des mises à jour des coordonnées de contact). L'Envoi de documents ou de graphiques du client à la Banque via l'Espace de communication en ligne est exclu sauf s'il est explicitement activé par la Banque.

2.2 Si la relation d'affaires ne prend pas effet ou est ensuite résiliée (par

exemple, par l'exercice d'un droit de rétractation légal), la Banque peut immédiatement désactiver la fonctionnalité de banque en ligne, y compris l'Espace de communication en ligne et, si nécessaire, supprimer le contenu.

2.3 La Banque est en droit à tout moment de bloquer ou restreindre l'accès partiellement ou complètement à la fonctionnalité de banque en ligne, y compris l'Espace de communication en ligne, si des circonstances justifient l'hypothèse que la sécurité des accès est compromise, un accès non autorisé ou frauduleux peut être possible, ou la Banque est en droit de résilier la relation d'affaires avec le client pour motif légitime.

3. Mise à disposition des documents et renonciation du client à d'autres modes de remise

3.0 Le client déclare son consentement à ce que la Banque fournisse tous les documents relatifs à la relation d'affaires entre le client et la Banque chiffré et avec force obligatoire dans l'Espace de communication en ligne, sauf si expressément convenu par écrit avec le client ou requis par la loi.

3.1 Le client reconnaît et déclare son consentement que de tels documents n'ont pas besoin de lui être fournis d'une autre manière. Le client renonce particulièrement à l'envoi postal de ces documents.

3.2 Toutefois, la Banque reste en droit de fournir au client des informations et des documents par d'autres moyens appropriés si la loi l'exige ou si cela s'avère raisonnable au vu d'autres circonstances (par exemple, en cas de panne temporaire du service de banque en ligne).

3.3 Nonobstant cela, la Banque est en droit d'envoyer des documents individuels ou tous les documents au client par envoi postal ou autrement en cas de problèmes techniques si elle estime que cela est approprié au regard des intérêts du client.

4. **Moment d'accès**

4.0 Les documents déposés par la Banque dans l'Espace de communication en ligne sont réputés reçus lorsque le client a été informé par la Banque du dépôt et de la possibilité de récupération via la zone de banque en ligne, et qu'un accusé de réception habituel par le client peut être supposé, c'est-à-dire au plus tard le jour ouvrable suivant l'information de la Banque. Si le client a déjà récupéré les documents plus tôt, ils sont réputés reçus à ce moment antérieur. Cette disposition relative au caractère réputé reçu ne porte pas atteinte au point de départ de tout délai légal de rétractation impératif, lequel court à compter de la date à laquelle le client a effectivement reçu les informations précontractuelles pertinentes exigées par le droit impératif applicable.

4.1 À partir du Moment d'accès où le document respectif est réputé reçu conformément à la section 4.1, les délais liés à cette réception commencent (par ex., un délai de rétractation).

5. **Intégrité des documents dans l'espace de banque en ligne**

5.0 La Banque garantit l'immutabilité des documents au sein de l'Espace de communication en ligne.

5.1 Cette obligation ne s'applique pas si les documents sont conservés ou conservés en mémoire en dehors de l'Espace de communication en ligne. Une fois que ces documents sont

conservés ou utilisés par le client en dehors de l'Espace de communication en ligne (par exemple, après téléchargement), la Banque n'assume aucune responsabilité pour l'intégrité des documents ou leur contenu.

5.2 En raison de paramètres matériels ou logiciels individuels, une impression ne correspond pas toujours visuellement à l'affichage à l'écran.

6. **Notification**

6.0 Lorsqu'un nouveau document est téléchargé dans l'Espace de communication en ligne, la Banque enverra une Notification par e-mail à l'adresse électronique fournie par le Client. Le Client vérifiera régulièrement son application de messagerie électronique personnelle et les dossiers de courrier indésirable de l'application de messagerie électronique qu'il utilise. Le Client accepte de recevoir ces notifications non chiffrées par e-mail.

6.1 Le Client est tenu de veiller à ce que l'adresse électronique fournie pour la réception des e-mails lors de l'établissement de la relation d'affaires avec la Banque soit prête à l'emploi. Le Client est tenu d'informer la Banque sans délai de toute modification de l'adresse électronique.

7. **Obligation de coopération du client**

7.0 Le client est tenu de vérifier l'Espace de communication en ligne à des intervalles réguliers et raisonnables, mais au moins une fois par mois, et sans délai à l'occasion d'événements spécifiques (par ex., après des instructions à la Banque ou après un courriel de notification conformément à la section 6.1 des présentes conditions) pour les messages entrants.

7.1 Par la présente, le Client déclare que la Banque a rempli ses obligations de transmission et de notification avec la réception des documents dans l'Espace de communication en ligne et l'email de notification correspondant adressé au client.

7.2 Le Client est tenu de récupérer les documents publiés par la Banque dans l'Espace de communication en ligne et d'en vérifier le contenu pour en assurer l'exactitude et l'exhaustivité.

7.3 Nonobstant l'article [6 (2)] des Conditions générales de la Banque, le client doit notifier à la Banque les réclamations rapidement après réception des documents, au moins sous forme textuelle (par exemple, via une application de messagerie électronique ou en utilisant l'Espace de communication en ligne).

8. **Durée de conservation**

Les documents fournis dans l'Espace de communication en ligne sont disponibles pendant toute la durée de la relation d'affaires respective entre le Client et la Banque. Après la résiliation de la relation d'affaires respective entre le Client et la Banque, les documents fournis dans l'Espace de communication en ligne resteront accessibles pendant 30 jours calendaires supplémentaires jusqu'à la suspension de l'intégralité de la fonction de banque en ligne. Le Client est responsable de la conservation des documents après la résiliation de la relation d'affaires. Toute obligation légale de conservation de la Banque demeure inchangée.

9. **Reconnaissance des documents**

la Banque ne garantit pas que les documents publiés dans l'Espace de communication en ligne seront acceptés par des tiers, notamment

les autorités et institutions compétentes (telles que les autorités fiscales). Le Client est tenu d'obtenir de manière indépendante des informations auprès de l'autorité ou de l'institution responsable le concernant quant à l'acceptation des documents.

10. **Maintenance et modification des services**

10.0 La Banque peut restreindre, redéfinir, développer davantage ou cesser l'Espace de communication en ligne, en partie, et/ou imposer des conditions à son utilisation par le Client.

10.1 La Banque informera le Client de telles modifications et/ou de la cessation de l'Espace de communication en ligne avec un préavis approprié et, le cas échéant, conseillera le Client sur une méthode de communication alternative.

10.2 La Banque ne garantit pas la disponibilité constante et ininterrompue de l'Espace de communication en ligne ni les documents qui y sont contenus. La Banque peut interrompre l'accès à l'Espace de communication en ligne notamment pour des plages de maintenance.

10.3 L'accès peut également être interrompu en raison de circonstances indépendantes de la volonté de la Banque (par exemple, panne de connexion internet).

11. **Fin de la relation d'affaires**

Après la fin de la relation d'affaires respective entre le Client et la Banque, les documents seront disponibles dans l'Espace de communication en ligne pendant 30 jours calendaires supplémentaires. Après cette période, la Banque est en droit de

bloquer l'accès à l'Espace de
communication en ligne.