CONTRAT D'ACCEPTATION EN PAIEMENT A DISTANCE SECURISE PAR CARTES DE PAIEMENT

Le **Contrat d'acceptation en paiement à distance sécurisé par cartes de paiement** (ci-après désigné, le « Contrat ») est composé des documents suivants :

1. Les Conditions Générales de l'acceptation en paiement à distance sécurisé par cartes de paiement comportant deux parties :
   - une partie I « Conditions Générales communes à tous les schémas de cartes »
   - une partie II « Conditions Générales spécifiques à chaque schéma de cartes »
2. Les Conditions Spécifiques de fonctionnement de l'Option « Services E-transactions » :
3. Les Conditions Spécifiques de fonctionnement de l'Option d'acceptation en paiement à distance par cartes de paiement **HORS INTERNET**
4. Annexe 1 « Référentiel Sécuritaire Accepteur »,
5. Annexe 2 « Référentiel Sécuritaire PCI-DSS »,
6. Le barème tarifaire
7. Les Conditions Particulières

La souscription au présent Contrat nécessite la signature préalable ou concomitante d'un compte professionnel dans les livres de la Banque.

Les conditions de fonctionnement des Options sont parties intégrantes du Contrat et trouveront à s'appliquer, en sus des Conditions Générales du Contrat et sauf dispositions contraires dudit Contrat, dès lors que le Client a choisi une ou plusieurs de ces Options aux Conditions Particulières.

CONDITIONS GENERALES DE L'ACCEPTATION EN PAIEMENT A DISTANCE SECURISE PAR CARTES DE PAIEMENT

PARTIE I - CONDITIONS GENERALES COMMUNES A TOUS LES SCHEMAS DE CARTES

La présente partie I détaille les conditions qui s'appliquent à l'ensemble des paiements acceptés par l'Accepteur.

Les conditions spécifiques à chaque Schéma de carte dont la (l'une des) marque(s) est apposée sur la Carte sont détaillées dans la partie II ci-dessous.

ARTICLE 1 - DEFINITIONS

Les termes dotés d'une majuscule ont la signification qui leur est attribuée ci-dessous ou dans les Conditions Particulières.

« Accepteur » : désigne tout commerçant, toute association, tout prestataire de services, toute personne exerçant une profession libérale, et d'une manière générale, tout professionnel vendant et/ou louant des biens et/ou des prestations de services ou toute entité dûment habilitée à recevoir des dons ou percevoir des cotisations, susceptible d'utiliser un Système d'Acceptation reconnu par le(s) schéma(s) de cartes de paiement (ci-après « Schéma(s) ») dûment convenu(s) avec l'Acquéreur dans le cadre du présent Contrat. **Dans le cadre du présent Contrat, l'Accepteur est le Client.**

« Acquéreur » : désigne tout établissement de crédit ou tout autre établissement habilité à organiser l'acceptation des cartes portant la(les) Marque(s) du ou des Schéma(s) visé(s) en partie II des présentes Conditions Générales. **L'Acquéreur est la Banque.**

« Carte » : désigne un instrument de paiement qui permet au payeur d'initier une opération de paiement. La Carte porte une ou plusieurs Marques.

Lorsqu'elle est émise dans l'Espace Economique Européen (ci-après l'« EEE » - Il comprend les Etats membres de l'Union Européenne, l'Islande, le Liechtenstein et la Norvège), la Carte porte au moins l'une des mentions suivantes :
- crédit ou carte de crédit,
- débit,
- prépayé,
- commercial,

ou l'équivalent dans une langue étrangère.

« Catégorie de carte » : désigne les catégories de Cartes suivantes :

- crédit ou carte de crédit,
- carte de débit,
- carte prépayée,
- carte commerciale.

« Cryptogramme Visuel » : désigne l'élément de sécurité matérialisé par trois chiffres au dos de la Carte de paiement qui est communiqué par le titulaire de la Carte lors du paiement.

« **Données de sécurité personnalisées** » : désignent des données personnalisées fournies à un titulaire de carte de paiement par la Banque à des fins d'authentification (exemple : le code confidentiel).

« **Marque** » : désigne tout nom, terme, sigle, symbole, matériel ou numérique, ou la combinaison de ces éléments susceptible de désigner un Schéma.

Les conditions de fonctionnement spécifiques à chaque Marque figurent en partie II des Conditions Générales du présent Contrat.

« **Partie(s)** » : désigne collectivement ou individuellement, d'une part, le Client et/ou d'autre part, la Banque.

« **Paiements récurrents et/ou échelonnés** » (ci-après les "Paiements Récurrents") : désignent plusieurs opérations de paiement successives et distinctes (série d'opérations) ayant des montants et des dates déterminés ou déterminables et/ou à des échéances convenues entre le Client et le titulaire de la Carte.

« **Point de vente en ligne**» : désigne le site internet sur lequel est initié l'ordre de paiement.

« Point de vente » : désigne l'adresse à laquelle se situent les locaux du commerçant au profit duquel l'opération de paiement est initiée. Toutefois:

- dans le cas de contrats à distance, le point de vente est l'adresse du siège d'exploitation fixe à partir de laquelle le commerçant exerce ses activités, quel que soit le lieu où se situent son site internet ou ses serveurs, et par l'intermédiaire de laquelle l'opération de paiement est initiée;
- si le commerçant ne dispose pas d'un siège d'exploitation fixe, le point de vente est l'adresse à laquelle le marchand possède une licence d'exploitation valable et par l'intermédiaire de laquelle l'opération de paiement est initiée;
- si le commerçant ne dispose ni d'un siège d'exploitation fixe ni de licence d'exploitation valable, le point de vente est l'adresse de correspondance qu'il utilise pour le paiement des taxes qu'il acquitte en rapport avec ses activités de vente et par l'intermédiaire de laquelle l'opération de paiement est initiée.

« **Règlement** » : désigne le Règlement UE n°2015/751 du 29 avril 2015.

« **Schéma** » : désigne un ensemble unique de règles, de pratiques, de normes et/ou de lignes directrices de mise en œuvre régissant l'exécution d'opérations de paiement liées à une Carte tel que défini à l'article 2 du Règlement.

Les Schémas (tels que, par exemple CB, Visa, Mastercard, UnionPay, Discover, Diners ou JCB) reposent sur l'utilisation de Cartes auprès des Clients acceptant les Marques desdits Schémas, et cela dans le cadre des seules dispositions et procédures définies ou homologuées par lesdits Schémas.

« **Solution de paiement** » : désigne un outil permettant à un titulaire de Carte de stocker de façon sécurisée les références de ses cartes de paiement afin de lui permettre de réaliser des opérations de paiement par Internet (via un PC ou une tablette), ou un téléphone mobile, avec une authentification sécurisée sans le contraindre à saisir à chaque opération ses références bancaires (tels que, par exemple, Paylib).

« **Système d'Acceptation** » : désigne les logiciels et protocoles, conformes aux spécifications définies par chaque Schéma, et nécessaires à l'initialisation, à l'enregistrement, à la transmission et au traitement sécurisé des ordres de paiement par Cartes portant la (l'une des) Marque(s) dudit Schéma. Le Client doit s'assurer que le Système d'Acceptation a fait l'objet d'un agrément par l'entité responsable du Schéma, le cas échéant en consultant la liste des Systèmes d'Acceptation reconnus par l'entité responsable du Schéma.

ARTICLE 2 : ELIGIBILITE / DECLARATIONS

2.1 Condition d'éligibilité :

Le Client doit être titulaire d'un compte ouvert dans les livres de la Banque.

2.2 Déclarations :

Le Client déclare :

- Respecter les lois et règlements (y compris en matière fiscale), les dispositions professionnelles ainsi que les bonnes pratiques applicables aux ventes et prestations réalisées à distance ainsi que celles applicables au commerce électronique, et notamment aux échanges utilisant les réseaux et les différents terminaux de communication (ex : mobile et ordinateur). A cet effet le Client organise la traçabilité adéquate des informations liées au paiement à distance ;
- faire son affaire personnelle de l'obtention de toutes les autorisations légales, réglementaires ou administratives ou de la réalisation de toutes formalités qui pourraient être nécessaires à son activité ;
- s'abstenir de toute activité qui pourrait être pénalement sanctionnée, telle que la mise en péril de mineurs, des actes de pédophilie, des actes de contrefaçon d'œuvres protégées par un droit de propriété intellectuelle et/ou d'instruments de paiement, le non-respect de la protection des données personnelles, des atteintes aux systèmes de traitement automatisé de données, des actes de blanchiment, le non-respect des dispositions relatives aux jeux d'argent et de hasard, aux courses de chevaux, aux loteries et le non-respect des dispositions relatives aux conditions d'exercice de professions réglementées ;
- s'engager à signaler sans délai à la Banque toute modification relative à son activité (nature des biens et des services proposés) ;
- que l'ensemble des informations et pièces fournies lors de son entrée en relation avec la Banque ainsi que toutes celles fournies tout au long de la durée du Contrat sont exactes, complètes et actualisées ;
- s'engager à communiquer à la Banque, sur demande de celle-ci, tout document constatant son inscription au Registre du Commerce et des Sociétés ou au Répertoire des Métiers, la dénomination, la forme juridique, le siège social et le type d'activité de l'entreprise (extrait K-Bis de moins de trois mois, pouvoirs des dirigeants, statuts), ainsi qu'une copie de son assurance responsabilité civile. La Banque se réserve le droit de demander tout autre document (indice de cotation Banque de France, trois derniers bilans, …) qu'elle jugerait utile.

ARTICLE 3 : OBLIGATIONS DU CLIENT

Le Client s'engage à :

3.1 Afficher visiblement chaque Marque qu'il accepte, notamment en apposant cette information de façon apparente sur son Point de vente en ligne et/ou sur tout autre support de communication.

Pour la ou les Marques qu'il accepte, le Client doit accepter toutes les Cartes émises hors de l'EEE sur lesquelles figure(nt) cette(ces) Marque(s), quelle que soit la Catégorie de carte.

3.2 Afficher visiblement chaque Catégorie de carte qu'il accepte ou refuse en apposant cette information de façon apparente sur son Point de

vente en ligne et/ou sur tout autre support de communication.

3.3 Afficher visiblement le montant minimum éventuel à partir duquel la Carte est acceptée afin que le titulaire de la Carte en soit préalablement informé.

3.4 En cas de présence de plusieurs Marques sur la Carte, respecter la Marque choisie par le titulaire de la Carte pour donner l'ordre de paiement.

3.5 Garantir la Banque, et, le cas échéant, les Schémas, contre toute conséquence dommageable pouvant résulter pour eux du manquement aux obligations visées à l'article 2.2.

3.6 Afin que le titulaire de la Carte n'ait pas de difficulté à vérifier et identifier les opérations de paiement qu'il a initiées, vérifier avec la Banque la conformité des informations transmises pour identifier son Point de vente.

Les informations doivent indiquer une dénomination commerciale ou sociale connue des titulaires de Carte et permettre de dissocier ce mode de paiement des autres modes de paiement (ex : automate et règlement en présence physique du titulaire de la Carte).

3.7 Accepter en contrepartie d'actes de vente et/ou de prestations de services offerts à sa clientèle et qu'il fournit ou réalise lui-même ou à titre de dons ou pour le règlement du montant de cotisations, les paiements à distance sécurisés effectués avec les Cartes (Catégories de carte et Marques) qu'il a choisies d'accepter ou qu'il doit accepter.

3.8 Ne pas collecter, au titre du présent Contrat, une opération de paiement pour laquelle il n'a pas reçu lui-même le consentement exprès du titulaire de la Carte.

3.9 Transmettre les enregistrements des opérations de paiement à la Banque, dans les délais prévus dans les Conditions Particulières convenues avec lui.

3.10 Afficher visiblement sur tout support, et notamment sur le Point de vente en ligne, le montant à payer ainsi que la devise dans laquelle ce montant est libellé.

3.11 Utiliser obligatoirement un Système d'Acceptation conforme aux spécifications du Schéma concerné et les procédures de sécurisation des ordres de paiement donnés à distance par les titulaires de Cartes proposées par la Banque.

3.12 Régler, conformément aux Conditions Particulières et/ou au barème tarifaire portant les principales conditions générales de banque ou tout autre document convenu entre les Parties, les commissions, frais et, d'une manière générale, toute somme due au titre de l'acceptation des Cartes.

3.13 Faire son affaire personnelle des litiges liés à la relation sous-jacente qui existe entre lui et le titulaire de la Carte et de leurs conséquences financières.

3.14 A la demande de la Banque, selon les volumes d'opérations cartes acceptées, respecter les exigences du référentiel de sécurité PCI DSS figurant en annexe du présent Contrat.

Respecter les exigences du Référentiel Sécuritaire Accepteur annexé aux présentes ainsi que les exigences du Référentiel Sécuritaire PCI DSS annexé aux présentes et leurs mises à jour dont il peut prendre connaissance à l'adresse suivante : https://fr.pcisecuritystandards.org/minisite/env2/

3.15 Respecter, pendant toute la durée du Contrat, les engagements pris à l'article « Eligibilité / Déclarations » ci-dessus.

3.16 Prévoir, dans ses relations contractuelles avec les tiers, tels que les prestataires de services techniques ou sous-traitants intervenant dans le traitement et le stockage des données de paiement sensibles liées à l'utilisation des Cartes, que ces derniers :

- s'engagent à respecter tant le Référentiel Sécuritaire PCI DSS que le Référentiel Sécuritaire Accepteur et leurs mises à jour et,

- acceptent que des audits soient réalisés dans leurs locaux et que les rapports puissent être communiqués, comme précisé à l'article 3.18 ci-dessous.

3.17 Permettre à la Banque et/ou au(x) Schéma(s) concerné(s) de faire procéder dans les locaux du Client, aux frais de ce dernier, ou dans ceux des tiers visés à l'article 3.16 ci-dessus, à la vérification et au contrôle périodique par un tiers indépendant du fonctionnement des services de paiement sur Internet en fonction des risques de sécurité liés au Système d'Acceptation utilisé. Cette vérification, appelée "procédure d'audit", s'inscrit dans le respect des procédures de contrôle et d'audit définies par le Schéma concerné.

Le Client autorise la communication du rapport à la Banque et au(x) Schéma(s) concerné(s).

3.18 Au cas où le rapport remis aux Parties ou au Schéma concerné, par le tiers indépendant, à l'issue de la procédure d'audit révélerait un ou plusieurs manquements aux clauses du Contrat et/ou aux exigences du Référentiel Sécuritaire Accepteur et/ou du Référentiel Sécuritaire PCI DSS, la Banque pourra procéder, le cas échéant à la demande d'un Schéma, à une suspension de l'acceptation des Cartes par le Client dans les conditions de l'article « Suspension de l'acceptation », voire à une demande de résiliation du présent Contrat, dans les conditions prévues à l'article « Durée et résiliation du contrat » de la présente partie I des Conditions Générales.

ARTICLE 4 : OBLIGATIONS DE LA BANQUE

La Banque s'engage à :

4.1 Fournir au Client les informations le concernant directement sur le fonctionnement du/des Schéma(s) visé(s) dans la partie II des présentes Conditions Générales et son/leur évolution, les Catégories de cartes et les Marques dont il assure l'acceptation ainsi que les frais applicables à chacune des Catégories de cartes et Marques acceptées par lui, y compris les commissions d'interchange et les frais versés au(x) Schéma(s).

4.2 Respecter le choix de la Marque utilisée pour donner l'ordre de paiement conformément au choix du Client ou du titulaire de la Carte.

4.3 Inscrire le Client dans la liste des accepteurs habilités à recevoir des paiements à distance sécurisés par Cartes.

4.4 Indiquer au Client la liste et les caractéristiques des Cartes (Marques et Catégorie de Carte) pouvant être acceptées et lui fournir à sa demande le fichier des codes émetteurs (BIN).

4.5 Créditer le compte du Client des sommes qui lui sont dues, selon les modalités prévues dans les Conditions Particulières.

4.6 Ne pas débiter, au-delà du délai maximum de quinze (15) mois à partir de la date du crédit initial porté au compte du Client, les opérations non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.

