Conditions d'utilisation des Services One

Article 1 Conditions d'utilisation des Services One

1.1 Conditions d'utilisation des Services One et autres documents pertinents

Les présentes Conditions d'utilisation s'appliquent aux services en ligne désignés par le terme "one" ("**Services One**") et fournis par la Banque cantonale du Valais (la "**Banque**") aux titulaires (les "**Titulaires**") d'une carte de Debit Mastercard (les "**Cartes**").

Viseca Payment Services SA (le "**Sous-Traitant**") agit en qualité de sous-traitant dans le cadre de la fourniture des Services One. Le Titulaire autorise la Banque à fournir au Sous-Traitant les données concernant le Titulaire, la Carte et le(s) compte(s) au(x)quel(s) la Carte est rattachée. **En vue de ces communications, le Titulaire délie la Banque du respect du secret bancaire et professionnel (article 47 de la loi fédérale sur les banques et dispositions similaires).**

Les Services One sont accessibles par:

- le site Internet "one" (le "**Site Internet**"); et
- l'application "one" (l'"**Application**").

Des informations additionnelles sur le traitement des données personnelles des Titulaires figurent dans la Notice en matière de protection des données de la Banque (disponible sur le site Internet de la banque), dont la version en vigueur peut être consultée sous le lien ci-dessus ou obtenue auprès de la Banque (la "Déclaration de protection des données BCVS").

Les présentes Conditions d'utilisation sont applicables en sus des Conditions d'utilisation de la carte de Debit Mastercard (disponibles sur le site Internet de la Banque, les "Conditions d'utilisation DMC"). En cas de contradiction, les présentes Conditions d'utilisation priment sur les Conditions d'utilisation DMC.

1.2 Qu'est-ce que sont les Services One?

Les Services One comprennent des services de la Banque, dispensés par le Sous-Traitant pour le compte de la Banque. L'utilisation des Services One requiert une inscription préalable. Les nouveaux Services One introduits sont mis à disposition des Titulaires moyennant des mises à jour (*updates*). La Banque informe les Titulaires de manière adéquate sur les développements et, le cas échéant, sur les changements des présentes Conditions d'utilisation qui y sont liés.

1.3 Quelles fonctions proposent les Services One?

Les Services One peuvent – à l'heure actuelle ou à l'avenir – comprendre en particulier les fonctions suivantes:

- Compte d'utilisateur pour la gestion des données personnelles;
- Aperçu des transactions et des Cartes enregistrées;
- Affichage et activation des factures électroniques;
- Confirmation des transactions en ligne, p. ex. par le biais de 3-D Secure (cf. Article 5);
- Enregistrement de la Carte pour les solutions de paiement mobile (Mobile Payment);
- Activation de la Carte pour le service Click to Pay;
- Notifications *push*, services SMS;
- Blocage de la Carte et commande de cartes de remplacement et de nouveaux codes NIP;
- Affichage et échange de points surprize;
- Classification des transactions et contrôle des dépenses;
- Formulaire de contact et service clientèle.

Article 2 Utilisation des Services One

2.1 Droit d'usage

Le Titulaire n'est autorisé à utiliser les Services One que si le Titulaire est en mesure de mettre en œuvre les présentes Conditions d'utilisation et les exigences qui s'y rattachent (en particulier ch. 3.2).

2.2 Traitement de données personnelles dans le cadre des Services One

En utilisant les Services One, le Titulaire prend acte que la Banque (et le Sous-Traitant) procède(nt) aux traitements de données personnelles listés ci-dessous (en sus de ceux listés dans la Déclaration de protection des données BCVS), lesquels traitements sont fondés sur l'exécution du contrat conclu entre la Banque et le Titulaire dans le cadre des Services One:

- Traitement des données personnelles qui sont ou seront collectées lors de l'utilisation des Services One (soit les données d'identification du Titulaire, les données relatives au compte auquel la Carte est rattachée et les transactions opérées à travers la Carte et/ou les Services One).
- Communication électronique par e-mail (en utilisant l'adresse e-mail indiquée lors de l'inscription) ainsi qu'à travers l'Application (par exemple notification de changements d'adresse, notification de modifications des Conditions d'utilisation ou notifications en lien avec la lutte contre l'utilisation frauduleuse de Cartes).

