DISPOSITIONS PARTICULIÈRES RELATIVES AUX SERVICES BAS E-BANKING

BANQUE ALTERNATIVE SUISSE

Les dispositions particulières relatives aux services e-BAS e-banking régissent l'utilisation des services BAS e-banking par la/le client-e et d'autres utilisatrices-teurs. La/Le « **cocontractant-e** » est la personne qui a établi la relation d'affaires avec la banque. Les « **utilisatrices-teurs** » sont les personnes qui utilisent les services e-banking en tant que cocontractant-e ou mandataire.

En utilisant les services e-banking, la/le client-e ou l'utilisatrice-teur accepte les présentes dispositions particulières relatives aux services BAS e-banking ainsi que la déclaration de confidentialité. Les conditions générales (CG), le règlement de dépôt ainsi que les autres conventions conclues entre la/le client-e et la banque sont contraignants pour l'utilisatrice-teur. La/Le client-e est tenu d'informer les utilisatrices-teur de ces dispositions et de leur communiquer toutes les autres informations essentielles, en particulier concernant les risques.

La banque se réserve le droit de modifier à tout moment les dispositions particulières relatives aux services BAS e-banking.

1. Étendue des services e-banking

Les services e-Banking permettent à la/au client-e d'effectuer ses opérations bancaires en ligne et de consulter des informations. Elle/Il peut notamment consulter des informations sur son compte et son dépôt, transmettre des ordres de paiement et de bourse, consulter des informations sur ses cartes et procéder à des mutations de carte.

L'étendue des services e-banking disponibles est définie par la banque et peut être modifiée, développée, augmentée ou réduite à tout moment.

2. Accès aux services e-banking

2.1 Conditions techniques

Les services e-banking sont accessibles via Internet par l'intermédiaire d'un opérateur de réseau (fournisseur d'accès internet). À cette fin, l'utilisatrice-teur doit disposer du matériel et des logiciels appropriés, qui relèvent de sa responsabilité.

L'utilisatrice-teur est tenu de prendre les mesures de sécurité nécessaires, notamment de protéger de manière adéquate ses terminaux contre tout accès non autorisé par des tiers et contre les cyber-risques, et de maintenir à jour les paramètres de sécurité de ses terminaux.

2.2 Vérification de la légitimation

L'accès aux services e-banking est accordé à toute personne qui s'est légitimée vis-à-vis de la banque en saisissant ses données de légitimation personnelles (telles que l'identification via l'application BAS banking, un mot de passe, des codes de légitimation, un token matériel, ci-après dénommés « moyens de légitimation »). Les moyens de légitimation personnels sont mis à la disposition de l'utilisatrice-teur pour une utilisation conforme à leur destination. La banque peut à tout moment remplacer ou modifier les moyens de légitimation pour des raisons objectives.

Si une légitimation est effectuée au moyen de données biométriques, il incombe à l'utilisatrice-teur de s'assurer qu'elle/il est la seule personne dont les données biométriques sont enregistrées sur l'appareil. La banque n'a pas la possibilité de consulter les données biométriques enregistrées sur l'appareil d'accès concerné, ni de les contrôler ou de les influencer. L'appareil utilisé doit être protégé par l'utilisatrice-teur contre tout accès non autorisé.

Dans le cadre de la vérification de la légitimation, la banque est autorisée à communiquer à des tiers mandatés les moyens de légitimation de l'utilisatrice-teur.

2.3 Responsabilité d'utilisation

La/Le client-e assume les risques et les dommages causés par les utilisatrices-teurs lors de l'utilisation des services e-banking.

Toute personne qui se légitime avec les moyens de légitimation, indépendamment de sa relation juridique interne avec la/le client-e, d'inscriptions au registre du commerce, de publications ou de réglementations divergentes dans les documents de signature, peut être considérée par la banque comme un-e utilisatrice-teur correctement légitimé-e. La banque peut donc accepter, sans vérification supplémentaire de la légitimité, des ordres et des communications juridiquement contraignantes de la part d'une telle personne. Cela vaut également si cette personne est un utilisatrice-teur non autorisé qui a pu se légitimer. La/Le client-e est responsable de l'ensemble des actions effectuées sur la base de la vérification de la légitimation susmentionnée.