4.7 Selon les modalités convenues avec le Client, communiquer au moins une fois par mois les informations suivantes :

- la référence lui permettant d'identifier l'opération de paiement,
- le montant de l'opération de paiement exprimé dans la devise dans laquelle son compte est crédité,
- le montant de tous les frais appliqués à l'opération de paiement et le montant de la commission de service acquittée par le Client et de la commission d'interchange.

Le Client peut demander à ce que les informations soient regroupées par Marque, Catégorie de carte et par taux de commission d'interchange applicable à l'opération.

4.8 Indiquer et facturer au Client les commissions de services à acquitter séparément pour chaque Catégorie de carte et chaque Marque selon les différents niveaux de commission d'interchange.

Le Client peut demander à ce que les commissions de services soient regroupées par Marque, Catégorie de carte et par taux de commission d'interchange applicable à l'opération.

ARTICLE 5 : GARANTIE DU PAIEMENT

5.1 Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées tant à l'article « Mesures de sécurité » ci-dessous que dans la partie II des Conditions Générales du présent Contrat, ainsi qu'aux Conditions Particulières.

5.2 Toutes les mesures de sécurité sont indépendantes les unes des autres.

5.3 En cas de non-respect d'une seule de ces mesures les opérations ne sont réglées que sous réserve de bonne fin d'encaissement.

5.4 La Banque pourra contrepasser le montant des opérations non garanties qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.

ARTICLE 6 : MESURES DE SECURITE

Le Client s'engage à :

6.1 Informer immédiatement la Banque en cas de fonctionnement anormal de son Point de vente en ligne et/ou du Système d'Acceptation et/ou de toutes autres anomalies (absence d'application des procédures de sécurisation des ordres de paiement, dysfonctionnement du Système d'Acceptation, etc.).

6.2 En cas de survenance d'un incident de sécurité majeur, notamment en cas de collecte et/ou d'utilisation frauduleuse des données, coopérer avec la Banque et les autorités compétentes le cas échéant. Le refus ou l'absence de coopération de la part du Client pourra conduire la Banque à mettre fin au présent Contrat conformément à l'article « Durée et résiliation du contrat » de la présente partie I des Conditions Générales.

6.3 Lors du paiement, le Client s'engage à :

6.3.1 Appliquer la procédure de sécurisation des ordres de paiement suivante :

3D Secure désigne le protocole sécurisé de paiement sur Internet (VerifiedbyVisa© pour VISA et MastercardSecurecode© pour MASTERCARD) permettant de sécuriser les transactions et

d'obtenir de la Banque un justificatif d'acceptation matérialisant les contrôles effectués et la validité de l'ordre de paiement.

En complément de la demande d'autorisation, le programme 3D Secure génère une demande d'authentification du titulaire de la Carte pour les paiements effectués au moyen de cartes CB, VISA ou MASTERCARD, et ce à partir de la page de paiement d'acceptation.

La réponse à la demande d'authentification générée par le programme 3D Secure est systématiquement transmise au Client. L'obtention du justificatif d'acceptation se matérialise par une réponse positive à la demande d'authentification.

Les opérations ne seront pas garanties en cas de contestation de l'ordre de paiement par le titulaire de la Carte si le Client n'a pas obtenu ce justificatif d'acceptation. La Banque pourra contrepasser le montant des opérations contestées par les titulaires de Carte pour lesquelles un justificatif d'acceptation n'a pas été obtenu.

Lorsque la Carte n'est pas émise par la Banque, les contestations relatives aux opérations sont matérialisées par un "impayé" adressé par la banque du titulaire de la Carte à la Banque.

L'activation ou la désactivation du 3D Secure est effectuée sous la seule et unique responsabilité du Client. A nouveau, les opérations ne seront pas garanties en cas de contestation de l'ordre de paiement par le titulaire de la Carte si le Client n'a pas obtenu le justificatif d'acceptation.

6.3.2 Obtenir de la Banque un justificatif d'acceptation matérialisant les contrôles effectués et la validité de l'ordre de paiement.

6.3.3 Vérifier l'acceptabilité de la Carte c'est-à-dire :

- la période de validité (fin et éventuellement début),
- que la Marque (ou Catégorie de carte) est indiquée dans les Conditions Particulières ou figure dans la partie II des Conditions Générales du présent Contrat ou tout autre document ultérieur convenu entre les Parties.

6.3.4 Obtenir une autorisation d'un montant identique à l'opération.

6.4 Après le paiement, le Client s'engage à :

6.4.1 Transmettre à la Banque dans les délais et selon les modalités prévus dans les Conditions Particulières, les enregistrements électroniques des opérations et s'assurer que les opérations de paiement ont bien été portées au crédit du compte dans les délais et selon les modalités prévus dans les Conditions Particulières.

Le Client ne doit transmettre que les enregistrements électroniques des opérations pour lesquelles un ordre de paiement a été donné à son profit. Toute opération ayant fait l'objet d'une autorisation transmise par la Banque doit être obligatoirement remise à cette dernière.

6.4.2 Envoyer au titulaire de la Carte, à sa demande, un ticket précisant, entre autres, le mode de paiement utilisé.

6.4.3 Communiquer sans délai, à la demande de la Banque, tout justificatif des opérations de paiement.

6.4.4 Ne pas stocker sous quelque forme que ce soit le Cryptogramme Visuel.

6.4.5 Prendre toutes les précautions utiles pour que soient assurées la confidentialité et l'intégrité des données à caractère personnel du titulaire de la Carte qu'il est amené à recueillir à l'occasion de son activité et notamment lors de l'initiation d'une opération par Carte ainsi que le contrôle de l'accès à celles-ci et ce, conformément aux dispositions de la loi Informatique et Libertés.

6.4.6 Les mesures de sécurité énumérées ci-dessus pourront être modifiées et complétées pendant toute la durée du présent Contrat, selon la procédure prévue à l'article « Modifications » de la présente partie I des Conditions Générales.

ARTICLE 7 : MODALITES ANNEXES DE FONCTIONNEMENT

7.1 Réclamation

7.1.1 Toute réclamation doit être formulée par écrit à la Banque, dans un délai maximum de six (6) mois à compter de la date de l'opération contestée, sous peine de forclusion.

7.1.2 Ce délai est réduit à une durée de quinze (15) jours calendaires à compter de la date de débit en compte résultant d'une opération non garantie, notamment en cas d'impayé.

7.2 Convention de preuve

De convention expresse entre les Parties, les enregistrements électroniques constituent la preuve des opérations de paiement remises à la Banque. En cas de conflit, les enregistrements électroniques produits par la Banque ou le Schéma, dont les règles s'appliquent à l'opération de paiement concernée, prévaudront sur ceux produits par le Client, à moins que ce dernier ne démontre l'absence de fiabilité ou d'authenticité des enregistrements produits par la Banque ou le Schéma.

7.3 Transaction crédit

Le remboursement partiel ou total d'un achat d'un bien ou d'un service ou d'un don ou d'une cotisation réglé(e) par Carte doit, avec l'accord du titulaire de la Carte, être effectué avec les données de la Carte utilisée pour l'opération initiale. Le Client doit alors utiliser la procédure dite de "transaction crédit" selon les règles du Schéma qui s'appliquent à l'opération de paiement concernée ou dans les Conditions Particulières convenues avec la Banque, effectuer la remise correspondante à la banque à qui il avait remis l'opération initiale. Le montant de la "transaction crédit" ne doit pas dépasser le montant de l'opération initiale.

ARTICLE 8 : MODIFICATIONS

La Banque peut modifier à tout moment les dispositions du présent Contrat.

8.1 La Banque peut notamment apporter à tout moment :

- des modifications techniques telles que l'acceptabilité de nouvelles Cartes, les modifications de logiciel, le changement de certains paramètres, la remise en l'état du Système d'Acceptation à la suite d'un dysfonctionnement, etc.
- des modifications sécuritaires telles que :
  - la suppression de l'acceptabilité de certaines Cartes,
  - la suspension de l'acceptabilité de Cartes portant certaines Marques.

8.2 Les nouvelles conditions entrent généralement en vigueur au terme d'un délai minimum fixé à un (1) mois à compter de l'envoi par tout moyen d'une lettre d'information ou de notification. Les modifications imposées par les lois et/ou règlements prennent effet dès leur entrée en vigueur sans qu'une information ne soit obligatoirement envoyée par la Banque.

D'un commun accord, les Parties peuvent déroger à ce délai en cas de modifications importantes.

8.3 Le délai est exceptionnellement réduit à cinq (5) jours calendaires lorsque la Banque ou le Schéma concerné constate une utilisation anormale de Cartes perdues, volées ou contrefaites.

8.4 La Banque peut notamment proposer un nouveau Schéma et/ou une nouvelle Marque et/ou une Solution de paiement. A cette fin, la Banque fera parvenir par tout moyen les conditions spécifiques et tarifaires afférentes au nouveau Schéma et/ou à la nouvelle Solution de paiement et/ou à la nouvelle Marque proposée. Au terme d'un délai d'un (1) mois, sauf désaccord du Client signifié par tout moyen à la Banque, cette dernière rendra compatible pour l'acceptation du nouveau Schéma, de la nouvelle Solution de paiement ou de la nouvelle Marque le Système d'Acceptation dont elle est propriétaire.

8.5 Passés les délais visés au présent article, les modifications et/ou conditions spécifiques et tarifaires afférentes aux nouveaux Schémas, aux nouvelles Solutions de paiement ou nouvelles Marques proposées sont réputées acceptées par le Client s'il n'a pas résilié le présent Contrat. Elles lui sont dès lors opposables.

8.6 Le non-respect des nouvelles conditions contractuelles (techniques, sécuritaires ou autres), dans les délais impartis, peut entraîner la résiliation du présent Contrat dans les conditions prévues ci-dessous.

ARTICLE 9 : DUREE ET RESILIATION DU CONTRAT

Le présent Contrat est conclu pour une durée indéterminée, sauf dispositions contraires visées dans les Conditions Particulières.

9.1 Le Client d'une part, la Banque d'autre part, peuvent, à tout moment, sans justificatif ni préavis (sauf dérogation particulière convenue entre les Parties), sous réserve du dénouement des opérations en cours, résilier le présent Contrat, sans qu'il soit nécessaire d'accomplir aucune autre formalité que l'envoi d'une lettre recommandée avec demande d'avis de réception. Le Client garde alors la faculté de continuer à accepter les Cartes de tout Schéma avec tout autre acquéreur de son choix.

Lorsque cette résiliation fait suite à un désaccord sur les modifications prévues à l'article «Modifications » ci-dessus, elle ne peut intervenir qu'au-delà du délai prévu dans cet article pour l'entrée en vigueur de ces modifications.

9.2 En outre, à la demande de tout Schéma, la Banque peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à la résiliation du présent Contrat. Elle peut être décidée notamment pour l'une des raisons visées à l'article 10.2 ci-dessous. Elle est notifiée par écrit et doit être motivée. Son effet est immédiat.

9.3 Toute cessation d'activité du Client, cession ou mutation du fonds de commerce, entraîne la résiliation immédiate de plein droit du présent Contrat sous réserve du dénouement des opérations en cours.

9.4 En cas de manquement aux déclarations stipulées à l'article « Eligibilité / Déclarations » et/ou aux obligations stipulées aux articles « Obligations du Client » et « Mesures de

sécurité » ci-dessus, la Banque se réserve le droit, sans aucune indemnité et sans préavis, de suspendre ou de mettre fin à tout ou partie du présent Contrat, sans préjudice de toutes autres actions de droit commun qui pourraient être engagées par la Banque. Le Client en sera informé par tout moyen.

9.5 Dans le cas où, après résiliation du présent Contrat, il se révélerait des impayés, ceux-ci seront à la charge du Client ou pourront faire l'objet d'une déclaration de créances.

9.6 Le Client sera tenu de restituer à la Banque les dispositifs techniques et sécuritaires et les documents en sa possession dont la Banque est propriétaire. Sauf dans le cas où il a conclu un ou plusieurs autres contrats d'acceptation en paiement à distance sécurisé par cartes de paiement, le Client s'engage à retirer immédiatement de son Point de vente en ligne, ainsi que de ses supports de communication, tout signe d'acceptation des Cartes, du (des) Schéma(s) concerné(s).

ARTICLE 10 : SUSPENSION DE L'ACCEPTATION

10.1 La Banque peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à une suspension de l'acceptation de tout ou partie des Cartes portant certaines Marques acceptées par le Client. La suspension est précédée, le cas échéant, d'un avertissement au Client, voire d'une réduction de son seuil de demande d'autorisation. Elle est notifiée par tout moyen et doit être motivée. Son effet est immédiat.

La suspension peut également intervenir à l'issue d'une procédure d'audit telle que visée à l'article 3 ci-dessus au cas où le rapport d'audit révélerait un ou plusieurs manquements tant aux clauses du présent Contrat qu'au Référentiel Sécuritaire Accepteur et/ou au Référentiel Sécuritaire PCI DSS, annexés au présent Contrat et leurs mises à jour.

10.2 La suspension peut être décidée en raison notamment :

- du non-respect répété des obligations du présent Contrat et du refus d'y remédier ou d'un risque de dysfonctionnement important du (des) Système(s) d'Acceptation du (des) Schéma(s) concerné(s),
- d'une participation à des activités frauduleuses, notamment d'une utilisation anormale de Cartes perdu(e)s, volé(e)s ou contrefait(e)s,
- d'un refus d'acceptation répété et non motivé des Marques / Catégories de cartes/ Solutions de paiement qu'il a choisi d'accepter ou qu'il doit accepter,
- de plaintes répétées d'autres membres ou partenaires du (des) Schéma(s) concerné(s) et qui n'ont pu être résolues dans un délai raisonnable,
- de retard volontaire ou non motivé de transmission des justificatifs,
- d'un risque aggravé en raison des activités du Client,
- du non-respect d'une ou plusieurs obligations portées par l'article « éligibilité / déclaration » ci-dessus.

10.3 Le Client s'engage alors à restituer à la Banque les dispositifs techniques et sécuritaires et les documents en sa possession dont la Banque est propriétaire et à retirer immédiatement de son Point de vente en ligne ainsi que de ses supports de communication, tout signe d'acceptation des Cartes, ou Marque du (des) Schéma(s) concerné(s).

10.4 La période de suspension est au minimum de six (6) mois, éventuellement renouvelable. A l'expiration de ce délai, le Client peut demander la reprise du présent Contrat auprès de la Banque, ou souscrire un nouveau contrat d'acceptation en paiement à distance sécurisé par cartes de paiement avec un autre acquéreur de son choix.

ARTICLE 11 : MESURES DE PREVENTION ET DE SANCTION PRISES PAR LA BANQUE

11.1 En cas de manquement du Client aux stipulations du présent Contrat ou aux lois en vigueur ou en cas de constat d'un taux d'impayés anormalement élevé ou d'utilisation anormale de Cartes perdu(e)s, volé(e)s ou contrefait(e)s, la Banque peut prendre des mesures de sauvegarde et de sécurité consistant, en premier lieu, en un avertissement au Client valant mise en demeure, précisant les mesures à prendre pour remédier au manquement ou résorber le taux d'impayés anormalement élevé constaté.

11.2 Si dans un délai de trente (30) jours, le Client n'a pas remédié au manquement ayant justifié l'avertissement ou n'a pas mis en œuvre les mesures destinées à résorber le taux d'impayés constaté, la Banque peut soit procéder à une suspension de l'acceptabilité des Cartes dans les conditions précisées à l'article « Suspension de l'acceptation » ci-dessus, soit résilier de plein droit avec effet immédiat, sous réserve du dénouement des opérations en cours, le présent Contrat, par lettre recommandée avec demande d'avis de réception.

11.3 De même, si dans un délai de trois (3) mois à compter de l'avertissement, le Client est toujours confronté à un taux d'impayés anormalement élevé, la Banque peut décider la résiliation de plein droit avec effet immédiat, sous réserve des opérations en cours, du présent Contrat, notifiée par lettre recommandée avec demande d'avis de réception.

ARTICLE 12 : SECRET BANCAIRE ET PROTECTION DES DONNEES A CARACTERE PERSONNEL

12.1 Lors de la signature ou de l'exécution des présentes, chacune des parties peut avoir accès à des données à caractère personnel ou couvertes par le secret bancaire.