Par ailleurs, le Titulaire prend acte que la Banque (respectivement le Sous-Traitant lorsque le traitement est délégué) procède(nt) aux traitements de données personnelles suivants, sur la base de l'intérêt légitime de la Banque à la promotion de ses produits et services:

- Réception de messages et informations concernant des produits et services de la Banque à des fins de

marketing (publicité). Ces messages peuvent être distribués par la Banque par e-mail ou directement dans l'Application ou sur le Site Internet. Ces traitements de données personnelles comprennent en particulier le rattachement par la Banque de données collectées dans le cadre des Services One avec les données déjà existantes dans le cadre de la relation-client pour la création de profils à des fins de *marketing* (mais également à des fins de gestion des risques).

Le Titulaire peut indiquer en tout temps à la Banque qu'il ne souhaite pas que la Banque procède à des traitements de données personnelles le concernant en vue de proposer des produits et services et/ou à d'autres fins de *marketing* (droit "opt-out"). Une telle indication doit être communiquée à la Banque en utilisant les coordonnées qui se trouvent dans la Déclaration de protection des données BCVS (disponible sur le site Internet de la Banque).

2.3 Refus ou retrait par le Titulaire de son consentement

Si le Titulaire refuse les traitements visés au chiffre 2.2 (hormis les traitements à des fins de *marketing* / troisième point au chiffre 2.2 ci-dessus), l'Application ou le Site Internet ou certains de leurs services individuels ne pourront, selon les circonstances, pas ou plus être utilisés.

2.4 Effet des confirmations

Chaque confirmation effectuée moyennant l'Application ou la saisie d'un code SMS est considérée comme une opération effectuée par le Titulaire. Le Titulaire s'engage à prendre à sa charge les débits de la Carte résultant de ces confirmations et autorise irrévocablement la Banque à exécuter les ordres et démarches respectifs.

2.5 Disponibilité / blocage / modifications

La Banque peut en tout temps (et même sans préavis) totalement ou partiellement interrompre, limiter, suspendre ou remplacer par une autre prestation les Services One. La Banque a en particulier le droit de bloquer temporairement ou définitivement l'accès du Titulaire aux Services One (par exemple en cas de soupçon d'abus).

2.6 Droits de propriété intellectuelle et licence

Tous les droits (en particulier droit d'auteur et droit des marques) sur les logiciels, textes, images, vidéos, noms, logos et autres données et informations, accessibles, à l'heure actuelle ou dans le futur, par les Services One, appartiennent exclusivement à la Banque ou aux partenaires et tiers respectifs (par exemple le Sous-Traitant). Les noms et logos visibles dans le cadre des Services One sont des marques protégées.

La Banque octroie au Titulaire une licence non exclusive, non transmissible, de durée indéterminée, révocable en tout temps et gratuite pour télécharger l'Application, l'installer sur un appareil que le Titulaire possède durablement et l'utiliser conformément aux présentes Conditions d'utilisation.

Article 3 Risques, exclusion de garantie et obligation générale de diligence et de communiquer

3.1 Risques lors de l'utilisation des Services One

Le Titulaire prend acte et accepte que l'utilisation des Services One comporte des risques.

En particulier, il est possible que, lors de l'utilisation des Services One, des tiers non autorisés utilisent frauduleusement la ou les Cartes, le nom d'utilisateur et mot de passe, les appareils employés ou les données personnelles du Titulaire (ou des personnes liées au Titulaire). Ce faisant, le Titulaire peut subir un préjudice financier (par exemple lorsque son compte est indûment débité ensuite d'une utilisation frauduleuse de la Carte ou de l'Application) et une violation de ses droits de la personnalité (par exemple en cas d'utilisation abusive de ses données personnelles). En outre, il existe un risque que les Services One ou l'un des services proposés dans le cadre des Services One ne puisse pas être utilisé.