La/Le client-e reconnaît sans réserve toutes les transactions, opérations, conventions et déclarations qui sont effectuées dans le cadre des services e-banking en utilisant les moyens de légitimation de l'utilisatrice-teur. Tous les ordres, instructions et communications qui parviennent à la banque par ce biais sont contraignants pour la/le client-e.

2.4 Passation d'ordres

La banque est chargée par la/le client-e d'exécuter les ordres qui lui sont transmis par le biais des services e-banking ainsi que de se conformer aux instructions et communications, si la vérification de la légitimation a été effectuée conformément au système. Si des ordres sont transmis à la banque dans le cadre de l'utilisation des services e-banking, celle-ci est en droit d'en refuser certains à sa discrétion.

Si l'utilisatrice-teur n'a pas été désigné-e séparément comme mandataire de la/du client-e auprès de la banque en dehors des services e-banking et que la banque l'a accepté en tant que tel, la banque n'exécute aucun ordre ni instruction que l'utilisatrice-teur aurait transmis en dehors des services e-banking.

La banque a le droit, à tout moment et sans indication de motif, de refuser des instructions, des ordres et des communications via les services e-banking.

Si l'utilisatrice-teur a passé à la banque un ordre qui n'a pas été exécuté ou qui n'a été exécuté que partiellement, elle/il doit immédiatement introduire une réclamation auprès de la banque.

2.5 Blocage de l'accès

L'utilisatrice-teur peut bloquer lui-même son accès aux services e-banking ou le faire bloquer. La/Le client-e peut demander à la banque de bloquer l'accès d'un utilisatrice-teur. Le blocage peut être demandé pendant les heures d'ouverture habituelles auprès de l'agence bancaire qui gère le compte ou, en dehors des heures d'ouverture habituelles, auprès de la hotline e-banking et doit être confirmé immédiatement par écrit à la banque.

En cas d'urgence, l'utilisatrice-teur peut bloquer son accès de sa propre initiative en saisissant délibérément plusieurs fois des identifiants erronés jusqu'à ce que le blocage de sécurité soit activé. Le blocage peut être levé par la banque sur demande de la/du client-e.

S'il existe des raisons de soupçonner que des tiers non autorisés ont eu connaissance des moyens de légitimation de l'utilisatrice-teur ou ont eu accès aux services e-banking, ou en cas de soupçon d'abus, l'utilisatrice-teur doit immédiatement faire procéder au blocage et en informer la banque.

La banque est à tout moment en droit de bloquer totalement ou partiellement l'accès de l'utilisatrice-teur, sans indication de motifs et sans préavis.

3. Coûts et indemnisation

Les prestations générales fournies par la banque dans le cadre des services e-banking sont mises gratuitement à la disposition de la/du client-e. La banque se réserve le droit d'introduire des frais applicables à l'utilisation des services e-banking ou de modifier ceux-ci. L'introduction de frais ou la modification des frais est communiquée à la/au client-e par voie électronique, par notification dans les services e-banking ou par tout autre moyen approprié. À défaut d'une opposition écrite dans un délai d'un mois à compter de la notification, l'introduction ou la modification est considérée comme approuvée.

La/Le client-e autorise la banque à débiter les frais et commissions éventuels d'un compte à son nom.

4. Devoirs de diligence

L'utilisatrice-teur est tenu de modifier immédiatement le mot de passe qui lui a été communiqué par la banque. L'utilisatrice-teur doit ensuite modifier régulièrement son mot de passe.

L'utilisatrice-teur est tenu de garder secrets tous les moyens de légitimation et de les protéger contre toute utilisation abusive par des personnes non autorisées. En particulier, un mot de passe ne doit pas être enregistré après sa modification, ni conservé sans protection sur l'ordinateur de l'utilisatrice-teur, ni communiqué à des tiers non autorisés. Le mot de passe ne doit pas non plus être composé de données évidentes ou faciles à deviner (telles que des noms, des dates de naissance, des numéros de téléphone, des plaques d'immatriculation, etc.).