12.2 **Secret bancaire**

Les informations relatives au Client, collectées par la Banque, nécessaires pour l'exécution des ordres de paiement transmis et leur sécurisation, ne seront utilisées et ne feront l'objet de diffusion auprès d'entités tierces que pour les seules finalités de traitement des opérations de paiement ordonnées en exécution du présent Contrat, de réponses aux obligations légales et réglementaires, de prévention des fraudes et de traitement des réclamations, qu'elles émanent des titulaires de Cartes ou d'autres entités, la Banque étant à cet effet, de convention expresse, déliée du secret bancaire. Elles sont conservées pour une durée maximale correspondant à la durée de la relation contractuelle augmentée des délais légaux de conservation et de prescription auxquels la Banque est tenue.

12.3 Protection des données à caractère personnel du Client

En application de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés, modifiée par la loi du 6 août 2004 (ci-après la « Loi Informatique, Fichiers et Libertés »), il est précisé que :

12.3.1 Les informations personnelles recueillies par la Banque à l'occasion du présent Contrat sont nécessaires à l'exécution des ordres de paiement transmis et leur sécurisation, ainsi que pour satisfaire à des obligations légales ou permettre à la Banque de poursuivre un intérêt légitime dans le respect des droits du client. Elles pourront faire l'objet de traitements informatisés, pour les finalités et dans les conditions ci-dessous précisées :

Elles seront principalement utilisées par la Banque pour les finalités suivantes : la connaissance du Client, la gestion de la relation bancaire et financière, le recouvrement, la prospection (sous réserve du respect des dispositions légales se rapportant à cette finalité) et l' animation commerciale, les études statistiques, l'évaluation et la gestion du risque, la sécurité et la prévention des impayés et de la fraude, le respect des obligations légales et réglementaires notamment en matière de gestion du risque opérationnel et de lutte contre le blanchiment. Tout défaut de communication de ces données aura pour conséquence l'impossibilité de conclure le présent Contrat. Elles ne seront utilisées et ne feront l'objet de diffusion auprès d'entités impliquées dans le fonctionnement du(des) Schéma(s) que pour les seules finalités de traitement des opérations de paiement ordonnées en exécution du présent Contrat. Le client est informé que les informations personnelles le concernant pourront également être transmises aux destinataires suivants :

a) l'organe central du Groupe Crédit Agricole, tel que défini par le Code monétaire et financier, afin que celui-ci puisse satisfaire, au bénéfice de l'ensemble du Groupe, à ses obligations légales et règlementaires, notamment en matière de déclarations prudentielles auprès de toute autorité ou tout régulateur compétent ;

b) toute entité du Groupe Crédit Agricole, à des fins de prospection commerciale ou de conclusion de contrats,

c) les médiateurs, auxiliaires de justice et officiers ministériels dans le cadre de leurs missions de recouvrement de créances, ainsi que les personnes intervenant dans le cadre de la cession ou du transfert de créances ou de contrats ;

d) les bénéficiaires d'opération de paiement et à leur prestataire de service de paiement à des fins de lutte contre le blanchiment des capitaux et le financement du terrorisme et dans le respect de la règlementation en matière d'embargos et de sanctions internationales ;

e) les partenaires de la Banque, pour permettre aux Clients de bénéficier des avantages du partenariat auquel elle a adhéré, le cas échéant, et ce dans le cadre exclusif des accords de partenariat

f) les sociétés du Groupe Crédit Agricole chargées de la gestion ou de la prévention de risques opérationnels (évaluation du risque, sécurité et prévention des impayés et de la fraude, lutte contre le blanchiment des capitaux…) au bénéfice de l'ensemble des entités du Groupe ;

g) toute entité du Groupe Crédit Agricole en cas de mise en commun de moyens ou de regroupement de sociétés afin de permettre à ces entités de réaliser les missions faisant l'objet de cette mise en commun ;

h) les sous-traitants de la Banque et notamment ceux participant à l'exécution des opérations de paiements, et ce pour les seuls besoins des travaux de sous-traitance ;

i) Crédit Agricole SA ou toute entité du Groupe, et leurs sous-traitants, dans le cadre de la mise en place de systèmes informatisés d'analyse des données des clients des entités du Groupe Crédit Agricole ayant pour objet l'élaboration de modèles algorithmiques prédictifs avec comme finalités (i) la passation, la gestion et l'exécution de contrats relatifs à des produits bancaires et/ ou assurantiels, (ii) l'amélioration des services rendus aux Clients et l'adéquation des produits bancaires et/ou assurantiels proposés aux Clients, (iii) l'élaboration de statistiques et d'études actuarielles et simulations relatives aux contrats conclus avec la banque et (iv) la lutte contre la fraude.

Elles sont conservées pour une durée maximale correspondant à la durée de la relation contractuelle augmentée des délais légaux de conservation et de prescription auxquels la Banque est tenue.

12.3.2 La liste des destinataires susceptibles d'être bénéficiaires d'informations collectées dans le cadre du présent Contrat pourra être communiquée au Client sur simple demande adressée à la Banque.

12.3.3 Le Client, personne physique, ou la personne physique le représentant, ou sur laquelle portent les données à caractère personnel ci-dessus visées, a le droit d'en obtenir communication et, le cas échéant, d'en exiger la rectification et de s'opposer, pour des motifs légitimes, à ce qu'elles fassent l'objet d'un traitement auprès de la Banque, en écrivant par lettre simple à cette dernière.

12.4 Protection des données à caractère personnel des titulaires de Cartes

12.4.1 Le Client aura accès à différentes données à caractère personnel concernant notamment les titulaires de Cartes. Ces informations ne comprennent pas le code confidentiel (ou tout autre Donnée de sécurité personnalisée) d'utilisation de la Carte et le Cryptogramme Visuel. Le Client ne peut utiliser ces données à caractère personnel que pour l'exécution du Contrat. Sauf obligations légales et réglementaires, il ne peut en faire un quelconque usage qui ne soit pas directement lié avec l'exécution du Contrat. Il s'assure également de l'existence et de la mise en œuvre de dispositifs de protection et de contrôle des accès physiques et logiques à ces données.

12.4.2 Les titulaires de Cartes sur lesquels des données à caractère personnel ont été recueillies doivent pouvoir disposer des droits d'accès, de rectification et d'opposition auprès du Client. A cet égard, le Client s'engage d'ores et déjà à leurs permettre d'exercer ces droits. Dans les cas où le Client souhaite effectuer un traitement des données personnelles pour d'autres finalités que celles décrites au présent Contrat, il s'engage à respecter l'ensemble de la réglementation encadrant ces traitements et notamment la Loi Informatique, Fichiers et Libertés

12.5 Obligations des Parties

12.5.1 Chaque Partie est responsable des données qu'elle traite et est également responsable de la conformité aux prescriptions de la Loi Informatique, Fichiers et Libertés des données transmises à l'autre Partie.

12.5.2 Les Parties s'engagent à se conformer aux dispositions légales applicables aux données à caractère personnel et, à ce titre, s'engagent à respecter les formalités administratives préalables auprès de la CNIL. Le Client s'engage à transmettre, à la première demande de la Banque, la preuve du respect des formalités administratives préalables auprès de la CNIL (déclaration, autorisation, etc.) effectuées dans le cadre du Contrats.

12.5.3 Les Parties s'engagent également à garantir la sécurité et la confidentialité des données, dûment documentées et auditées, conformément aux prescriptions légales et ce y compris en cas de sous-traitance.

12.5.4 Chaque Partie s'engage à collaborer de bonne foi pour les différentes formalités administratives à l'égard de la CNIL et s'engage à faire ses meilleurs efforts pour assurer la conformité des traitements liés au Contrat à l'égard de la Loi Informatique, Fichiers et Libertés.

12.5.5 Chaque Partie s'engage à prendre toutes les précautions nécessaires pour assurer la sécurité des données stockées dans le cadre du Contrat (copie de sauvegarde etc.).

12.5.6 Les Parties s'engagent à s'informer :

(i) régulièrement des évolutions des moyens techniques et organisationnels et/ou de toute évolution de la réglementation ayant une incidence sur les obligations respectives des parties visées dans le présent Contrat ;
(ii) mutuellement de tout incident de sécurité qui aurait pour conséquence une violation des données traitées dans le cadre du Contrat ;
(iii) de tout recours à des prestations externalisées d'hébergement, notamment « Cloud », qui engendrerait un transfert des données vers des Etats ne présentant pas un niveau de protection suffisant par rapport à la réglementation communautaire applicable en la matière.

12.5.7 Les Parties étant tenues par des obligations réciproques, chaque Partie s'engage à permettre à l'autre, dans le cadre du présent Contrat, un accès aux données à caractère personnel en vue de permettre la bonne exécution du Contrat.

ARTICLE 13 : REFERENCEMENT

Sauf convention contraire, la Banque est autorisée à citer à titre de référence le nom du Client, l'adresse de son site Internet (notamment par l'insertion d'un lien hypertexte sur les sites du Groupe Crédit Agricole) et les prestations réalisées pour le Client.

ARTICLE 14 : NON RENONCIATION

Le fait pour le Client ou pour la Banque de ne pas exiger à un moment quelconque l'application d'une clause du présent Contrat, que ce soit de façon permanente ou temporaire, ne peut en aucun cas être considéré comme constituant une renonciation aux droits de cette partie découlant de ladite clause.

ARTICLE 15 : TITRE – PERMANENCE

15.1 En cas de difficulté d'interprétation entre les titres des articles du Contrat et ses annexes et le texte de leur contenu, le texte des articles primera.
15.2 Si l'une quelconque des stipulations du présent Contrat est nulle au regard d'une règle de droit ou d'une loi en vigueur, elle sera réputée non écrite, mais n'entraînera pas la nullité du présent Contrat.

ARTICLE 16 : LOI APPLICABLE ET TRIBUNAUX COMPETENTS

Le présent Contrat et toutes les questions qui s'y rapportent seront régis par le droit français et tout différend relatif à l'interprétation, la validité et/ou l'exécution du présent Contrat est soumis à la compétence des tribunaux français, y compris les procédures tendant à obtenir des mesures d'urgence ou conservatoires, en référé ou sur requête.

ARTICLE 17 : LANGUE DU CONTRAT

La langue utilisée dans le Contrat et pour toute communication effectuée en application des présentes est le français.

ARTICLE 18 : DOMICILIATION

Pour l'exécution du présent Contrat et ses annexes ainsi que de ses suites, les Parties font respectivement élection de domicile en leurs sièges ou adresses indiqués dans les Conditions Particulières.

ARTICLE 19 : RENSEIGNEMENT – RECLAMATION

L'agence est à la disposition du Client pour lui fournir tous les renseignements qu'il pourrait souhaiter sur le fonctionnement du Contrat et répondre à ses éventuelles réclamations.
Dans ce dernier cas, le Client a aussi la possibilité, en écrivant à l'adresse de la Caisse régionale, de faire appel au service client qui s'efforcera de trouver la meilleure solution à son différend.
L'agence ou le service « Clients-Réclamations » répond au Client sur support papier ou sur un support durable convenu avec lui dans les 15 jours ouvrables suivant la réception de la réclamation. Si une réponse ne peut être exceptionnellement donnée dans ce délai de 15 jours pour des raisons échappant au contrôle de la Caisse régionale, celle-ci envoie une réponse d'attente motivant le délai complémentaire nécessaire et précisant la date ultime à laquelle le Client recevra une réponse définitive. Cette réponse définitive devra lui être adressée dans les trente-cinq jours ouvrables suivant la réception de la réclamation.
Si le Client n'a pas pu résoudre au préalable son différend auprès du service « Clients-Réclamations » par une réclamation écrite, il a également la possibilité, si la réglementation le prévoit, de s'adresser gratuitement à l'instance de règlement extrajudiciaire des litiges proposée par la Caisse Régionale, dont les coordonnées et les modalités de saisine sont disponibles sur le site Internet de la Caisse régionale ca-nord-est.fr
Aux fins de cette procédure, le Client autorise expressément la Caisse Régionale à communiquer à l'instance de règlement extrajudiciaire compétente tous les documents et informations utiles à l'accomplissement de sa mission. Le Client délie la Caisse Régionale du secret bancaire le concernant, pour les besoins de cette procédure.

ARTICLE 20 : DEMARCHAGE BANCAIRE ET FINANCIER

Lorsqu'un acte de démarchage précède la conclusion du présent Contrat, le Client dispose d'un délai de quatorze (14) jours calendaires révolus pour se rétracter sans frais ni pénalités et sans être tenu d'indiquer les motifs de sa décision. Ce délai court à compter de la conclusion du Contrat ou de la réception des conditions contractuelles et informations préalables si celle-ci est postérieure.
Le commencement d'exécution ne prive pas le Client du droit de rétractation.
La rétractation met fin au Contrat de plein droit. Le Client sera tenu au paiement du prix correspondant à l'utilisation du produit pour la période comprise entre la date de commencement d'exécution du Contrat et de la date de rétractation, à l'exclusion de toute autre somme.

Le Client peut exercer son droit de rétractation au moyen du formulaire joint ou d'une déclaration dénuée d'ambigüité (lettre, télécopie ou courrier électronique) envoyée à son agence.

ARTICLE 21 : LUTTE CONTRE LE BLANCHIMENT DES CAPITAUX, LE FINANCEMENT DU TERRORISME, LA CORRUPTION ET LA FRAUDE – RESPECT DES SANCTIONS INTERNATIONALES

La Banque est tenue de respecter les dispositions légales et réglementaires relatives à la lutte contre le blanchiment des capitaux, le financement du terrorisme et plus généralement, à exercer une vigilance constante sur les opérations effectuées par ses clients.

La Banque est également tenue d'agir conformément aux lois et réglementations en vigueur dans diverses juridictions, en matière de sanctions économiques, financières ou commerciales, et de respecter toute mesure restrictive relative à un embargo, au gel des avoirs et des ressources économiques , à des restrictions pesant sur les transactions avec des individus ou entités ou portant sur des biens ou des territoires déterminés émises, administrées ou mises en application par le Conseil de sécurité de l'ONU, l'Union européenne, la France, les États-Unis d'Amérique (incluant notamment le bureau de contrôle des Actifs Etrangers rattaché au Département du Trésor, l'OFAC et le Département d'État) et par des autorités locales compétentes pour édicter de telles sanctions (ci-après les « Sanctions Internationales »).

La Banque peut être amenée à suspendre ou rejeter une opération de paiement ou de transfert émise et/ou reçue, qui pourrait être ou qui, selon son analyse, serait susceptible d'être, sanctionnée par toute autorité compétente, ou le cas échéant, à bloquer les fonds et les comptes du Client.

La Banque peut être amenée à demander au Client de lui fournir des informations concernant les circonstances et le contexte d'une opération tels que la nature, la destination et la provenance des mouvements des fonds, ainsi que des justificatifs nécessaires pour appuyer ces explications, notamment en cas d'opération particulière par rapport aux opérations habituellement enregistrées sur son compte.

Le Client est tenu de communiquer immédiatement les informations exigées. Tant que le Client n'a pas fourni les informations demandées par la Banque ou que les informations ne sont pas jugées suffisantes, la Banque se réserve le droit de ne pas exécuter ses instructions.

La Banque peut également être amenée à réaliser des investigations dans le cadre de la réalisation de toute opération qui pourrait être ou qui, selon son analyse, serait susceptible d'être, sanctionnée par toute autorité compétente, conduisant le cas échéant, à retarder l'exécution des instructions du Client.

PARTIE II - CONDITIONS GENERALES SPECIFIQUES A CHAQUE SCHEMA DE CARTE DE PAIEMENT

La présente partie II des Conditions Générales précise les Conditions Générales spécifiques à chaque Schéma dont la (l'une des) marque(s) est apposée sur la Carte ; elles viennent compléter les Conditions Générales communes précisées en partie I.