Les abus sont rendus possibles ou facilités en particulier par:

- la violation par le Titulaire des obligations de diligence ou de communiquer (cf. ch. 3.2) (par exemple lors du traitement négligent de son nom d'utilisateur / mot de passe ou l'absence d'annoncer une perte de la Carte);
- les réglages sélectionnés par le Titulaire ou le manque d'entretien des appareils et systèmes employés pour l'utilisation des Services One (par exemple ordinateurs, téléphones portables, tablettes et autre infrastructure informatique), par exemple par l'absence d'un verrouillage d'écran, par l'absence ou l'insuffisance d'un pare-feu (*firewall*) ou d'une protection anti-virus ou par l'utilisation d'un logiciel obsolète;
- des interventions de tiers ou d'erreurs dans la transmission de données sur Internet (tels que le piratage, le *phishing* ou la perte de données);
- des confirmations erronées dans l'Application ou par l'insertion d'un code SMS (par exemple en cas de vérification insuffisante, par le Titulaire, d'une demande de confirmation);
- la sélection effectuée par le Titulaire de paramètres de sécurité faibles pour les Services One, en particulier dans le cadre de l'utilisation de l'Application (par exemple sauvegarde du *login*).

Si le Titulaire respecte ses obligations de diligence lors de l'utilisation des appareils et du mot de passe ainsi que les obligations de vérification des demandes de confirmation, le Titulaire peut réduire ces risques d'utilisation abusive. De plus amples informations sur la réduction de risques lors de l'utilisation des Services One sont disponibles sur le Site Internet https://one.viseca.ch/login/login?lang=fr.

La Banque ne fournit aucune garantie et ne donne aucune assurance que le Site Internet et l'Application soient accessibles en permanence ou fonctionnent sans interruption ou que des abus peuvent être reconnus et évités avec certitude.

3.2 Obligations générales de diligence du Titulaire

3.2.1 Obligations générales de diligence en lien avec les appareils et systèmes employés, en particulier les appareils mobiles

Les Services One permettent, notamment, l'authentification du Titulaire par le biais de l'appareil mobile du Titulaire (par exemple téléphone mobile, tablette; "**appareil mobile**"). La conservation soigneuse en permanence de ces appareils mobiles par le Titulaire est un facteur de sécurité essentiel. Le Titulaire doit employer les appareils mobiles avec la diligence appropriée et assurer leur protection adéquate.

Ainsi, le Titulaire est tenu de respecter notamment les obligations de diligence suivantes en lien avec l'emploi des appareils et systèmes, en particulier des appareils mobiles:

- Le numéro de téléphone ou l'adresse e-mail du Titulaire doivent être modifiés sur le Site Internet ou dans l'Application;
- Il convient de définir un mot de passe qui ne comporte pas de combinaisons faciles à deviner telles que numéro de téléphone, date de naissance, numéro de plaque minéralogique, etc. Il ne doit pas être noté ni enregistré de façon non sécurisée;
- Le verrouillage de l'écran doit être activé pour les appareils mobiles et des mesures de sécurité supplémentaires doivent être mises en place afin de prévenir tout accès par des tiers non autorisés;
- Des programmes de protection contre les virus et de sécurité Internet doivent être installés sur les appareils mobiles ainsi que sur les ordinateurs de bureau et ordinateurs portables et mis à jour régulièrement;
- L'Application doit être téléchargée uniquement sur les plateformes officielles (p. ex. Apple Store ou Google Play Store);
- Les mises à jour (updates) de l'Application doivent être installées sans tarder;
- En cas de perte d'un appareil mobile, la carte SIM, l'appareil mobile ou le compte utilisateur doivent être bloqués ou réinitialisés et, si nécessaire, les données effacées;
- L'Application doit être supprimée avant toute vente ou prêt de longue durée de l'appareil à un tiers;
- Les interventions dans le système d'exploitation sont interdites.

3.2.2 Obligations générales de diligence en lien avec le mot de passe

Outre la possession de l'appareil mobile, le nom d'utilisateur et le mot de passe servent d'éléments supplémentaires à l'authentification du Titulaire.