La banque ne contactera à aucun moment la/le client-e ou l'utilisatrice-teur par voie électronique ou téléphonique pour lui demander ses données d'accès ou lui demander de communiquer ses moyens de légitimation pour l'utilisation des services e-banking.

La/Le client-e supporte toutes les conséquences résultant de la divulgation et de l'utilisation abusive des moyens de légitimation des utilisatrices-teurs.

L'utilisatrice-teur prend acte du fait qu'il doit saisir lui-même tous les ordres à traiter dans le cadre des services e-banking. En règle générale, les ordres saisis de manière erronée ne peuvent pas être modifiés. La banque n'a aucune obligation de surveillance.

5. Relevés de compte/dépôt électroniques

La/Le client-e reconnaît que les communications écrites et les communications sous forme électronique ont la même valeur contraignante.

Dès que les relevés de compte/dépôt électroniques sont accessibles à l'utilisatrice-teur dans l'environnement des services e-banking, ils sont considérés comme ayant été remis à la/au client-e. Une fois que l'utilisatrice-teur a consulté les relevés de compte/dépôt électroniques, ceux-ci restent disponibles pendant au moins trois mois.

L'utilisatrice-teur est seul-e responsable de la conservation des relevés de compte/dépôt. Les conditions générales de la banque s'appliquent à toute réclamation concernant les transactions effectuées. La/Le client-e a le droit d'obtenir à tout moment les relevés de compte/dépôt sous forme papier. La/Le client-e accepte le barème des frais de la banque.

6. Canal de communication sécurisé

Dans le cadre des services e-banking, la banque met à la disposition de l'utilisatrice-teur un canal de communication sécurisé avec la banque, par lequel l'utilisatrice-teur et la banque peuvent échanger des messages et des documents. Les messages et documents transmis par l'utilisatrice-teur sont traités pendant les heures d'ouverture habituelles de la banque.

Aucun ordre urgent (tel que des ordres de paiement ou des ordres boursiers) ne doit être transmis via le canal de communication sécurisé.

Les messages et les documents sont réputés avoir été remis à la/au client-e dès qu'ils deviennent accessibles à l'utilisatrice-teur dans l'environnement des services e-banking. L'utilisatrice-teur doit donc s'assurer de prendre connaissance en temps utile des communications et documents correspondants et d'en informer la/le client-e.

La banque est autorisée à supprimer les documents mis à disposition sous forme numérique dans l'e-banking en cas de dépassement de l'espace de stockage ou à l'expiration d'un délai.

7. Signature électronique de documents

Certains documents peuvent être signés électroniquement à l'aide de services e-banking, conformément à l'autorisation de signature. Les documents mis à disposition pour une signature électronique doivent être soigneusement vérifiés par l'utilisatrice-teur en ce qui concerne leur exhaustivité et leur exactitude. En cas d'incomplétude ou d'inexactitude, l'utilisatrice-teur doit immédiatement introduire une réclamation auprès de la banque. Ces documents peuvent être signés numériquement. En signant électroniquement ces documents, la/le client-e déclare accepter leur contenu et confirme les avoir lus et compris. Les documents signés électroniquement ont la même valeur que ceux signés à la main. Les copies imprimées signées à la main a posteriori n'ont de valeur juridique que si elles sont acceptées par la banque.

L'utilisatrice-teur fournit à la banque les données nécessaires à l'émission des certificats de signature électronique (prénom, nom, date de naissance, nationalité, type et numéro de pièce d'identité) et autorise la banque à les transmettre à un prestataire de services de certification mandaté par la banque pour ce faire.

Les documents signés dans l'environnement des services e-banking sont mis à disposition de l'utilisatrice-teur par la banque pour une durée déterminée. L'utilisatrice-teur doit enregistrer ces documents en dehors des services e-banking.