I. DISPOSITIONS SPECIFIQUES AUX SCHEMAS INTERNATIONAUX

ARTICLE 1 - DEFINITION DES SCHEMAS DE CARTES DE PAIEMENT INTERNATIONAUX

1.1 Les schémas de cartes de paiement internationaux permettent la réalisation, dans les conditions prévues dans les Conditions Particulières et les présentes Conditions Générales (parties I et II), de réaliser des opérations de paiement en France ainsi qu'à l'étranger.

1.2 Les schémas internationaux inclus dans le périmètre du présent Contrat sont notamment :

(i) VISA Inc. et VISA Europe

(ii) Mastercard Europe SA

1.3 Les schémas internationaux reposent sur l'utilisation des Cartes portant notamment les marques suivantes :

(i) Pour VISA Inc. et VISA Europe : Visa, V PAY, Visa Electron

(ii) Pour Mastercard Europe SA : Mastercard, Maestro.

ARTICLE 2 - DISPOSITIONS SPECIFIQUES AUX SCHEMAS VISA ET MASTERCARD

2.1 Obligations de la Banque

Par dérogation à l'article 4.6 de la partie I Conditions Générales, la Banque s'engage à ne pas débiter, au-delà du délai maximum de 24 (vingt-quatre) mois à partir de la date du crédit initial porté au compte du Client les opérations de paiement non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.

2.2 Garantie de paiement

Pour les opérations de paiement réalisées à l'aide d'une Carte émis(e) hors de l'EEE, la garantie de paiement n'est pas acquise en cas de contestation du titulaire de la Carte liée à la relation sous-jacente.

II. DISPOSITIONS SPECIFIQUES AU SCHEMA CB

1. Le Schéma CB repose sur l'utilisation de Cartes portant la Marque CB (ci-après les "Cartes CB") auprès des Clients adhérant au Schéma CB dans le cadre des seules dispositions et procédures définies ou homologuées par le GIE CB.

Le GIE CB intervient notamment, pour des raisons sécuritaires, dans les modifications du seuil de demande d'autorisation, la suppression de l'acceptabilité de certaines Cartes CB ou application de paiement CB et la suspension de l'adhésion au Schéma CB. Il établit les conditions du contrat d'adhésion, la Banque définissant certaines conditions spécifiques de fonctionnement.

Lorsque la Banque représente le GIE CB, le terme de "représentation" ne concerne que l'ensemble des conditions techniques d'acceptation de la Carte CB et de remise des opérations à la Banque, et non la mise en jeu de la garantie du paiement visée à l'article 5 de la partie I des Conditions Générales du présent Contrat.

2. Disposition relatives aux Cartes CB et Solutions de paiement CB

Sont utilisables dans le Schéma CB et dans le cadre du présent Contrat :

- Les cartes sur lesquelles figure la Marque CB,
- les solutions de paiement CB.

3. Dispositions sur l'acceptation de Cartes CB

En complément des dispositions de la partie I des Conditions Générales du présent Contrat, le Client s'engage :

- à accepter les Cartes CB pour le paiement d'achats de biens ou de prestations de services offerts à sa clientèle et réellement effectués même lorsqu'il s'agit d'articles vendus à titre de promotion ou de soldes, pour le paiement de dons et en contrepartie du règlement du montant de cotisations.
- à transmettre les enregistrements des opérations de paiement à la Banque dans les délais prévus dans les Conditions Particulières convenues avec lui. Au-delà d'un délai maximum de 6 (six) mois après la date de l'opération, l'encaissement des opérations de paiement n'est plus réalisable dans le cadre du Schéma CB.
- en cas de demande d'audit par le GIE CB, à permettre à la Banque de faire procéder aux frais du Client dans les locaux du Client ou dans ceux des tiers visés à l'article 3.16 de la partie I des Conditions Générales du présent Contrat, à la vérification par un tiers indépendant du respect tant des clauses du présent Contrat que des exigences du Référentiel Sécuritaire Accepteur et/ou du Référentiel Sécuritaire PCI/DSS. Cette vérification, appelée « procédure d'audit », peut intervenir à tout moment dès la conclusion du présent Contrat et/ou pendant sa durée.

Au cas où le rapport remis aux Parties par le tiers indépendant à l'issue de la procédure d'audit révélerait un ou plusieurs manquements à ces clauses ou exigences, le GIE CB peut procéder à une suspension de l'acceptation des Cartes CB, voire à une radiation du Schéma CB tel que prévu à l'article 5.4 de la présente Partie II des Conditions Générales.

Le Client autorise la communication du rapport à la Banque et au GIE CB.

4. Réclamation

Toute réclamation doit être formulée par écrit à la Banque, dans un délai maximum six (6) mois à compter de la date de l'opération contestée, sous peine de forclusion.

Ce délai est réduit à une durée de quinze (15) jours calendaires à compter de la date de débit en compte résultant d'une opération non garantie.

5. Mesures de prévention et de sanction mises en œuvre par la Banque

5.1 En cas de manquement du Client aux dispositions relatives au Schéma CB du présent Contrat ou aux lois en vigueur ou en cas de constat d'un taux d'impayés anormalement élevé ou d'utilisation anormale de Cartes CB perdues, volées ou contrefaites, la Banque peut prendre des mesures de sauvegarde et de sécurité consistant, en premier lieu, en un avertissement au Client valant mise en demeure précisant les mesures à prendre pour remédier au manquement ou résorber le taux d'impayés anormalement élevé constaté.

5.2 Si dans un délai de trente (30) jours, le Client n'a pas remédié au manquement ayant justifié l'avertissement ou n'a pas mis en œuvre les

mesures destinées à résorber le taux d'impayés constaté, la Banque peut résilier de plein droit avec effet immédiat le présent Contrat, par lettre recommandée avec demande d'avis de réception.

5.3 De même, si dans un délai de trois (3) mois à compter de l'avertissement, le Client est toujours confronté à un taux d'impayés anormalement élevé, la Banque peut décider la résiliation de plein droit avec effet immédiat du présent Contrat, notifiée par lettre recommandée avec demande d'avis de réception.

5.4. Mesures de prévention et de sanction mises en œuvre par le GIE CB

En cas de manquement du Client aux dispositions du présent Contrat concernant les mesures de sécurité ou en cas de taux d'impayés constaté anormalement élevé (notamment dans les hypothèses où le Client ventile ses remises en paiement entre plusieurs acquéreurs de sorte qu'aucun de ceux-ci n'est en mesure d'avoir une vision globale de son taux d'impayés), le GIE CB peut prendre des mesures de sauvegarde et de sécurité consistant en :

- la suspension de l'acceptation des Cartes CB par le Client. Cette suspension intervient s'il n'est pas remédié aux problèmes constatés dans un délai de trois (3) mois suivant la mise en demeure d'y remédier.
  Ce délai peut être ramené à quelques jours en cas d'urgence et à un (1) mois au cas où le Client aurait déjà fait l'objet d'une mesure de suspension dans les vingt-quatre (24) mois précédant l'avertissement.
  La suspension de l'adhésion au Schéma CB peut être immédiate lorsqu'elle est décidée en raison d'un des motifs suivants :
  - une utilisation anormale de Cartes perdues, volées ou contrefaites,
  - une utilisation du Système d'Acceptation non agrée,
  - un risque de dysfonctionnement important du Schéma CB,
  - une utilisation anormale ou détournée du Système d'Acceptation.

  La suspension est notifiée par l'envoi d'une lettre recommandée et motivée, avec demande d'avis de réception. Cette suspension prend effet deux (2) jours francs à compter de la réception de la notification.
- La radiation de l'adhésion du Client au Schéma CB en cas de survenance de manquements d'une exceptionnelle gravité, de comportement dolosif ou frauduleux ou en cas de persistance d'un taux anormalement élevé d'incidents ayant déjà justifié antérieurement une mesure de suspension vis-à-vis du Client concerné. Cette radiation est notifiée par l'envoi d'une lettre recommandée et motivée avec demande d'avis de réception.

5.5. En cas de suspension ou de radiation, le Client s'engage alors à restituer à la Banque les dispositifs techniques et sécuritaires et les documents en sa possession dont la Banque est propriétaire et à retirer immédiatement de ses supports de communication tout signe d'acceptation des Cartes CB

5.6. La période de suspension est au minimum de six (6) mois, éventuellement renouvelable.

A l'expiration de ce délai, le Client peut, sous réserve de l'accord préalable du GIE CB, demander la reprise d'effet du présent Contrat auprès de la Banque, ou souscrire un nouveau contrat d'acceptation avec un autre acquéreur de son choix.

Cette reprise d'effet ou cette nouvelle d'adhésion pourra être subordonnée à la mise en œuvre de recommandations d'un auditeur désigné par le GIE CB ou l'acquéreur concerné, et portant sur le respect des bonnes pratiques en matière de vente et/ou de prestations réalisées à distance.

LES CONDITIONS SPECIFIQUES DE FONCTIONNEMENT DE L'OPTION « SERVICES E-TRANSACTIONS »

Les présentes conditions spécifiques détaillent les conditions de fonctionnement de l'Option « Services E-Transactions ». Elle trouve à s'appliquer en sus des Conditions Générales du Contrat et sauf dispositions contraires dudit Contrat que le Client aura souscrit préalablement ou concomitamment.

Les Services E-transactions sont des services techniques d'accès et d'utilisation de la plateforme E-transactions permettant la réalisation technique et la gestion de paiements à distance. Ces Services incluent aussi des prestations d'assistance technique et de contournement des anomalies.

ARTICLE 1 : DEFINITIONS

Au-delà des définitions insérées dans la partie I des Conditions Générales du Contrat, dans le cadre de l'Option « Services E-transactions », les termes suivants sont définis :

« Anomalies » : désigne tout dysfonctionnement ou toute non-conformité fonctionnelle ou technique de la Plateforme E-transactions par rapport aux exigences techniques et fonctionnelles résultant des présentes conditions de fonctionnement de l'Option.

« 3D Secure » : désigne le protocole sécurisé de paiement sur Internet (VerifiedbyVisa© pour VISA et Mastercard Securecode© pour MASTERCARD) permettant de sécuriser les transactions en demandant des informations complémentaires à l'Utilisateur de l'Instrument de paiement avant la validation du paiement afin de l'authentifier.

« Back office » : désigne les fonctions de la Plateforme E-transactions permettant notamment le suivi et la gestion des ordres de paiement.

« Fonctionnalité(s) » : désigne le(s) service(s) et option(s) dont le Client dispose ou peut disposer dans le cadre de l'Option « Services E-transactions » en fonction de l'Offre qu'il aura choisie.

« Identifiants » : désigne le couple identifiant/mot de passe permettant au Client de se connecter sur le Site.

« Instrument de paiement » : désigne tout dispositif personnalisé et/ou ensemble de procédures arrêté pour initier un ordre de paiement via la Plateforme E-transactions. Il peut s'agir d'une Carte ou d'une Solution de paiement du type Paylib ou MasterPass ou d'un moyen de payer fourni par la Banque ou par un prestataire de services de paiement autre que la Banque.

« Logiciel E-transactions » : désigne l'ensemble des modules applicatifs ou techniques permettant de remplir une ou plusieurs fonctions et la documentation associée.

« Marketplace » : ou « place de marché » désigne une plateforme (par exemple un site internet) offrant (i) la possibilité à plusieurs commerçants en ligne de vendre leurs produits et/ou services sur cette plateforme technique commune facilitant ainsi la mise en relation entre acheteurs et vendeurs, et (ii) un service d'intermédiaire entre un commerçant et la banque acquéreur réalisant ainsi notamment une activité d'agrégation de transactions.

« Offre(s) » : désigne (i) l'offre Access, ou (ii) l'offre Premium, ou (iii) l'Offre « Téléphone, Fax, Courrier », que choisit le Client lorsqu'il souscrit à l'Option « Services E-transactions ».

« Plateforme E-transactions » : désigne la plateforme informatique mise à disposition du Client par la Banque, permettant l'exécution technique de l'opération de paiement entre le Client et l'Utilisateur de l'Instrument de paiement, et d'assurer les contrôles lors des paiements par Cartes.

« Recette » : désigne le processus qui a pour objet de vérifier la conformité des Services E-transactions et leurs paramétrages aux besoins du Client.

« Serveur du Client » : désigne tout système informatique permettant d'offrir à distance la vente de biens ou de services. Pour le paiement par Carte de paiement via la Plateforme E-transactions, le Serveur du Client n'intervient pas dans les transactions par Carte.

« Services E-transactions » : désigne les services fournis par la Banque dans le cadre de l'Option « Services E-transactions » comprenant un droit d'accès et d'utilisation de la Plateforme E-transactions et un SAV.

« Service après-vente » ou « SAV » : désigne l'assistance technique à l'utilisation de la Plateforme E-transactions.

« Service ou offre « Téléphone, Fax, Courrier » » : désigne les services de vente à distance par téléphone, fax ou courrier.

« Site » : désigne le site Internet E-transactions édité par la Banque et dont les url sont guest.e-transactions.fr/Vision et guest1.e-transactions.fr/Vision.

« Terminal » : désigne tout dispositif technique permettant à l'Utilisateur de l'Instrument de paiement d'effectuer, hors des locaux du Client, des transactions de paiement à distance avec sa Carte.

« Utilisateur de l'Instrument de paiement » : désigne toute personne qui achète les produits, services ou informations offerts à la vente à distance par le Client sur une boutique virtuelle ou par toute autre plateforme de vente à distance.

ARTICLE 2 : OBJET

Les présentes conditions spécifiques de fonctionnement définissent les conditions dans lesquelles la Banque met à la disposition du Client les Services E-transactions en fonction de l'Offre retenue par ce dernier.

ARTICLE 3 : DESCRIPTION DES OFFRES

Lors de la souscription par le Client à l'Option « Services E-transactions », celui-ci a la possibilité

de choisir entre les Offres « Access » et/ou « Téléphone, Fax, Courrier » ou « Premium ». Chaque Offre est composée d'un socle de Fonctionnalités incluses et d'une ou plusieurs Fonctionnalités optionnelles.

Les Fonctionnalités attachées aux Offres mentionnées dans le présent article sont détaillées à l'article 4 ci-dessous.

L'Offre retenue et les Fonctionnalités optionnelles choisies par le Client figurent aux Conditions Particulières.

La Banque fournira au Client les informations nécessaires (notamment via des manuels mis à sa disposition) pour l'intégration des différentes Fonctionnalités à son système d'information.

3.1 Offre « Access »

(i) Fonctionnalités incluses :
- Plateforme E-transactions pour l'acceptation des paiements à distance (a) avec les Cartes portant les Marques et les Catégories de cartes proposées par la Banque et/ou (b) avec une ou plusieurs Solutions de paiement proposées par la Banque et/ou (c) par le biais de tout autre Instrument de paiement souscrit conformément à l'article 5.3 des présentes conditions spécifiques. Ces Instruments de paiement sont choisis par le Client aux Conditions Particulières ;
- 3D Secure systématique pour chaque opération de paiement ;
- Journal de rapprochement bancaire ;
- Gestion manuelle des encaissements.

(ii) Fonctionnalité optionnelle :
- Option « No Show » (garantie de réservation).

3.2 Offre « Premium »

(i) Fonctionnalités incluses :
- Plateforme E-transactions pour l'acceptation des paiements à distance (a) avec les Cartes portant les Marques et les Catégories de cartes proposées par la Banque et/ou (b) avec une ou plusieurs Solutions de paiement proposées par la Banque et/ou (c) par le biais de tout autre Instrument de paiement souscrit conformément à l'article 5.3 des présentes conditions spécifiques. Ces Instruments de paiement sont choisis par le Client aux Conditions Particulières ;
- Gestion manuelle ou automatisée des encaissements ;
- Paiement avec remise fractionnée ;
- Paiement en « n fois » ;
- « One clic » ;
- Abonnement simple et complexe ;
- Paramétrage du 3D Secure ;
- Personnalisation de la page de paiement ;
- Affichage multilingue et affichage multidevises ;
- - Journal de rapprochement bancaire.

(ii) Fonctionnalités optionnelles :
- Option « No Show » (garantie de réservation).
- Offre « Téléphone, Fax , Courrier ».