Le Titulaire est tenu de respecter notamment les obligations de diligence suivantes en lien avec le mot de passe:

- Le Titulaire doit choisir un mot de passe qui n'est pas déjà employé pour d'autres services et qui ne doit pas être constitué de combinaisons facilement déchiffrables (telles que numéros de téléphone, dates de naissance, plaques minéralogiques, noms du titulaire ou de personnes proches, des suites de chiffres ou de lettres répétées ou qui se suivent directement telles que "123456" ou "aabbcc");

- Le mot de passe doit rester confidentiel. Il ne doit pas être divulgué ou rendu accessible à des tiers. Le Titulaire prend acte que la Banque ne demandera jamais au Titulaire de divulguer son mot de passe;

- Le mot de passe ne doit pas être noté ou être enregistré de manière non sécurisée;

- Le Titulaire doit modifier le mot de passe ou réinitialiser le compte d'utilisateur ou le faire réinitialiser par la Banque lorsqu'il y a un soupçon qu'un tiers ait connaissance du mot de passe ou pris possession d'autres données;

- La saisie du mot de passe doit être effectuée seulement de façon à ne pas être visible pour des tiers.

3.2.3 Obligations générales de diligence en lien avec les demandes de confirmation

Les confirmations lient juridiquement le Titulaire.

De ce fait, le Titulaire est tenu de respecter les devoirs de diligence généraux suivants en lien avec les confirmations dans l'Application ou par la saisie du code SMS:

- Le Titulaire ne doit confirmer que si la demande de confirmation est directement liée à une opération ou une démarche spécifique du Titulaire (par exemple un paiement, un *login* ou un contact avec la Banque);

- Avant de confirmer, le Titulaire doit vérifier si l'objet de la demande de confirmation correspond à la démarche concernée. Lors de demandes de confirmation en lien avec la technologie "3-D Secure", le Titulaire doit vérifier les détails de paiement affichés.

3.3 Obligations générales de communiquer du Titulaire

Les événements suivants doivent être immédiatement communiqués à la Banque (dont les coordonnées sont disponibles sur son site Internet www.bcvs.ch):

- Perte d'un appareil mobile (en vue du blocage de l'Application), mais non pas un égarement de courte durée;

- Un soupçon d'abus lié par exemple à la réception par le Titulaire d'une demande de confirmation qui n'est pas liée à une opération effectuée par le Titulaire (paiement en ligne, *login* du Titulaire, contact avec la Banque ou autres processus semblables);

- Toute autre suspicion qu'une demande de confirmation dans l'Application ou un code SMS ne proviennent pas de la Banque;

- Cas de soupçon d'abus, notamment du nom d'utilisateur, du mot de passe, des appareils mobiles, du Site Internet, de l'Application, ou soupçon qu'un tiers non autorisé soit entré en possession de ces informations ou objets;

Article 4 Responsabilité

Il appartient au Titulaire de mettre en œuvre les obligations de diligence afin de prévenir l'utilisation non autorisée des Services One. Il appartient au Titulaire de prendre des mesures appropriées afin de prévenir le risque de fraude dans l'utilisation des Services One. Le Titulaire supporte tout dommage résultant de la violation de ses devoirs de diligence.

Plus généralement, les dommages résultant de défauts de légitimation ou de fraudes non décelées sont à la charge du Titulaire, sauf en cas de faute grave de la Banque.

Article 5 3-D Secure

5.1 Qu'est-ce que 3-D Secure?

3-D Secure est une norme de sécurité reconnue au niveau international pour les transactions en ligne avec des cartes. Les Titulaires sont tenus d'utiliser cette norme de sécurité pour les paiements lorsque c'est possible. Lors de l'enregistrement pour les Services One, 3-D Secure est activé pour toutes les Cartes qui sont libellées au nom du Titulaire et qui sont liées à la relation d'affaires enregistrée qui existe entre le Titulaire et la Banque. Une fois activé, 3-D Secure ne peut plus être désactivé, pour des raisons de sécurité.

Les paiements effectués moyennant 3-D Secure peuvent être confirmés (autorisés) dans l'Application.

Conformément aux Conditions d'utilisation DMC (disponibles sur le site Internet de la Banque), chaque utilisation de la Carte autorisée par le biais de la technologie 3-D Secure est considérée comme ayant été effectuée par le Titulaire.

5.2 Activation de Cartes pour 3-D Secure

Lors de l'inscription auprès des Services One, la technologie 3-D Secure est activée pour toutes les Cartes au nom du Titulaire qui sont en lien avec la relation d'affaires entre le Titulaire et la Banque.

5.3 Désactivation de 3-D Secure

Pour des raisons de sécurité, 3-D Secure ne peut plus être désactivé après une activation.

* * *