La/Le client-e reconnaît expressément la validité et la force probante des certificats et signatures électroniques émis par les prestataires de services de certification utilisés par la banque pour toutes les actions et transactions avec celle-ci.

8. Services de notification

Dans le cadre des services e-banking, la banque offre à l'utilisatrice-teur la possibilité d'être informé de certains événements par voie de communication électronique (par exemple, SMS, courriel ou notifications push). En activant les services de notification, l'utilisatrice-teur accepte explicitement l'envoi des notifications sélectionnées. La/Le client-e et l'utilisatrice-teur prennent acte du fait que ces notifications impliquent la transmission de données à caractère personnel et de données soumises au secret bancaire. Cette transmission peut s'effectuer via des canaux non sécurisés qui ne sont pas contrôlés par la banque.

Pour des raisons techniques, la banque ne peut pas garantir que ces notifications parviennent effectivement à l'utilisatrice-teur. Les raisons techniques peuvent être, par exemple, des retards, des erreurs d'acheminement ou des interruptions de service.

9. Interface API vers des prestataires tiers

9.1 Étendue

La banque propose à la/au client-e ou aux utilisatrices-teur l'échange de données et d'informations liées aux comptes et aux dépôts avec des prestataires tiers (par ex. des fintech) (« échange d'informations »), lorsque cela est nécessaire à la fourniture de certains services. Cet échange d'informations s'effectue via une interface API (Application Programming Interface) sécurisée mise à disposition par la banque. Grâce à cette interface, les utilisatrices-teurs peuvent utiliser des logiciels ainsi que d'autres solutions techniques et services de prestataires tiers en lien avec les services e-banking de la banque. La sélection minutieuse d'un prestataire de services tiers et sa surveillance incombent exclusivement à l'utilisatrice-teur. La banque n'a aucune obligation de surveillance ou de contrôle du prestataire tiers.

La banque transmet les données au prestataire tiers conformément aux instructions de l'utilisatrice-teur. Le prestataire tiers correspondant doit être sélectionné et activé par l'utilisatrice-teur.

La transmission des données s'effectue indirectement via la plateforme « bLink » de SIX BBS AG (SIX) (« plateforme »). L'obligation de la banque se limite à la transmission des données ou à la réception de données (« cas d'utilisation ») via cette interface. La banque publie les cas d'utilisation proposés sur son site Internet.

Une fois l'interface validée par la banque, cette dernière répondra aux demandes de données correspondantes et acceptera les ordres des prestataires de services tiers (« appels de service »). Si l'appel de service contient un ordre à la banque (par ex. un ordre de paiement), une validation supplémentaire dans les services e-banking de la banque peut être nécessaire.

Les données transmises dans le cadre de l'échange d'informations peuvent différer des autres données et justificatifs communiqués par la banque. La valeur des transactions peut par exemple être comptabilisée à la date de la transaction et non à la date de valeur.

La banque se réserve le droit d'adapter l'étendue de l'offre de services. Notamment, de nouveaux cas d'utilisation peuvent être ajoutés, tandis que les cas existants peuvent être modifiés ou interrompus.

9.2 Clé d'identification

Après l'activation de l'échange d'informations dans les services e-banking de la banque à l'aide des moyens de légitimation valides, la banque émettra une clé d'identification électronique (« token »). Le token est transmis par la banque au prestataire tiers via la plateforme. La banque n'a aucune influence sur l'utilisation légitime du token par le prestataire tiers. Si un appel de service provenant du prestataire tiers ou de la plateforme est muni du token correspondant, la banque y répond. Le prestataire tiers est lui-même responsable de la gestion sécurisée et du traitement des données qu'il effectue. La banque n'assume aucune obligation de surveillance ou autre à cet égard.

9.3 Obligations de diligence particulières

Si l'utilisatrice-teur souhaite mettre fin à l'échange d'informations entre la banque et un prestataire de services tiers qu'il a sélectionné et activé, ou le limiter à certains appareils, il doit supprimer ou restreindre l'échange d'informations avec ce prestataire tiers. La résiliation ou la restriction doit être effectuée dans les services e-banking de la banque. Jusqu'à ce que l'utilisatrice-teur procède à cette suppression ou restriction, les appels de service du prestataire tiers continueront d'être traités.

