

ANNEXE : CONDITIONS D'UTILISATION DE 3D SECURE

Objet :

3D Secure est une norme internationalement reconnue d'identification du titulaire d'une carte de débit ou de crédit pour les paiements en ligne utilisant l'appellation « MasterCard® SecureCode™ » pour les paiements par MasterCard® et « VERIFIED by VISA » pour les paiements par Visa. Elle a pour but de renforcer la sécurité des transactions sur Internet. Le titulaire de carte pourra vérifier directement sur le site du marchand si celui-ci a choisi de sécuriser les achats en ligne via la norme 3D Secure.

Les présentes Conditions définissent les modalités d'utilisation de la nouvelle version de la technologie 3D Secure. Elles complètent et font partie intégrante des conditions générales de la banque émettrice concernant l'utilisation des cartes Visa ou MasterCard (ci-après les « Conditions générales d'utilisation des Cartes ») entre la Banque (ci-après « la Banque émettrice ») ayant émis la carte de crédit ou de débit (ci-après la « Carte ») et le titulaire et/ou l'utilisateur de la carte (ci-après le « Client »).

Art. 1 : Activation du 3D Secure pour une Carte

- (1) La Banque se réserve le droit d'activer automatiquement la technologie 3D Secure pour les cartes éligibles du Client.
- (2) Sans activation de 3D Secure, une transaction auprès d'un marchand sur Internet nécessitant une identification 3D Secure ne peut être exécutée.

Art. 2 : Utilisation de la Carte et autorisation

- a) Exécution d'une transaction 3D Secure au moyen d'un token associé à un certificat LuxTrust (ci-après « le certificat LuxTrust ») :

Par ce moyen, le Client doit valider l'exécution de la transaction 3D Secure en saisissant son identifiant LuxTrust, son mot de passe LuxTrust ainsi que le mot de passe à usage unique indiqué sur son token LuxTrust.

- b) Exécution d'une transaction 3D Secure au moyen de LuxTrust Mobile :

Par ce moyen, le Client doit valider l'exécution de la transaction 3D Secure par son application LuxTrust Mobile qui aura été préalablement installée sur son smartphone et activée en suivant la procédure ad hoc. Lors de cette validation, il lui sera demandé de confirmer la transaction dans l'application après saisie du mot de passe LuxTrust Mobile ou, le cas échéant, en utilisant les données biométriques. La saisie des éléments de sécurité requis confirme l'approbation du paiement par carte conformément aux dispositions des Conditions générales d'utilisation des Cartes de la Banque émettrice.

Art. 3 : Obligation de diligence

- (1) Le Client doit assurer la sécurité et la confidentialité de ses éléments de sécurité et de tout instrument ou dispositif (carte de crédit ou de débit, « token » LuxTrust) nécessaires à la validation d'une transaction.

Ainsi, il ne doit pas noter les éléments de sécurité ou les sauvegarder sous un format électronique dans leur forme intégrale ou modifiée, codifiée ou non, ni les communiquer à une tierce personne.

- (2) Lors de la validation de la transaction 3D Secure, le Client doit s'assurer que le portail dédié comporte les éléments de protection suivants :
 - l'adresse du portail commence par « https »,
 - la barre d'adresse du portail doit afficher un cadenas,
 - le portail reprend le logo « MasterCard® SecureCode™ » ou « VERIFIED by VISA »,
 - la présence de l'image secrète LuxTrust définie par le Client s'il choisit la validation via le token LuxTrust,
 - le contexte de la transaction qui apparaît sur l'image secrète ou sur l'application LuxTrust Mobile. Ce contexte reprend les données de la transaction que le client veut valider.

En cas d'absence d'un de ces éléments de protection sur le portail dédié, le Client doit s'abstenir de valider la transaction et est seul responsable de tout dommage pouvant résulter d'une saisie de ses éléments de sécurité et d'une éventuelle validation de l'opération.

- (3) En cas d'absence d'un de ces éléments de protection sur le portail dédié ou de soupçon quant à une utilisation frauduleuse des éléments de sécurité du Client, celui-ci doit immédiatement informer la Banque émettrice et procéder au blocage de la Carte conformément aux dispositions reprises aux Conditions générales d'utilisation des Cartes de la Banque émettrice de la Carte.

Art. 4 : Traitement des données à caractère personnel

- (1) Le Client mandate la Banque émettrice pour le traitement de ses données à caractère personnel afin d'assurer le bon fonctionnement de la Carte et afin de garantir la prévention, la détection et l'analyse d'opérations frauduleuses.
- (2) En sus des dispositions relatives au traitement des données à caractère personnel prévues aux Conditions générales d'utilisation de la Carte de la Banque émettrice, le Client autorise spécifiquement la Banque émettrice à transmettre ses données à caractère personnel à des tiers dont l'intervention est nécessaire dans le cadre de 3D Secure.

Dans ce contexte, le Client reconnaît expressément avoir été informé que l'utilisation de 3D Secure nécessite l'intervention de sociétés tierces intervenant dans le cadre de la validation par certificat LuxTrust. Les données transmises sont également susceptibles d'être stockées auprès de ces sociétés tierces, en ce compris à l'étranger.

- (3) La Banque émettrice, responsable du traitement des données à caractère personnel, s'engage à traiter ces données conformément à la législation applicable relative à la protection des personnes à l'égard du traitement des données à caractère personnel.
- (4) Le client peut refuser la transmission de l'information concernée dans le cadre de 3D Secure en contactant le service client.

Art. 5 : Responsabilité

(1) Les clauses de responsabilité figurant dans les Conditions générales d'utilisation des Cartes ainsi que dans les Conditions générales de la Banque émettrice restent valables dans le cadre de l'utilisation de 3D Secure.

La Banque émettrice ne garantit pas la disponibilité systématique du service 3D Secure et ne saurait être tenue responsable de tout dommage résultant d'une panne, interruption (y compris en cas de maintenance nécessaire) ou surcharge des systèmes de la Banque émettrice ou de l'un des tiers mandatés par la Banque émettrice.

(2) La Banque émettrice ne saurait être tenue responsable de tout échec de la technologie 3D Secure, respectivement pour tout dommage, résultant d'une panne, d'un mauvais fonctionnement ou de l'interruption des réseaux de communications électroniques (Internet, téléphonie mobile) et serveurs publics, d'un conflit social ou d'autres événements en dehors de son contrôle.