3.3 Offre « Téléphone, Fax, Courrier »

(i) Fonctionnalités incluses :
- Plateforme E-transactions pour l'acceptation des paiements à distance avec les Cartes portant les Marques et les Catégories de cartes proposées par la Banque ou souscrites conformément à l'article 5.3 des présentes conditions spécifiques.
- Abonnement simple et complexe ;
- Journal de rapprochement bancaire ;
- Paiement en « n fois ».

(ii) Fonctionnalités optionnelles :
- Option « No Show » (garantie de réservation) ;
- Requête informatique ;
- Le traitement par lot ;

ARTICLE 4 : DESCRIPTION DES FONCTIONNALITES

E-transactions permet, selon l'Offre et les Fonctionnalités optionnelles retenues par le Client aux Conditions Particulières, de recueillir, sécuriser, contrôler, enregistrer et remettre en recouvrement les ordres de paiement, et de suivre et d'effectuer des opérations de Back office sur ces ordres de paiement. La sécurité des transactions repose sur l'authentification du Client par une clé HMAC générée par le Client, la demande d'autorisation auprès de la banque de l'Utilisateur de l'Instrument de paiement et la confidentialité et l'intégrité des données qui transitent chiffrées sur Internet.

De manière générale, les moyens d'authentification concernant l'accès aux « Services E-transactions » et le traitement des opérations du Client doivent être conservés en sécurité. A ce titre, la clé HMAC est une donnée sensible qui lui permet de se connecter à la Plateforme E-transactions. Il est de la responsabilité du Client de tout mettre en œuvre pour protéger cette clé HMAC sur ses serveurs.

4.1 Le Paiement avec remise fractionnée

4.1.1 Le paiement avec remise fractionnée permet au Client de différer le paiement d'une même transaction en plusieurs fois en fonction du calendrier de livraison du bien ou service objet du paiement.

4.1.2 Le Client remet à la Banque la fraction de l'opération correspondante et déclenche par conséquent le paiement au fur et à mesure des livraisons.

4.1.3 Fonctionnement:
- Toute transaction peut être remise de manière fractionnée.
- Le montant maximum à fractionner correspond au montant de l'opération globale.
- Chacune des échéances fait l'objet d'une demande d'autorisation.
- **Seule la fraction de la transaction remise initialement peut faire l'objet d'une garantie de paiement telle que détaillée à l'article 5 de la partie I des Conditions Générales du Contrat. En conséquence, les remises suivantes ne seront réglées au Client que sous réserve de bonne fin d'encaissement et ce, en l'absence de contestation de l'Utilisateur de l'Instrument de paiement.**

4.1.4 Cette fonctionnalité est gérée au travers de la gestion automatisée des encaissements.

4.2 Paiement en « n fois »

4.2.1 La Fonctionnalité paiement en « n fois » permet de proposer un échelonnement des paiements par carte de paiement dans un délai de quatre-vingt-dix (90) jours maximum dans le cadre d'une transaction. Les montants et les dates sont paramétrables.

4.2.2 Dans son Back office, le Client peut suivre les échéances des paiements des Utilisateurs des Instruments de paiement.

4.2.3 Le Client peut mettre fin à un paiement en « n fois » dans le Back office. Cependant, le Client qui souhaite mettre fin à un paiement en « n fois » devra s'assurer du fait que les engagements contractuels qu'il a pris envers l'Utilisateur de l'Instrument de paiement lors de l'achat du bien ou de la souscription du service à distance lui permettent de réaliser une telle opération. La responsabilité de la Banque ne pourra être recherchée si le Client met fin à un paiement en « n fois » en contradiction avec les engagements contractuels qu'il a pris vis à vis de l'Utilisateur de l'Instrument de paiement.

4.2.4 Fonctionnement:
- **Seule la première échéance de la série bénéficie de la garantie de paiement telle que détaillée à l'article 5 de la partie I des Conditions Générales du Contrat. Les opérations de paiement suivantes ne sont réglées que sous réserve de bonne fin d'encaissement et ce en l'absence de contestation de l'Utilisateur de l'Instrument de paiement.**
- Chacune des échéances fait l'objet d'une demande d'autorisation.
- Le système contrôle que la date de validité de la Carte de paiement ne soit pas postérieure à la dernière échéance de paiement.
- L'ensemble de la transaction doit avoir lieu dans un délai maximum de quatre-vingt-dix (90) jours.
- L'avance des fonds est assurée par le Client, il ne génère pas de ligne de crédit pour l'Utilisateur de l'Instrument de paiement.

4.2.5 Conformément au Code de la consommation, les opérations de crédit comportant un délai de remboursement ne dépassant pas trois (3) mois qui ne sont assorties d'aucun intérêt ni d'aucuns frais ou seulement d'intérêts et de frais d'un montant négligeable ne constituent pas des opérations de crédit à la consommation. Le paiement en « n fois » ne constitue donc pas une opération de crédit à la consommation.

4.3 La Requête informatique

La Requête informatique est une Fonctionnalité optionnelle de l'Offre « Téléphone, Fax, Courrier » qui permet au Client d'intégrer la Plateforme E-transactions à son système d'information afin d'effectuer un certain nombre de traitements automatiques : demandes d'autorisation et résultat du paiement (acceptation ou rejet) sur la base de règles prédéfinies (stock, profil client, etc.).

4.4 Le traitement par lot

4.4.1 Le traitement par lot est une Fonctionnalité optionnelle de l'Offre « Téléphone, Fax, Courrier ».

4.4.2 Cette Fonctionnalité est destinée au Client ayant une activité de vente à distance qui enregistre plusieurs dizaines de paiements par jour et qui a besoin d'une saisie des paiements en masse (stockage des transactions sur fichier et gestion des demandes d'autorisation en rafale sur une plateforme dédiée et sécurisée).

4.4.3 Pour traiter des paiements, notamment recueillis par courrier, et après les avoir saisis dans son système d'information, le Client expédie l'ensemble des paiements via une connexion sécurisée en mode SFTP (Secure File Transfer Protocol) sur la Plateforme E-transactions.

4.4.4 La Plateforme E-transactions relève périodiquement les fichiers de paiements expédiés par le Client et déclenche les demandes d'autorisation pour chacun des paiements. Le résultat des demandes d'autorisation est renvoyé au Client via la connexion sécurisée SFTP. Les transactions sont ensuite traitées comme les opérations saisies manuellement dans E-transactions, et sont visibles dans le Back office.

4.5 Type de remise

Dans le cadre de son adhésion au système de paiement à distance sécurisé, le Client s'engage à

transmettre les enregistrements des opérations à la Banque dans les conditions, notamment les délais, prévus aux Conditions Particulières.

La présente Fonctionnalité permet de paramétrer techniquement sur la Plateforme E-transactions ce transfert ou « remise » :

4.5.1 Remise immédiate

La Plateforme E-transactions transmet automatiquement les enregistrements à la Banque.

4.5.2 Remise avec différé simple

La Plateforme E-transactions peut être paramétrée pour définir un nombre de jours fixe pour transmettre les enregistrements d'opérations.

4.5.3 Remise avec différé avancé

Ce service est inclus dans la « Gestion automatisée des encaissements ». Une fois activée, ce service permet au Client de déclencher manuellement le transfert des enregistrements d'opérations à la Banque (par exemple lors de l'envoi des colis). En conséquence, les remises automatiques sont désactivées.

4.6 L'abonnement simple ou complexe

4.6.1 La gestion des paiements par abonnement simple permet de gérer des ordres de paiement périodiques pour les Utilisateurs d'Instrument de paiement. Ainsi, une fois le paiement initial effectué, l'Utilisateur de l'instrument de paiement sera débité suivant une fréquence préalablement définie et selon des engagements contractuels définis entre lui et le Client.

4.6.2 La gestion de l'abonnement simple est une gestion de base : elle ne prévoit que des cas simples d'abonnements, basés sur la reconduction périodique de paiement d'une même somme, sur une période souhaitée initialement. Ces paramètres ne peuvent pas, par la suite, être modifiés.

4.6.3 L'abonnement complexe est inclus dans la « Gestion automatisée des encaissements ». Dans ce cas toutes les fonctionnalités sont paramétrables (fréquence, montant, etc.) puisque c'est le Client qui définit, pour chaque paiement, la totalité des paramètres à prendre en compte.

4.6.4 L'abonnement peut se terminer de 3 façons :

- A l'échéance : lorsque tous les ordres de paiements prédéterminés par le Client ont été traités avec succès, l'abonnement se termine automatiquement.
- Echec d'un ordre de paiement : quand un ordre de paiement est refusé, les prochains débits s'arrêtent automatiquement et le Client en est informé. Il reviendra au Client d'informer l'Utilisateur de l'Instrument de paiement de l'échec d'un ordre de paiement et des conséquences de cet échec sur l'abonnement.
- Résiliation par le Client : le Client peut mettre fin à un ou à des abonnements à partir de son Back office. Cependant, le Client qui souhaite mettre fin à un ou des abonnements devra s'assurer du fait que les engagements contractuels qu'il a pris envers l'Utilisateur de l'Instrument de paiement lors de la souscription à l'abonnement lui permettent de réaliser une telle opération. La responsabilité de la Banque ne pourra être recherchée si le Client met fin à un abonnement en contradiction avec les engagements contractuels qu'il a pris vis à vis de l'Utilisateur de l'Instrument de paiement.

4.7 One clic

4.7.1 Le paiement « one clic » permet à l'Utilisateur de l'Instrument de paiement de ne plus ressaisir les numéros de sa carte de paiement pour effectuer un prochain achat à l'exception du Cryptogramme Visuel et du code 3D Secure si cette Option est activée.

4.7.2 En cas d'activation de cette Fonctionnalité, le Client est informé que les opérations ne font plus l'objet d'une garantie de paiement.

4.7.3 Pour bénéficier du « one clic », le Client doit disposer de la « Gestion Automatisée des encaissements ».

4.8 Journal de rapprochement bancaire

Le Client via son Back office E-transactions pourra visualiser les flux remis en banque avant compensation.

4.9 Personnalisation de la page de paiement

4.9.1 La page de paiement (par défaut en fond blanc avec le logo de la Banque) peut être personnalisée pour avoir la même charte graphique que celle du site du Client. Le Client doit communiquer son image de fond d'écran à la Banque (en format gif) et sa feuille de style (fichier .css). Les différents droits patrimoniaux attachés aux éléments de personnalisation (image de fond, feuille de style) sont concédés à titre gratuit par le Client à la Banque pendant toute la durée de l'utilisation de cette Fonctionnalité par le Client et pour tous les pays cibles des Services E-transactions.

4.9.2 La concession de droits portera sur les droits définis ci-après :

- le droit de reproduire ou faire reproduire en tout sur tout support les éléments de personnalisation ;
- le droit d'adapter ou de faire adapter tout ou partie des éléments de personnalisation, le droit de corriger, de faire évoluer, de maintenir, de modifier, d'assembler, de transcrire, d'arranger, d'interfacer et de traduire les éléments de personnalisation ;
- le droit de diffuser ou faire diffuser tout ou partie des éléments de personnalisation de quelque manière que ce soit, par tous procédés quels qu'ils soient, connus ou inconnus à ce jour, et notamment par tous réseaux de télécommunication, actuels ou futurs, tels que l'Internet, l'Intranet, par tous moyens de télédiffusion ainsi que la radiodiffusion par tous moyens de télécommunication ;
- le droit de commercialiser, y compris la location et le prêt à titre gratuit ou onéreux ;
- le droit de faire tout usage et toute exploitation, à titre personnel ou au bénéfice de tiers, à titre onéreux ou gratuit, des éléments de personnalisation.

4.10 L'affichage multilingue

4.10.1 Le Client a la possibilité de proposer à l'Utilisateur de l'Instrument de paiement une page de paiement dans sa langue.

4.10.2 Les langues disponibles sont : Français, Anglais, Espagnol, Italien, Allemand, Hollandais, Suédois et Portugais.

4.11 L'affichage multi devise

Sur la page de paiement et à titre informatif uniquement, les devises suivantes peuvent être affichées en bas de page avec les conversions dynamiques (www.xe.com) : Euro, Franc Suisse, Dollar US, Yen, Yuan, Livre Sterling et Dollar canadien.

4.12 3D Secure

4.12.1 3D Secure désigne le protocole sécurisé de paiement sur Internet (VerifiedbyVisa© pour VISA et MastercardSecurecode© pour MASTERCARD) permettant de sécuriser les transactions et d'obtenir de la Banque un justificatif d'acceptation matérialisant les contrôles effectués et la validité de l'ordre de paiement.
En complément de la demande d'autorisation, le programme 3D Secure génère une demande d'authentification de l'Utilisateur de l'Instrument de paiement pour les paiements effectués au moyen de cartes CB, VISA ou MASTERCARD, et ce à partir de la page de paiement d'acceptation.
La réponse à la demande d'authentification générée par le programme 3D Secure est systématiquement transmise au Client. L'obtention du justificatif d'acceptation se matérialise par une réponse positive à la demande d'authentification.
Les opérations ne seront pas garanties en cas de contestation de l'ordre de paiement par l'Utilisateur de l'Instrument de paiement si le Client n'a pas obtenu ce justificatif d'acceptation.
La Banque pourra contrepasser le montant des opérations contestées par les Utilisateurs d'Instrument de paiement pour lesquelles un justificatif d'acceptation n'a pas été obtenu.
Lorsque la Carte n'est pas émise par la Banque, les contestations relatives aux opérations sont matérialisées par un "impayé" adressé par la banque du titulaire de la Carte à la Banque.

14.2.2 Dans le cadre de l'Offre « Premium » de l'Option « Services E-transactions », le 3D Secure peut être **débrayable** (activé en fonction de la connaissance de l'Utilisateur de l'Instrument de paiement) ou **paramétrable** (activé en fonction du montant du panier, de l'origine de la carte, de l'adresse IP, de la cohérence adresse IP/Carte, etc.).

4.12.3 L'activation ou la désactivation du 3D Secure est effectuée sous la seule et unique responsabilité du Client. A nouveau, les opérations ne seront pas garanties en cas de contestation de l'ordre de paiement par l'Utilisateur de l'Instrument de paiement si le Client n'a pas obtenu le justificatif d'acceptation.

4.13 Gestion des encaissements

4.13.1 L'option de « Services E-transactions » comprend un service de Gestion des encaissements favorisant le suivi de l'activité du Client.

4.13.2 La Fonctionnalité Gestion des encaissements donne au Client la possibilité de consulter et d'intervenir sur les paiements réalisés sur son site marchand pour :

- les valider totalement ou partiellement pour les remiser à la Banque,
- les annuler totalement ou partiellement avant qu'ils ne soient remisés à la Banque,
- les rembourser totalement ou partiellement après qu'ils aient été remisés à la Banque.

4.13.3 Cette Fonctionnalité lui permet d'optimiser la gestion de sa trésorerie et d'améliorer le service qu'il rend aux Utilisateurs d'Instrument de paiement en évitant des décalages trop importants entre la livraison et l'encaissement des paiements.

4.13.4 Ce service peut être manuel ou automatisé au choix en fonction de l'Offre choisie par le Client.

4.13.5 Lors de l'installation du Logiciel E-transactions, le Client peut choisir le délai, par défaut "n jours" d'encaissement qu'il souhaite. Ce délai est compris entre 1 et 6 jours.

4.13.6 Le Client doit choisir, lors de la souscription à l'Option « Services E-transactions », entre deux

modes de remise à la Banque des paiements réalisés sur son site :

- soit il souhaite avoir une action de "validation" (manuellement ou de façon automatisée) des encaissements : dans ce cas il doit valider chacune des transactions afin qu'elles soient remisées. Les transactions non validées dans le délai "n jours" seront systématiquement remisées,
- soit il souhaite intervenir sur les transactions pour les "annuler" (manuellement ou de façon automatisée) : à l'inverse du cas précédent, les transactions qui n'auront pas été annulées dans le délai "n jours", seront systématiquement remisées.