Le prestataire tiers vérifie l'autorisation d'accès de l'utilisatrice-teur à l'aide des moyens de légitimation qui lui ont été délivrés. L'utilisatrice-teur garde ces moyens de légitimation confidentiels conformément aux dispositions du prestataire tiers et les protège contre toute utilisation abusive par des personnes non autorisées.

La/Le client-e prend acte du fait que l'ensemble des utilisatrices-teurs peuvent configurer des interfaces API correspondantes avec des prestataires tiers.

9.4 Prestataires de services tiers agréés

Les utilisatrices-teurs peuvent sélectionner eux-mêmes les prestataires tiers à activer. Ils ne peuvent toutefois sélectionner que des prestataires tiers agréés par la banque et la plateforme. La banque se réserve le droit d'exclure certains prestataires tiers sans avoir à en indiquer les motifs.

La/Le client-e et les utilisatrices-teurs prennent acte du fait que les droits d'accès accordés auprès du prestataire tiers peuvent différer de ceux accordés auprès de la banque. Le prestataire tiers fournit ses services sans intervention ni contrôle de la part de la banque. Il incombe donc à la/au client-e ou à l'utilisatrice-teur de contrôler les droits d'accès auprès du prestataire tiers et de les modifier si nécessaire.

9.5 Utilisation des données par le prestataire de services tiers

La/Le client-e et les utilisatrices-teurs reconnaissent que la transmission de données au prestataire tiers via la plateforme implique que ce dernier prend connaissance des données correspondantes. Par la présente, elles/ils déchargent la banque de ses obligations de confidentialité et consentent à la divulgation de ces données. Le flux de données s'effectue via l'appel de services, qui est envoyé indirectement à la banque par le prestataire tiers via la plateforme.

La transmission des données, qu'elle soit effectuée via la plateforme vers le prestataire tiers ou du prestataire tiers vers les systèmes des utilisatrices-teurs, ainsi que l'utilisation des données par le prestataire tiers lui-même, sont régies exclusivement par les contrats du prestataire tiers, en particulier sa politique de confidentialité. Le prestataire tiers est seul responsable de la sécurité et du respect des règles de protection des données dans le cadre de ses prestations. La banque n'exerce aucun contrôle et n'a aucune influence sur l'utilisation des données ni sur les mesures de sécurité mises en place par le prestataire tiers. Les données peuvent être stockées également à l'étranger par ce dernier. Dans ce cas, les données ne sont pas soumises aux dispositions de protection du droit suisse, notamment au secret bancaire. Le prestataire tiers agit exclusivement en qualité de personne auxiliaire engagée par l'utilisatrice-teur. Par conséquent, la banque décline toute obligation de surveillance ou de contrôle et toute autre responsabilité pour les prestations ou omissions du prestataire tiers.

9.6 Utilisation des données par la plateforme

Les données de la/ du client-e ou de l'utilisatrice-teur peuvent être traitées et enregistrées par l'exploitant de la plateforme. Elles peuvent être utilisées par l'exploitant de la plateforme aux fins suivantes :

- Exploitation de la plateforme
- Assistance et surveillance des requêtes de données et des ordres
- Extension de l'échange d'informations

La banque n'a aucun contrôle sur l'utilisation des données par l'exploitant de la plateforme.

9.7 Utilisation des données par la banque

La/Le client-e et l'utilisatrice-teur acceptent que la banque utilise les données qu'elle reçoit de tiers dans le cadre de l'échange d'informations à des fins de conseil global, qu'elle les vérifie et qu'elle les réutilise dans le cadre des dispositions légales.

9.8 Responsabilité lors de l'utilisation de l'échange d'informations

La banque n'a aucune influence sur l'échange d'informations, la prestation de services par le prestataire tiers et l'exploitant de la plateforme. La banque n'exerce aucune fonction de surveillance ou de contrôle sur le prestataire tiers et l'exploitant de la plateforme et elle décline toute garantie ou responsabilité pour leurs activités ou omissions.

