Conditions particulières d'utilisation du système d'identification 3D Secure pour les paiements en ligne effectués par carte bancaire

Les conditions particulières ci-dessous régissent l'utilisation de 3D Secure pour les transactions en ligne effectuées avec des cartes de paiement émises par Solarisbank AG (la « **Banque** »).

1. Objet - Définitions

1.1 La Banque permet au titulaire d'une carte de paiement qu'elle a émise et approuvée aux fins de transactions en ligne (la « **Carte** ») de bénéficier du processus 3D Secure[1], mis en place par les commerçants, participants pour sécuriser les transactions en ligne par carte bancaire.
1.2 Le processus 3D Secure (appelé « Mastercard Identity Check » dans le réseau Mastercard, et « VISA SECURE » dans le réseau VISA) est une norme d'authentification de paiement pour les achats sur Internet par Carte.
1.3 Afin d'autoriser les transactions en ligne par Carte, le titulaire de la Carte doit utiliser certains éléments d'authentification (cf. Clauses 4.1 et 7.1 des Conditions pour les services de banque en ligne).
1.4 Les éléments d'authentification comprennent un numéro d'authentification de transaction mobile (le « **mobileTAN** »). Un mobileTAN est envoyé à l'appareil portable du titulaire de la Carte par SMS (Short Message Service) par la Banque ; une authentification in-app où les titulaires de la Carte sont redirigés vers l'application bancaire des partenaires de la Banque (« **authentication in-app** ») ; ou des questions de sécurité auxquelles seul le titulaire de la Carte peut répondre.
1.5 La Banque peut refuser une transaction par Carte en ligne si le titulaire de la Carte souhaite effectuer une transaction sans recourir à 3D Secure chez un commerçant en ligne participant.

2. Conditions préalables à l'utilisation

2.1 Chaque titulaire d'une Carte valide et débloquée participe automatiquement à la procédure 3D Secure. L'inscription a lieu automatiquement lorsque la Carte est activée. Un enregistrement spécifique n'est pas nécessaire. Afin d'utiliser 3D Secure, le titulaire de la Carte doit avoir enregistré son numéro de portable auprès de la Banque.
2.2 Afin de procéder à une authentification par 3D Secure via mobileTAN, le titulaire de la Carte doit fournir un numéro de téléphone portable à la Banque par l'intermédiaire d'un de ses partenaires. Le numéro peut être modifié à tout moment.
2.3 Afin de procéder à une authentification par 3D Secure grâce à l'authentification in-app, le titulaire de la Carte doit avoir réussi à lier son appareil portable au compte connecté à la Carte.

3. Authentification via 3D Secure

3.1 Le mobileTAN transmis par SMS comprendra au moins six chiffres et devra être saisi afin d'authentifier la transaction par Carte en ligne. En ce qui concerne la synchronisation des données, le titulaire de la Carte verra apparaître à l'écran les derniers chiffres du numéro de téléphone portable fourni à la Banque.
3.2 La Banque fournira le SMS gratuitement.
3.3 Pour l'authentification in-app, le titulaire de la Carte doit se connecter à l'application bancaire du partenaire de la Banque, vers lequel il est redirigé, et confirmer la transaction en ligne par Carte.
3.4. Pour s'authentifier en répondant à une question de sécurité, le titulaire de la Carte doit donner la bonne réponse à une question à laquelle il est le seul à pouvoir répondre.

4. Devoirs de prudence du titulaire de la Carte

4.1 Le titulaire de la Carte veillera à ce qu'aucun tiers n'accède à son appareil portable pour l'exécution de transactions en ligne. La Banque ne demandera pas au titulaire de la Carte de s'inscrire ou de fournir ses données d'inscription, ni par courrier électronique ni par téléphone.
4.2 Le titulaire de la Carte doit prendre les mesures nécessaires pour assurer la sécurité des SMS, par exemple en protégeant l'accès au téléphone par un mot de passe. La Banque n'est pas responsable si, en cas de perte, de vol ou de transmission de l'appareil portable, des tiers obtiennent un accès non autorisé au contenu du SMS et en font usage.
4.3 Le titulaire de la Carte doit vérifier les données transférées par SMS (voir clause 3.2). En cas de données incorrectes, le titulaire de la Carte doit annuler l'opération et en informer la Banque sans délai.

5. Traitement des données et fournisseurs de services

5.1 Lors de l'utilisation de 3D Secure, le numéro de la Carte, la date et l'heure de la transaction, le montant de la transaction, les informations sur le commerçant (nom, ID, URL) et l'adresse IP à partir de laquelle la transaction par carte a été effectuée sont stockés.
5.2 La Banque peut confier l'exploitation de la procédure 3D Secure à des prestataires de services. La Banque ne fournit des données à caractère personnel du titulaire de la Carte à ces prestataires de services (par exemple le numéro de carte de crédit) qu'aux fins de la relation contractuelle.
5.3. Pour plus d'informations sur le traitement des données à caractère personnel vous concernant, veuillez consulter les « *Informations sur le traitement des données* » qui peuvent être consultées à l'adresse suivante : http://solarisbank.com/customer-information/france/fr-iban/french/information-des-clients-sur-le-traitement-des-donnees.

[1] 3D Secure est un dispositif de sécurité complémentaire et n'est pas destiné à remplacer les obligations de sécurité, définies par les Conditions générales de la Banque et les autres conditions applicables, le cas échéant, auxquelles le Client doit se conformer.