4.13.7 Une fois ces étapes réalisées, la souplesse de la Fonctionnalité Gestion des encaissements donne la possibilité au Client :

- d'une part, de valider ou d'annuler partiellement une transaction (par exemple pour palier une indisponibilité d'un produit ou d'un service compris dans une commande de plusieurs articles), et
- d'autre part, d'élargir spécifiquement le délai d'encaissement au-delà de 6 jours (par exemple dans le cas où il est dans l'attente d'une livraison de son fournisseur). **Un délai d'encaissement reporté au-delà de 6 jours suivant la date de la transaction (date de la demande d'autorisation), implique une nouvelle demande d'autorisation conformément à la réglementation interbancaire**. **Dans ce dernier cas**, **les opérations ne seront pas garanties en cas de contestation de l'ordre de paiement par l'Utilisateur de l'Instrument de paiement.**

4.13.8 La Plateforme E-Transactions adresse au Client chaque jour par mail, un journal de fonds des opérations de paiements effectués sur son site.

4.14 <u>Gestion automatisée des encaissements</u>

4.14.1 Cette Fonctionnalité est destinée aux Clients qui traitent plusieurs dizaines de paiements en ligne par jour et qui sont équipés d'une gestion de commande informatisée.

4.14.2 La Banque propose au Client une interface informatique en plus de celle de l'acceptation des paiements à distance sur Internet, lui permettant d'utiliser en automatique, les fonctions de la gestion des encaissements.

4.14.3 Ce service est réservé aux Clients équipés d'un système informatique de traitement des commandes. Une interface en plus de celle de paiement à distance, permet d'interconnecter le système de gestion des commandes à l'environnement E-Transactions en mode sécurisé SSL 128, pour utiliser toutes les commandes possibles de la gestion des encaissements décrites ci-dessus.

4.15 <u>« No Show » (« garantie de réservation »)</u>

4.15.1 Objet

Cette Fonctionnalité optionnelle est ouverte aux Clients hôteliers. Le système No show (garantie de réservation) est un service par lequel le Client s'engage cumulativement:

(i) à maintenir à la disposition d'un Utilisateur d'Instrument de paiement souhaitant réserver une prestation d'hébergement, une chambre jusqu'à l'heure de libération des chambres le lendemain de la date prévue de son arrivée,
(ii) à fournir à cet Utilisateur de l'Instrument de paiement les prestations prévues à l'article 4.15.4 ci-après si la chambre retenue n'était pas disponible.

4.15.2 Modalités de réservation

Le Client doit fournir, de **manière préalable,** à l'Utilisateur de l'Instrument de paiement l'ensemble des informations suivantes :

- le contenu de la prestation (par exemple, caractéristique de la chambre, prix….),
- l'objet du service (article 4.15.1 ci-dessus),
- le fait que s'il n'est pas arrivé avant l'heure de libération de la chambre, il lui sera facturé par chambre réservée un montant correspondant à une nuit dans l'hôtel, taxes comprises (facture No show),
- qu'il peut toutefois annuler sa réservation, sans frais, au plus tard jusqu'à 18h (heure locale de l'hôtel) le jour d'arrivée prévu, en précisant qu'il s'agissait d'une réservation garantie et qu'il lui sera alors attribué un numéro d'annulation,
- Qu'il ne lui sera pas prélevé de facturation pour ce service.

4.15.3 Réservation

En cas d'accord de l'Utilisateur de l'Instrument de paiement, le client doit cumulativement :

- lui demander des données figurant en relief sur la carte (Numéro, nom et date de validité), ainsi que son adresse,
- Communiquer et / ou confirmer la réservation par lettre, en cas de demande expresse de l'Utilisateur de l'Instrument de paiement,
- Etablir une fiche de réservation au nom du client et mentionner sur cette fiche le numéro de la chambre qui lui est attribuée.

4.15.4 Fourniture des prestations compensatrices

Si, exceptionnellement, la chambre retenue n'était pas disponible au moment de l'arrivée de l'Utilisateur de l'Instrument de paiement quelle que soit son heure d'arrivée, jusqu'à l'heure de libération des chambres, l'hôtelier doit, sans aucun frais supplémentaire pour ledit Utilisateur :

- lui procurer pour une nuit une chambre dans un autre hôtel de classe au moins égale à un prix au plus égal au prix de la chambre réservée,
- le transporter jusqu'à cet hôtel,
- lui rembourser, s'il le souhaite, le prix de la communication téléphonique de trois minutes entre cet hôtel et sa famille ou son bureau,
- lui transmettre à la nouvelle adresse, pendant la période de réservation, tout message ou tout appel le concernant.

4.15.5 Annulation de la réservation

L'hôtelier doit accepter une annulation de réservation garantie si elle est faite avant dix-huit (18) heures (heure locale de l'hôtel), le jour prévu de l'arrivée. Il indiquera au client un numéro d'annulation à faire valoir en cas de contestation. L'hôtelier doit confirmer par écrit cette annulation en cas de demande de l'Utilisateur de l'Instrument de paiement.

4.15.6 Défection du client: émission d'une facture "No show"

Si l'Utilisateur de l'Instrument de paiement ne s'est pas présenté avant l'heure de libération des chambres et n'a pas annulé la réservation dans les conditions prévues à l'article 4.15.5 ci-dessus, l'hôtelier a la possibilité d'émettre une facture dite « No show » pour un montant correspondant au prix d'une nuitée.
La facture « No show » devra comporter les indications cumulatives suivantes :

- Numéro, nom, date de validité de la Carte,
- Montant dû et éventuel numéro d'autorisation,
- Date de transaction : celle du jour d'expiration de la réservation,
- Mention « No show » dans la zone prévue pour la signature,
- Numéro de la chambre réservée dans la zone prévue pour le numéro de certificat.

4.15.7 Garantie de paiement de la facture « No show »

Outre les cas visés dans les Conditions Générales du Contrat, la garantie de paiement de la facture « No show » ne sera pas acquise au Client dans les cas suivants :

- la réservation a été annulée à temps (avant 18 heures du jour prévu de l'arrivée) et le numéro d'annulation a été communiqué,
- l'Utilisateur de l'Instrument de paiement est bien arrivé à l'hôtel et il a réglé ses prestations sur place,
- l'utilisateur a bénéficié des prestations compensatrices (cf. article 4.15.4 ci-dessus),
- l'Utilisateur de l'Instrument de paiement a écrit qu'il n'a jamais participé à cette transaction, qu'il ne l'a jamais autorisée, ou qu'il conteste le montant,
- la réservation a été effectuée avec un numéro de carte erroné, inexistant ou périmé.

Pour chacun de ces cas, l'hôtelier autorise la Banque à débiter son compte du montant de la facture « No show ».
Il s'engage à conserver pendant un an à compter de la remise à l'encaissement de la facture « No show », la fiche de réservation portant le numéro de la chambre attribuée à l'utilisateur.

ARTICLE 5 : SOUSCRIPTION A DES INSTRUMENTS DE PAIEMENTS

Le Client peut choisir d'accepter tout ou partie des Marques, des Catégories de carte et Instruments de paiement proposés par la Banque, sous réserve d'information de sa clientèle.

5.1 <u>Marques / Catégories de cartes</u>

Par défaut, l'Option « Services E-transactions » intègre un service technique d'acceptation des paiements par Cartes portant une ou plusieurs des Marques suivantes : CB, VISA et Mastercard.

5.2 <u>PAYLIB</u>

Par défaut, l'Option « Services E-transactions » intègre l'acceptation technique des paiements par cartes via la Solution de paiement Paylib (ci-après « Paylib »).

5.2.1 Description de la Solution Paylib

Paylib est un service permettant à l'utilisateur du service de stocker de façon sécurisée les références de Cartes de paiement afin de permettre de réaliser des opérations de paiement (i) par Internet (via un PC ou une tablette) ou un téléphone mobile, avec une authentification sécurisée permettant au client final de ne pas saisir ses références bancaires lors de chaque opération, et (ii) en proximité sur un terminal de paiement via une application mobile.

Sur internet, Paylib s'appuie sur les acteurs et les interfaces monétiques existants : le parcours de paiement Paylib se substitue à la phase de saisie des numéros de carte, de la date de fin de validité et du numéro dit « CVX2 » par le titulaire de la Carte, ainsi qu'au processus 3D Secure pour les commerçants enrôlés 3D.

Les opérations de paiement Paylib contestées par le titulaire de la Carte pour défaut d'autorisation sont supportées par le prestataire de service de paiement qui a émis la Carte utilisée par le biais de

la Solution Paylib. En conséquence, les opérations de paiement Paylib entrent dans le cadre du paiement à distance sécurisé tel que défini par le Règlement Interbancaire du Paiement par Carte (RIPC) du Groupement des Cartes Bancaires « CB » et sont donc soumises aux règles propres à ce type de paiement, notamment en matière d'impayés.

5.2.2 Fonctionnement de Paylib

(i) Installation :

Paylib ne nécessite pas d'installation spécifique sur la Plateforme E-transactions.

(ii) Le bouton Paylib :

Le bouton Paylib apparaitra automatiquement sur la page de paiement proposée dans le cadre de L'Option « Services E-transactions » dès lors que l'enrôlement aura été réalisé. Si le Client a sa propre page de paiement, il lui appartient de paramétrer le bouton Paylib sur ladite page.

(iii) Parcours de paiement Paylib :

Le parcours de paiement est simplifié afin d'améliorer l'expérience client. Cependant, concernant notamment les processus d'authentification, il reste en tous points compatibles avec les Conditions Générales du Contrat.

Le titulaire du portefeuille Paylib :

- valide son panier et choisit le bouton Paylib,
- est redirigé vers la page de validation de paiement Paylib,
- saisit son adresse de courrier électronique et, dans l'hypothèse où celui-ci lui est demandé, son mot de passe Paylib,
- valide, le cas échéant, la demande de paiement selon les modalités imposées par sa banque.

L'ensemble des actions disponibles pour ce moyen de paiement sont réalisables via le Back office E-transactions qui fournira aussi un reporting pour ce moyen de paiement

Pour les opérations de paiements effectuées avec Paylib, le Client peut bénéficier de la garantie de paiement aux conditions détaillées dans la partie I des Conditions Générales du présent Contrat.

5.2.3 Obligations spécifiques du Client

Le Client s'engage à :

(i) Collaborer régulièrement et activement avec la Banque dans l'intérêt du bon fonctionnement de Paylib,

(ii) Ne pas revendre, partager, louer ou mettre Paylib à la disposition de tout tiers d'une quelconque autre façon.

Toute communication sous quelque forme que ce soit et quel qu'en soit le support devra (a) être conforme à la « charte d'utilisation de la marque et du logo Paylib », dont la version en vigueur au jour de la communication est disponible sur le site E-transactions, et (b) sera soumise à l'accord préalable et écrit de la Banque

5.2.4 Référencement du Client

Le Client autorise la Banque et la société Paylib Services (société par actions simplifiée dont le siège est situé au 1 boulevard Haussmann – 75009 Paris, immatriculée sous le numéro 522 048 032 RCS PARIS) à citer à titre de référence le nom du Client, son activité, son adhésion à la Solution Paylib et l'adresse de son site internet (notamment par l'insertion d'un lien hypertexte sur leurs propres sites).

5.3 <u>Autres Instruments de paiement non proposés par la Banque</u>

5.3.1 Le Client peut demander à pouvoir utiliser la Plateforme E-transactions pour accepter techniquement des paiements avec d'autres Marques ou Catégories de carte ou Solutions de paiement ou moyens de payer (ensemble dénommés les « Instruments de paiement ») non proposés par la Banque.

L'acceptation de ces autres Instruments de paiement nécessite la signature d'un contrat directement entre le Client et le prestataire de service de paiement concerné, la Plateforme E-transactions et donc la Banque n'intervenant uniquement que pour la transmission sécurisée des données.

5.3.2 Les Parties conviennent expressément que :

(i) L'accès aux services optionnels d'acceptation technique de ces autres Instruments de paiement non proposés par la Banque <u>nécessite au préalable</u> :
- la signature d'un contrat directement entre le Client et le prestataire de service de paiement, et
- l'accord de la Banque.

(ii) Les conditions d'adhésion et d'acceptation du/par le Client de ces autres Instruments de paiement sont détaillées dans le contrat signé directement entre le Client et le prestataire de service de paiement.

(iii) La Banque n'est pas partie à (a) l'adhésion du Client à ces autres Instruments de paiement, et (b) leur acceptation par le Client. Ainsi, la Banque offre uniquement la possibilité de configurer la Plateforme E-transactions pour recevoir techniquement ces Instruments de paiement.

(iv) La Banque reste étrangère à tout litige portant sur l'adhésion et l'acceptation du/par le Client de ces Instruments de paiement.

(v) le Client garantit la Banque contre toute action, revendication ou opposition intentée par le prestataire de service de paiement ou par des tiers au motif notamment que le recours aux Instruments de paiement par le Client constitue une contrefaçon de droits préexistants de propriété intellectuelle revendiqués par son personnel ou des tiers, ou un acte de concurrence déloyale et/ou parasitaire auquel l'exécution du présent Contrat aurait porté atteinte.

5.3.3 La mise en œuvre des autres Instruments de paiement sur la page de paiement de la Plateforme E-transactions sera réalisée grâce aux identifiants préalablement communiqué par le prestataire de service de paiement au Client. En fonction des Instruments de paiement, la Plateforme E-transactions collecte les données et les redirige au prestataire de service de paiement concernés ou redirige vers la page de paiement du prestataire de service de paiement.

5.3.4 Obligations spécifiques du Client Masterpass

Masterpass est une Solution de paiement technique proposée directement par Mastercard et permettant aux clients internautes du Client de stocker de façon sécurisée les données de sa (de ses) Carte(s) de paiement(s) afin de réaliser des paiements par Carte sur Internet sans avoir à ressaisir à chaque opération les données de cette dernière.

Les conditions d'adhésion et d'acceptation de la solution Masterpass de Mastercard auxquelles le Client doit se conformer sont disponibles sur le site suivant : https://masterpass.com/assets/pdf/masterpassoperatingrules.pdf

Les dispositions des articles 5.3.2 et 5.3.3 sont applicables à la solution Masterpass qui est souscrite directement entre Mastercard et le Client

5.4 <u>Retrait des Instruments de paiement</u>

Le Client peut demander lors de la souscription de la présente Option, ou à tout moment au cours de son exécution, la suppression de Paylib et/ou de la connexion à Masterpass par simple demande auprès de la Banque.

ARTICLE 6 : OBLIGATIONS DU CLIENT

6.1 Le Client s'engage à :

(i) collaborer régulièrement et activement avec la Banque dans l'intérêt du bon fonctionnement de l'Option ;

(ii) appliquer strictement les consignes d'accès et d'utilisation de la Plateforme E-transactions, des Instruments de paiement et des Fonctionnalités qu'il a souscrites et qui sont décrites dans la documentation mise à disposition, y compris lors des mises à jours du Logiciel E-transactions ;

(iii) ne pas utiliser l'Option à des fins de commercialisation de produits illicites ;

(iv) ne pas diffuser tout message ou toute information quelle que soit sa forme ou sa nature à caractère injurieux, diffamatoire, raciste, xénophobe, révisionniste ou portant atteinte à l'honneur à la réputation d'autrui, ou inciter à la discrimination, à la haine d'une personne ou d'un groupe de personnes en raison notamment de leur origine ou de leur appartenance à une ethnie, une nation, une nationalité, une religion déterminée ;

(v) ne pas diffuser tout message ou information, quelle que soit sa forme ou sa nature menaçant une personne ou un groupe de personnes, à caractère pornographique ou pédophile, incitant au vol, au crime et aux actes de terrorisme ou faisant l'apologie des crimes, des actes de terrorisme, des crimes de guerre ou des crimes contre l'humanité, ayant pour objet la promotion d'activités contraires à l'ordre public et aux bonnes mœurs, permettant à des tiers de se procurer directement ou indirectement des logiciels piratés, des numéros de séries de logiciels, des logiciels permettant des actes de piratage et d'intrusion dans les systèmes informatiques de télécommunication, des virus et d'une manière générale tout logiciel ou autre permettant de porter atteinte aux droits d'autrui et à la sécurité des personnes et des biens, protégé au titre de la propriété intellectuelle et/ou du droit des marques.