10. Multibanking

10.1 Étendue

Avec le multibanking, l'utilisatrice-teur peut demander à la banque de recevoir des données provenant de banques tierces ainsi que de leur transmettre des instructions. À cette fin, la banque met à disposition des interfaces appropriées ou fait appel aux plateformes d'un prestataire de services tiers (par exemple bLink de SIX BBS AG).

La banque se réserve le droit de refuser l'intégration de banques tierces si celles-ci ne répondent pas à ses exigences internes. En outre, la banque se réserve le droit de refuser les transmissions de données incomplètes (par exemple, les ordres de paiement incomplets).

10.2 Clé d'identification

Le processus d'activation et l'échange de données subséquent entre la banque et le compte d'une banque tierce connecté au multibanking s'effectuent à l'aide de leur token. Ce token est associé au moyen de légitimation valable pour les services e-banking.

10.3 Obligations de diligence particulières lors de l'utilisation du multibanking

L'utilisatrice-teur est tenu de vérifier les données transmises à une banque tierce (par ex. les ordres de paiement) et d'informer immédiatement la banque tierce en cas d'éventuelles divergences.

10.4 Protection des données lors de l'utilisation du multibanking

La/Le client-e et l'utilisatrice-teur acceptent que la banque utilise les données qu'elle reçoit de tiers dans le cadre du multibanking à des fins de conseil global, qu'elle les vérifie et qu'elle les réutilise dans le cadre des dispositions légales.

10.5 Responsabilité lors de l'utilisation du multibanking

La banque décline toute responsabilité concernant les plateformes de prestataires tiers, les banques tierces ainsi que les tiers auxquels ils font appel. La prestation de services est fournie avec le soin habituel dans le secteur bancaire. La banque n'exerce toutefois aucune influence ni fonction de surveillance sur les plateformes des prestataires tiers, les banques tierces ou les tiers auxquels ils font appel.

11. Factures électroniques (eBill)

La banque offre à l'utilisatrice-teur la possibilité de participer au système de facturation eBill et de recevoir et régler des factures électroniques. Les factures peuvent être validées soit individuellement, soit de manière groupée ou permanente. L'utilisatrice-teur définit les règles correspondantes.

Pour pouvoir participer au système de facturation eBill, la/le client-e doit s'identifier dans le cadre des services e-banking et s'enregistrer une seule fois auprès de SIX sur le portail eBill.

L'utilisatrice-teur peut autoriser directement le paiement des factures électroniques reçues via le système eBill dans le cadre des services e-banking ou les refuser par voie électronique. L'utilisatrice-teur est responsable de vérifier l'exactitude et l'exhaustivité des ordres de paiement.

La banque ne garantit pas l'exactitude et l'exhaustivité des factures électroniques. Toute réclamation concernant ces factures (par exemple, mode de livraison, contenu et montant) doit être adressée par la/le client-e à l'émetteur de la facture.

Le service eBill est fourni par SIX Paynet AG.

12. Particularités des opérations bancaires sur Internet et le réseau public de télécommunications

Dans le cadre de l'utilisation des services e-banking, les données entrantes et sortantes de la banque sont cryptées par celle-ci, à l'exception des informations relatives à l'expéditeur et au destinataire, pour autant que les procédés techniques utilisés le permettent.

La/Le client-e reconnaît qu'Internet et le réseau public de radiocommunications constituent des réseaux mondiaux et ouverts, accessibles en principe à tous, et que les services e-banking sont échangés entre l'utilisatrice-teur et la banque via des installations publiques non spécialement protégées. Cela s'applique aussi bien aux instructions électroniques de l'utilisatrice-teur reçues par la banque qu'aux messages électroniques transmis par la banque à l'utilisatrice-teur. Les données transmises via Internet peuvent quitter le territoire suisse de manière imprévisible, même si l'expéditeur et le destinataire se trouvent en Suisse. Comme les informations relatives à l'expéditeur et au destinataire ne sont pas cryptées dans le cadre des services e-banking, elles peuvent être lues par des tiers non autorisés. Des tiers non autorisés peuvent donc, tant en Suisse qu'à l'étranger, tirer des conclusions quant à l'existence d'une relation client entre la banque et la/le client-e.

L'utilisation des services e-banking depuis l'étranger ou via une passerelle privée (p. ex. VPN) se fait aux risques et périls de l'utilisatrice-teur. La banque décline expressément toute responsabilité quant aux risques ou conséquences découlant d'une telle utilisation.

13. Responsabilité de la banque

La banque respecte les obligations de diligence habituelles dans le cadre de la fourniture de services e-banking et de l'exploitation de son centre de calcul. Les interruptions prévisibles sont annoncées à l'avance dans la mesure du possible. Les interruptions de service pour cause de maintenance, d'extension ou d'adaptation du système de la banque, ainsi que celles résultant de menaces réelles ou suspectées à la sécurité opérationnelle, sont expressément réservées et ne donnent lieu à aucun droit de réclamation de la part de la/du client-e. Les interruptions de traitement sont résolues dans les meilleurs délais. Elles ne donnent lieu à aucun droit à indemnisation de la part de la/du client-e. La banque ne fournit pas l'accès technique à ses services. Ceci relève de la seule responsabilité de l'utilisatrice-teur. Elle/Il prend notamment acte du fait que la banque ne commercialise en principe pas les logiciels de sécurité spécifiques nécessaires aux services e-banking. La banque n'assume donc aucune garantie ni pour les fournisseurs d'accès ni pour les logiciels de sécurité.

La banque décline toute responsabilité quant à l'exactitude et l'exhaustivité des données et informations affichées ou transmises dans le cadre des services e-banking. En particulier les informations sur les comptes et dépôts (soldes, extraits, transactions, etc.) sont réputées provisoires et ne sont fournies qu'à titre indicatif. De même, toutes les communications dans le cadre des services e-banking ne constituent pas des offres fermes, sauf si l'offre est expressément désignée comme telle. En outre, les informations relatives aux devises ou aux cours des billets sont toujours fournies à titre indicatif.

La/Le client-e reconnaît que la transmission des données électroniques de l'utilisatrice-teur vers le centre de calcul de la banque et du centre de calcul de la banque vers l'utilisatrice-teur ne relève pas de la responsabilité de la banque. Elle doit être assurée par l'utilisatrice-teur lui-même ou par les tiers auxquels il fait appel. Seules les transactions effectuées sur le système de la banque, telles qu'elles apparaissent dans les enregistrements électroniques et les éventuelles impressions informatiques de la banque, engagent la banque. La banque décline toute responsabilité pour les dommages subis par la/le client-e à la suite d'erreurs de transmission, de défauts techniques, de perturbations ou d'interventions de tiers dans l'infrastructure de transmission des données.

La banque ne répond pas des préjudices subis par la/le client-e du fait du non-respect de ses obligations contractuelles ou des obligations contractuelles de l'utilisatrice-teur, ni des dommages indirects et consécutifs tels qu'un manque à gagner ou des prétentions de tiers.

La banque décline toute responsabilité pour les ordres non exécutés dans les délais ou exécutés de manière incomplète et les dommages qui en découlent, notamment les moins-values, dans la mesure où elle a fait preuve de la diligence habituelle.

14. Dispositions applicables aux procurations

L'autorisation accordée aux utilisatrices-teurs pour l'utilisation des services e-banking reste valable jusqu'à sa révocation adressée à la banque, nonobstant des publications et/ou inscriptions différentes au registre du commerce. La révocation doit être faite par écrit, la banque ayant cependant le droit – mais non l'obligation – d'accepter une révocation verbale. La procuration ne s'éteint ni avec le décès, la déclaration de disparition ou l'incapacité d'exercice des droits civils de la/du client-e ni avec l'incapacité de l'un des utilisatrices-teurs.

15. Résiliation

Le contrat de services BAS e-banking peut être résilié à tout moment sans préavis par la banque ou par écrit par la/le client-e.