(vi) ne pas créer tout lien hypertexte avec des sites ne respectant pas ces mêmes principes ;

(vii) accepter un contrôle de la Banque ou de toute société qu'elle aura désignée à cet effet sur son activité ;

(viii) faire seul son affaire des litiges qui pourraient survenir entre lui et l'Utilisateur de l'Instrument de paiement du fait du non-respect des obligations auxquelles il est astreint, notamment a) l'obligation d'informations précontractuelles et contractuelles; b) les règles relatives aux opérations de paiement différées qui pourraient être constitutives, sous conditions, d'opérations de crédit à la consommation ; c) les règles spécifiques

relatives à la fourniture de certains produits ou services ;

(ix) faire son affaire personnelle des litiges commerciaux et de leurs conséquences financières pouvant survenir avec les Utilisateurs d' Instruments de paiement concernant les biens et services dont le montant a été réglé par un des Instruments de paiement auxquels le Client aura souscrit ;

(x) faire son affaire personnelle de l'acquisition, de l'installation, de la maintenance de son système informatique et de son raccordement au réseau Internet, ainsi que de sa protection au moyen d'un « pare-feu » (firewall) et d'un antivirus à jour ;

(xi) faire ou faire faire les développements pour l'installation et l'activation du Logiciel E-transactions sur son système d'information et pour la connexion à la Plateforme E-transactions selon la documentation qui lui a été mise à disposition ; à cet égard, le Client déclare disposer des ressources matérielles et logicielles informatiques ainsi que des compétences nécessaires en vue du fonctionnement des Services E-transactions.

(xii) installer ou à faire installer et activer les mises à jour ou livraisons du Logiciel E-transactions dans un délai de six (6) mois maximum. Le téléchargement est possible à partir de la Plateforme E-transactions ;

(xiii) accepter les modifications consécutivement à toute demande de mise en production faite à la Banque, selon les termes de la documentation mise à disposition ;

(xiv) traiter toute question relative au fonctionnement de la Plateforme E-transactions avec le SAV de la Banque, à l'exclusion des Instruments de paiement ou des Marques de Cartes souscrits par ses soins. A ce titre, le Client reconnaît qu'il devra prendre l'attache du fournisseur de l'Instrument de paiement ou de la Marque de Carte auprès de qui il a souscrit ledit Moyen.

(xv) s'interdire notamment de dupliquer, corriger, décompiler et assembler le Logiciel API E-transactions avec un autre logiciel du marché ou spécifique.

(xvi) ne pas utiliser les Services E-transactions pour se positionner en tant qu'intermédiaire entre un commerçant tiers et la Banque (facilitateurs de paiement, galeries marchandes Internet, "agrégateurs" E-commerce, Marketplace) et de manière générale à toute autre fin que celle prévue aux présentes ;

(xvii) intégrer les Service E-transactions en « HMAC ». Le non-respect de cette condition pourra entrainer la résiliation de l'Option « Services E-transactions » dans les conditions prévues à l'article 11 ci-après. ;

(xviii) tenir informé dans les meilleurs délais la Banque de toute évolution de la relation contractuelle avec les fournisseurs d'Instruments de Paiement auxquels le Client aura souscrit (notamment en cas de résiliation).

6.2 Le Client est responsable de l'utilisation des Services E-transactions ainsi que de l'utilisation de ses éléments d'identification. A ce titre :

(i) Le Client s'engage à ne pas mettre à la disposition d'un tiers au Contrat ou de toute personne qu'il n'aura pas expressément habilitée, sous quelque forme que ce soit, directement ou indirectement, ses Identifiants et plus généralement, les méthodes d'accès à la Plateforme E-transactions et les informations transmises de façon sécurisée ;

(ii) Le Client reconnaît que toute utilisation des Services E-transactions avec leurs éléments d'Identification est présumée faite par le Client et lui sera imputée, à charge pour le Client d'apporter la preuve contraire.

6.3 Lors d'une opération de paiement par Cartes le Client s'engage également à respecter les indications données par la Plateforme E-transactions et suivre les procédures dont les modalités techniques lui ont été indiquées.

6.4 Dans l'hypothèse où le Client souhaiterait faire réaliser une prestation informatique, qu'elle qu'en soit sa nature, en relation directe ou indirecte avec l'objet du Contrat, il s'engage à s'adresser en priorité aux compétences de la Banque. En cas de non-respect de cet engagement, la Banque aura la faculté de résilier l'Option « Services E-transactions » dans les conditions prévues à l'article 11 ci-après.

Les modifications, extensions ou diminutions des travaux, demandées par le Client ne sont exécutées qu'après avoir fait l'objet d'un devis de la Banque et d'une acceptation du Client par la signature d'un avenant signé des deux parties.

Toutefois, la Banque a toujours la possibilité de refuser toute modification, extension ou diminution demandée par le Client.

La Banque attire l'attention du Client, qui se déclare pleinement informé et accepte les risques ainsi que leurs éventuelles conséquences financières, sur le fait que toute demande de modification en cours de projet est susceptible de générer des retards parfois significatifs par rapport aux plannings prévisionnels, qui sont produits à titre indicatif, le cas échéant.

6.5 Au cas où les informations fournies par le Client seraient fausses, incomplètes ou obsolètes, la Banque se réserve le droit, sans aucune indemnité et sans préavis, de suspendre ou de mettre fin à tout ou partie du Contrat, de supprimer tout ou partie de son site Internet ainsi que les données et les fichiers y figurant ou de supprimer l'accès au site internet, pages, fichiers et données, sans préjudice de toutes autres actions de droit commun qui pourraient être engagées par la Banque.

6.6 La Banque se réserve le droit de refuser, sans que cela ne puisse donner lieu au versement d'indemnités, l'accès à l'Option aux personnes communiquant lors de l'inscription des informations que la Banque jugerait incompatibles avec une bonne organisation et une bonne gestion de cette Option.

6.7 Dans l'hypothèse où la Banque se verrait enjoindre par une autorité administrative ou judiciaire compétente de retirer ou détruire de tels contenus, la Banque procèdera au retrait ou à la destruction ainsi ordonnée.

ARTICLE 7 : OBLIGATIONS DE LA BANQUE

7.1 La Banque assure directement, ou par l'intermédiaire de ses sous-traitants, les prestations relatives au Contrat, selon les normes en vigueur au moment de la signature de celui-ci. Elle garde l'entière maîtrise de ses choix en matière de moyens techniques et humains, pour assurer les Services E-transactions et sa sécurité ainsi que des lieux d'implantation du ou des centres techniques.

7.2 La Banque s'engage à :

(i) Mettre à disposition du Client la Plateforme E-transactions lui permettant d'accepter les opérations de paiement dans le système de paiement à distance avec le mode sécurisé SSL 128 (Secure Sockets Layer) ;

(ii) Configurer la Plateforme E-transactions pour permettre l'accès aux Fonctionnalités souscrites par le Client et permettre le traitement des transactions ;

(iii) Informer le Client sur les dispositifs de sécurité existants dans E-transactions et sur les évolutions mises en œuvre dans ce domaine ;

(iv) Fournir une assistance technique, accessible par téléphone et courrier électronique, liée à la fourniture et au fonctionnement de la Plateforme E-transactions.

ARTICLE 8 : CONDITIONS FINANCIERES

Les conditions financières sont détaillées dans les Conditions Particulières et/ou le barème tarifaire portant les principales Conditions Générales de Banque ou tout autre document convenu entre les Parties.

ARTICLE 9 : MODIFICATIONS

9.1 La Banque peut modifier à tout moment les conditions de fonctionnement de l'Option notamment les conditions financières dans les conditions et selon les modalités prévues à l'article 8 de la partie I des Conditions Générales du Contrat.

9.2 La Banque pourra également proposer un nouveau Schéma et/ou une nouvelle Marque et/ou un nouvel Instrument de paiement (tel que défini dans les présentes conditions. A cette fin, la Banque fera parvenir par tout moyen les conditions spécifiques et tarifaires afférentes au nouveau Schéma et/ou au nouvel Instrument de paiement et/ou à la nouvelle Marque proposée. Au terme d'un délai d'un (1) mois, sauf désaccord du Client signifié par tout moyen à la Banque, cette dernière rendra compatible pour l'acceptation du nouveau Schéma, du nouvel Instrument de paiement ou de la nouvelle Marque, le Système d'Acceptation dont elle est propriétaire.

ARTICLE 10 : INTERRUPTION / SUSPENSION

10.1 Pour préserver la sécurité et l'intégrité des échanges de données, notamment en cas d'actes ou de menaces d'actes de piratage, de malveillance ou de fraude, la Banque pourra suspendre l'exécution des Services E-transactions, sous réserve d'en informer le Client dès que possible et par tout moyen écrit.

10.2 Par ailleurs, la suspension et/ou la révocation de l'accès à la Plateforme E-transactions peut également intervenir notamment dans les cas suivants :

- le non-respect par le Client des procédures sécuritaires prévues dans le présent Contrat ;
- tout incident dans l'une ou l'autre des Fonctionnalités et/ou sur les comptes mouvementés ;
- la compromission d'un ou plusieurs outil(s) d'identification entendue comme la divulgation, la suspicion de divulgation ou de perte de l'outil conduisant à une possible perte d'intégrité et/ou de confidentialité des Services des Options.

10.3 La Banque, dès qu'elle est informée d'un tel événement, suspend immédiatement les Services E-transactions afin de procéder aux diligences requises et le cas échéant, peut résilier la présente Option dans les conditions prévues à l'article 11 ci-dessous.

10.4 Le Client doit informer immédiatement par écrit la Banque de tout événement susceptible d'entraîner la révocation de l'accès à la Plateforme E-transactions, au Logiciel E-transactions et aux outils de gestion.

10.5 Le Client est seul responsable des dommages causés aux tiers par une non révocation ou une révocation tardive du fait de la non dénonciation d'un événement susceptible d'entraîner la révocation de l'accès à la Plateforme E-transactions, au Logiciel E-transactions et aux outils de gestion. Le Client ne pourra en aucun cas mettre en jeu la responsabilité de la Banque du fait de cette suspension des Services E-transactions.

10.6 Dans l'hypothèse où la Banque viendrait à avoir connaissance de ce que le Client ne respecte pas les obligations légales et réglementaires auquel il peut être tenu en tant qu'éditeur de site internet, la Banque se réserve le droit de suspendre l'accès aux Services E-transactions.

10.7 Si, passé un délai de trente (30) jours calendaires à compter de la notification de la suspension, l'exécution des Services E-transactions est toujours suspendue, le présent Contrat pourra être résilié sans préavis par le Client moyennant l'envoi à la Banque d'un courrier en recommandé avec avis de réception.

ARTICLE 11 : DUREE ET RESILIATION DE L'OPTION

11.1 L'Option est conclue pour une durée indéterminée sauf dispositions contraires dans tout autre document signé par les Parties.

11.2 Le Client d'une part, la Banque d'autre part, peuvent, à tout moment, sans justificatif ni préavis (sauf dérogation particulière convenue entre les deux parties), sous réserve du dénouement des opérations en cours, mettre fin à l'Option, sans qu'il soit nécessaire d'accomplir aucune autre formalité que l'envoi d'une lettre recommandée avec demande d'avis de réception.

11.3 En cas de manquement aux obligations stipulées à l'article 6 des présentes conditions spécifiques, la Banque se réserve le droit, sans aucune indemnité et sans préavis, de suspendre ou de mettre fin à tout ou partie de l'Option, de supprimer tout ou partie de son site internet ainsi que les données et les fichiers y figurant ou de supprimer l'accès au site internet, pages, fichiers et données, sans préjudice de toutes autres actions de droit commun qui pourraient être engagées par la Banque.

11.4 La résiliation du contrat d'acceptation en paiement à distance sécurisé entraine la résiliation de l'Option « Services E-transactions » Cette résiliation de plein droit ne nécessitera aucune autre formalité qu'un simple courrier d'information au Client envoyé par tous moyens.

11.5 La Banque aura droit au paiement des travaux/services exécutés au titre de l'Option jusqu'au jour de la résiliation du Contrat ou de l'Option, sans préjudices des dommages intérêts auxquels elle pourrait prétendre le cas échéant.

ARTICLE 12 : CONVENTION DE PREUVE

Conformément aux dispositions du Code civil, les Parties entendent fixer, dans le cadre de la présente Option, les règles relatives aux preuves recevables entre elles en cas de litige. Les dispositions qui suivent constituent ainsi la convention de preuve passée entre les Parties, lesquelles s'engagent à respecter le présent article.

Les Parties s'engagent à accepter qu'en cas de litige les éléments d'identification utilisés dans le cadre de l'Option, les marques de temps établies de manière fiable et les documents électroniques échangés entre elles seront admissibles devant les tribunaux et feront preuve des données et des faits qu'ils contiennent ainsi que des manifestations de consentement et procédés d'authentification qu'ils expriment.

Dans le cadre de la relation entre les Parties, la preuve des connexions et d'autres éléments d'identification sera établie autant que de besoin à l'appui des journaux de connexion tenus à jour par les Parties.

La preuve contraire pourra être rapportée par tous moyens.

Les Parties font leur affaire personnelle de la conservation dans des conditions de sécurité appropriées et de l'archivage des traces informatiques en s'assurant de leur intégrité, de leur pérennité et de leur lisibilité.

Sous peine d'irrecevabilité, toute réclamation concernant la transmission d'un fichier ou la récupération des informations sur les plateformes des Services de la Banque doit être formulée par écrit dans un délai de deux mois à compter de la survenance de l'événement à l'origine de la demande.

Le Client reconnaît et accepte expressément qu'il ne pourra pas obtenir de la Banque une quelconque restitution desdites informations à l'expiration de ce délai. Les Parties s'interdisent de contester l'existence et l'exécution des opérations bancaires en cause passé ce délai.

ARTICLE 13 : PROPRIETE INTELLECTUELLE

13.1 Chacune des Parties reste propriétaire de l'ensemble de ses droits de propriété intellectuelle ou autres portant sur ses éléments préexistants à la conclusion de l'Option, comme par exemple les logiciels, interfaces, modules de communications outils, méthodes et documentations, logos, marques ou encore les signes distinctifs de chacune des Parties. Le Contrat ne transfère aucun de ces droits d'une Partie à l'autre.

13.2 De même, les idées, concepts, procédés, méthodes, savoir-faire ne font l'objet d'aucun transfert de propriété d'une Partie à l'autre.

13.3 En conséquence, le Client ne pourra désassembler, décompiler ou décrypter les éléments de propriété intellectuelle de la Banque et/ou de ses partenaires, et s'interdit d'utiliser notamment une méthode mécanique, électronique ou autre permettant de décompiler, désassembler ces éléments, que ce soit en tout ou partie, de pratiquer l'ingénierie inverse, de reconstituer la logique de ces éléments et de rendre, par tout autre manière ces éléments compréhensibles par l'homme, même aux fins d'interopérabilité, à moins que ces pratiques ne soient expressément autorisées par la loi.

13.4 L'Option et l'ensemble des éléments y figurant (informations, données, textes, sons, images, dessins, graphismes, signes distinctifs, logos, marques, etc.) sont la propriété exclusive de la Banque ou de ses fournisseurs ou sous-traitants qui lui ont concédé les droits nécessaires à la réalisation des présentes. L'ensemble de ces éléments est soumis aux dispositions du Code de la propriété intellectuelle et, à ce titre, est protégé contre toute utilisation non autorisée par la loi ou le présent Contrat.

13.5 La Banque concède, au Client une licence d'utilisation gratuite et non exclusive de l'Option strictement personnelle et incessible, pour la durée de la relation bancaire avec la Banque.

13.6 Toute autre reproduction, représentation ou diffusion, en tout ou partie, du contenu de l'Option, sur quelque support ou par tout procédé que ce soit, est interdite. Le non-respect de cette interdiction constitue une contrefaçon susceptible d'engager la responsabilité civile et pénale du contrefacteur.

13.7 Il est notamment strictement interdit d'utiliser ou de reproduire le nom « CREDIT AGRICOLE » et/ou son logo, seuls ou associés, à quelque titre que ce soit, et notamment à des fins publicitaires, sans l'accord préalable écrit de la Banque ou de Crédit Agricole SA.

13.8 Dans tous les cas, la Banque se réserve le droit d'interdire à tout moment l'utilisation de son nom, de sa marque, de son logo et de tout élément d'identification lorsque le Client ne respecte plus les conditions d'éligibilité, les déclarations et/ou les obligations prévues au Contrat.

Il est, en outre, précisé que :

(i) Les droits concédés au Client au titre des présents Services E-transactions s'entendent exclusivement d'un droit d'utilisation personnel, non exclusif et non transmissible du Logiciel E-transactions pour la durée de l'Option et sur la Plateforme E-transactions.

(ii) Le Client s'interdit de donner accès sous quelque forme que ce soit au Logiciel E-transactions ou de le mettre à disposition de quiconque, à l'exception de ses seuls employés (et prestataires soumis contractuellement à une obligation de confidentialité et de respect de la propriété intellectuelle au moins aussi contraignante que celle figurant aux présentes) identifiés et habilités à cette fin. Le Client n'est notamment pas autorisé à sous-licencier ou donner le Logiciel E-transactions en location.

(iii) Le Client peut utiliser le Logiciel E-transactions sur tout nouveau système informatique qui viendrait à se substituer à la configuration initiale.

(iv) Le Logiciel E-transactions et ses sauvegardes, soumis aux dispositions du Code de la propriété intellectuelle, sont et demeurent la propriété de la Banque.

(v) Le Client s'oblige à assurer la protection de la documentation du Logiciel E-transactions d'une façon adéquate au maintien des droits de la Banque et à prendre toute mesure appropriée vis-à-vis des personnes pouvant avoir accès au Logiciel E-transactions. Le Client s'engage à ne changer ni enlever aucune marque ou inscription figurant sur le Logiciel E-transactions et indiquant le nom du propriétaire.

(vi) La Banque autorise le Client à dupliquer partiellement ou en totalité la documentation, y apporter des modifications si nécessaires, et à la diffuser dans ses services, conformément au Code de la propriété intellectuelle.

(vii) La Banque se réserve les droits de propriété intellectuelle sur les éléments et livrables de toute nature réalisés et/ou fournis au Client dans le cadre du présent Contrat.

ARTICLE 14 : RECETTE

14.1 La Recette désigne le processus qui a pour objet de vérifier la conformité des Services E-

transactions et leurs paramétrages aux besoins du Client.

14.2 Ainsi, la Recette a pour objet de permettre au Client de vérifier que (i) les Services E-transactions sont fonctionnellement complets, et (ii) les Services E-transactions fonctionnent en parfaite conformité par rapport à ses besoins.

14.3 La Banque attire tout particulièrement l'attention du Client sur le fait que cette étape est fondamentale et qu'elle constitue une garantie de succès de la bonne exécution des Services E-transactions.

14.4 Le Client s'engage à réaliser des tests nécessaires sur les Services E-transactions en pré-production permettant de vérifier l'absence d'Anomalies et la conformité des Services E-transactions aux besoins du Client. Tant que ces vérifications n'auront pas été effectuées et que les tests feront ressortir des Anomalies, le Client ne doit pas passer au mode production.

14.5 Le passage des Services E-transactions en pré-production sur les Services E-transactions en production résulte du changement des adresses d'appel à la plateforme E-transactions. Le passage du service en pré-production sur le service en production résulte uniquement du processus technique qui est constitué de la mise à jour de la clé HMAC et des URL des pages du Site.

14.6 Cette opération vaut reconnaissance par le Client du fait que les Services E-transactions sont exempts d'Anomalie et sont conforme à ses besoins. Les Services E-transactions sont donc considérés comme mis en exploitation.

14.7 La Banque ne peut plus être tenue pour responsable de toute Anomalie ou non-conformité des Services E-transactions aux besoins du Client.

ARTICLE 15 : SOUS-TRAITANCE

15.1 La Banque assure certaines des prestations relatives à l'Option par l'intermédiaire de ses sous-traitants.

15.2 La Banque est responsable des prestations réalisées par ses sous-traitants. Elle garde l'entière maîtrise de ses choix en matière de moyens techniques et humains pour assurer les services liés à l'Option et leur sécurité, ainsi que des lieux d'implantation du ou des centres techniques.

ARTICLE 16 : GARANTIE ET RESPONSABILITE

16.1 Dispositions communes

16.1.1 Chacune des Parties assume l'entière responsabilité de ses actes et omissions pour l'ensemble des tâches qui lui incombent telles que visées aux présentes qui causeraient un dommage direct à son cocontractant. Elle est également responsable de ses préposés et de ses sous-traitants.

16.1.2 Aucune Partie ne sera tenue pour responsable vis-à-vis de l'autre de l'inexécution totale ou partielle de ses obligations ou des retards dans l'exécution du Contrat qui serait du fait de l'autre partie, de la survenance d'un cas de force majeure tel que détaillé à l'article 17 ci-après.

16.2 Responsabilité du Client

16.2.1 Le Client est seul et exclusivement responsable de l'utilisation des Services E-transactions qui doit notamment être conforme à la réglementation en vigueur et aux bonnes mœurs.

16.2.2 Le Client est seul responsable de la nature et de la qualité des informations fournies à la Banque : données, documents, fichiers et règles de traitement et des conséquences d'un manquement à son obligation d'information. Il est également seul responsable de l'usage qu'il fait des résultats que lui remet la Banque.

16.2.3 Le Client s'engage à ne pas modifier, essayer de modifier ou porter atteinte aux Services E-transactions sous quelque manière que ce soit et à ne pas utiliser de logiciel ou toute forme de programme informatique ayant pour but d'atteindre ou de rendre disponible un contenu protégé ou non disponible librement.

16.2.4 Le Client s'engage à informer la Banque sans délai, par tous moyens, de toute erreur, faute ou irrégularité qu'il constaterait dans l'utilisation des Services E-transactions, et ce, dès qu'il en aura connaissance.

16.2.5 Le Client s'engage à indemniser la Banque contre tout dommage subi par la Banque et contre toute action en responsabilité qui serait engagée à l'encontre de la Banque sur le fondement de la violation du présent Contrat et/ou d'un droit quelconque d'un tiers dont le Client serait responsable.

16.2.6 Enfin, du fait des limites des outils informatique et de l'Internet, que le Client déclare parfaitement connaître, la responsabilité de la Banque ne pourra en aucun cas être engagée, notamment en cas de difficulté d'accès au Logiciel E-transactions (qui est une solution informatique accessible en ligne à distance) ou au Site Internet, de contamination par malware, virus ou de destruction des données du Client, dont la protection incombe à ce dernier, d'intrusions malveillantes de tiers dans le Logiciel E-transactions ou le Site Internet, de détournements éventuels des Identifiants.

16.3 Responsabilité de la Banque

16.3.1 La Banque ne consent aucune garantie sur l'aptitude des Services E-transactions à répondre à des attentes ou besoins particuliers du Client.

16.3.2 De la même manière, la Banque n'est pas en mesure de garantir qu'aucune erreur ou autre trouble de fonctionnement ou d'utilisation n'apparaîtra au cours de l'utilisation du processus de Recette.

16.3.3 La Banque n'est pas responsable de l'indisponibilité des réseaux (logiciel ou matériel) qui ne sont pas entièrement sous son contrôle direct, ni de toute modification, suspension ou interruption de diffusion des Services E-transactions, ainsi que de la continuité, pérennité, conformité, compatibilité ou performance de ceux-ci ou à l'absence de bugs.

16.3.4 La Banque n'est pas responsable de l'utilisation qui sera faite des Instruments de Paiement que le Client aura souscrits et des éventuels litiges en découlant.

16.3.5 La Banque est tenue, s'agissant de la fourniture des Services E-transactions, par une obligation de moyens.

16.3.6 Au cas où la responsabilité de la Banque serait retenue, les Parties conviennent expressément que, toutes sommes confondues, la responsabilité de Banque sera limitée par sinistre et par an au montant de la facturation annuelle du Client au titre des Services E-transactions.

ARTICLE 17 : FORCE MAJEURE

17.1 Une Partie ne saurait être tenue responsable pour tout retard dans l'exécution de ses obligations ou pour toute inexécution de ses obligations résultant des conditions contractuelles régissant l'Option lorsque les circonstances y donnant lieu relèvent de la force majeure au sens du Code civil.

17.2 De façon expresse, sont considérés comme cas de force majeure ou cas fortuit les grèves totales ou partielles, lock-out, émeute, trouble civil, insurrection, guerre, intempérie, épidémie, blocage des moyens de transport ou d'approvisionnement pour quelque raison que ce soit, tremblement de terre, incendie, tempête, inondation, dégâts des eaux, restrictions gouvernementales ou légales, modifications légales ou réglementaires des formes de commercialisation, panne d'ordinateur, blocage des communications, y compris des réseaux de télécommunications filaires ou hertziens, toute remise en cause des fondements mathématiques régissant la théorie des algorithmes cryptographiques, utilisés pour les infrastructures à clé publique et tout autre cas indépendant de la volonté des parties empêchant l'exécution normale des conditions contractuelles régissant l'Option.

17.3 La Partie qui souhaite invoquer un cas de force majeure devra le notifier à l'autre Partie par tout moyen dans les meilleurs délais dès qu'elle aura connaissance d'un tel événement. Dans un premier temps, les cas de force majeure suspendront l'exécution des conditions contractuelles régissant l'Option. Dès lors que l'événement invoqué de force majeure a disparu, la Partie affectée en informera l'autre Partie sans délai et reprendra immédiatement l'exécution de son obligation. Si les cas de force majeure ont une durée supérieure à un (1) mois, l'Option pourra être résiliée automatiquement et de plein droit à l'initiative de la Partie la plus diligente par lettre recommandée avec avis de réception, sauf accord contraire entre les Parties.

ARTICLE 18: PRINCIPES DE SECURITE

18.1 Dispositifs de sécurité :

Le Client s'interdit de communiquer à quelque tiers que ce soit, et s'engage à protéger et conserver secrets, les mots de passe, identifiants, certificat ou tout autre dispositif de sécurité spécifique qui lui aurait été communiqué par la Banque dans le cadre de l'utilisation de l'Option.

18.2 Le Client est responsable de la garde, de la conservation et de la confidentialité desdits mots de passe, identifiants, certificats ou dispositifs de sécurité et, le cas échéant, des conséquences de leur divulgation ou de leur utilisation par des tiers.

18.3 Le Client s'engage à informer, sans délai, la Banque par lettre recommandée de toute atteinte à la confidentialité, perte, usage abusif ou anomalie constatée concernant ceux-ci.

18.4 Tout changement de ses mots de passe, identifiants, certificats et/ou dispositifs de sécurité est sous la responsabilité exclusive du Client.

ARTICLE 19: CESSION

19.1 La Banque se réserve la possibilité de céder, transférer ou apporter à un tiers, sous quelque forme que ce soit tout ou partie des droits et obligations des présentes, ou substituer un tiers pour l'exécution de tout ou partie des droits et obligations des présentes, ce que le Client accepte expressément par la présente clause. Par conséquent, le Client ne pourra s'opposer à toute cession ou transfert de tout ou partie des droits et obligations des présentes et s'engage à régulariser tout document y relatif.

19.2 La Banque, en aucun cas, ne restera tenue solidairement avec le cessionnaire des droits et obligations cédées ou transférées.

CONDITIONS SPECIFIQUES DE FONCTIONNEMENT DE L'OPTION D'ACCEPTATION EN PAIEMENT A DISTANCE PAR CARTES DE PAIEMENT HORS INTERNET

Les présentes conditions spécifiques de fonctionnement de l'Option d'acceptation en paiement à distance HORS INTERNET complètent la partie I des Conditions Générales du Contrat et s'appliquent toutes les fois où le paiement se fera à distance conformément à la définition ci-dessous « Paiement à distance ». La partie II des Conditions Générales s'applique en intégralité aux présentes conditions de fonctionnement.

La résiliation du Contrat d'acceptation en paiement à distance sécurisé par cartes de paiement entraine la résiliation de la présente Option de plein droit sans qu'aucune autre formalité qu'un simple courrier d'information au Client envoyé par tous moyens ne soit nécessaire.

ARTICLE 1 - DEFINITIONS

Les termes dotés d'une majuscule ont la signification qui leur est attribuée ci-dessous ou dans les Conditions Générales du Contrat ou dans les Conditions Particulières.

« **Equipement Electronique** » : désigne tout dispositif de paiement capable de lire une Carte (par exemple, un terminal de paiement électronique) équipée d'une puce au standard EMV ou d'une piste magnétique permettant l'authentification du titulaire de la Carte. L'Equipement Electronique est soit agréé, soit approuvé, par l'entité responsable du ou des Schéma(s) dont la ou les Marque(s) figure(nt) sur les Cartes acceptées sur cet Equipement.

L'agrément ou l'approbation de l'Equipement Electronique est une attestation de conformité avec des spécifications techniques et fonctionnelles définies par le(s) Schéma(s) concerné(s), qui dispose(nt) de la liste des Equipements Electroniques agréés ou approuvés.

« **Paiement à distance** » : désigne tout paiement par correspondance et assimilé notamment fax, email, courrier, téléphone, pour lequel l'opération de paiement est réalisée sur communication du numéro de la Carte, de sa date de fin de validité et de son Cryptogramme Visuel et, à chaque fois que cela est possible et/ou nécessaire, les nom et prénom du titulaire de la Carte.

ARTICLE 2 : OBLIGATIONS DU CLIENT

Le Client s'engage à :

2.1 Signaler au public de façon apparente chaque Marque qu'il accepte, notamment en apposant cette information sur ses supports de vente.

Pour la ou les Marques qu'il accepte, le Client doit accepter toutes les Cartes émises hors de l'EEE sur lesquelles figure(nt) cette(ces) Marque(s), quelle que soit la Catégorie de carte.

2.2 Afficher visiblement chaque Catégorie de carte qu'il accepte ou refuse en apposant cette information sur ses supports de vente.

2.3 Afficher visiblement le montant minimum éventuel à partir duquel la Carte est acceptée afin que le titulaire de la Carte en soit préalablement informé.

2.4 En cas de présence de plusieurs Marques sur la Carte, respecter la Marque choisie par le titulaire de la Carte pour initier l'ordre de paiement.

2.5 Respecter les lois et règlements (y compris en matière fiscale), les dispositions professionnelles ainsi que les bonnes pratiques applicables aux ventes et prestations réalisées à distance, et notamment aux échanges utilisant les réseaux et les différents terminaux de communication. A cet effet le Client organise la traçabilité adéquate des informations liées au paiement à distance.

2.6 S'abstenir de toute activité qui pourrait être pénalement sanctionnée, telle que la mise en péril de mineurs, des actes de pédophilie, des actes de contrefaçon d'œuvres protégées par un droit de propriété intellectuelle et/ou d'instruments de paiement, le non-respect de la protection des données personnelles, des atteintes aux systèmes de traitement automatisé de données, des actes de blanchiment, le non-respect des dispositions relatives aux jeux d'argent et de hasard, aux courses de chevaux, aux loteries et le non-respect des dispositions relatives aux conditions d'exercice de professions réglementées.

2.7 Garantir la Banque, et, le cas échéant, les Schémas, contre toute conséquence dommageable pouvant résulter pour eux du manquement aux obligations visées à l'article 2.6.

2.8 Afin que le titulaire de la Carte n'ait pas de difficulté à vérifier et identifier les opérations de paiement qu'il a effectuées, vérifier avec la Banque la conformité des informations transmises pour identifier son Point de vente.

Les informations doivent indiquer une dénomination commerciale ou sociale connue des titulaires de Carte et permettre de dissocier ce mode de paiement des autres modes de paiement (ex : automate, règlement en présence physique du titulaire de la Carte, règlement par Internet).

2.9 Accepter en contrepartie d'actes de vente et/ou de prestations de services offerts à sa clientèle et qu'il fournit ou réalise lui-même ou à titre de dons ou pour le règlement du montant de cotisations, les paiements à distance effectués avec les Cartes (Catégories de carte et Marques) qu'il a choisies d'accepter ou qu'il doit accepter.

2.10 Ne pas collecter au titre du présent Contrat une opération de paiement pour laquelle il n'a pas reçu lui-même le consentement exprès du titulaire de la Carte.

2.11 Utiliser obligatoirement un Equipement Electronique conforme aux spécifications du Schéma concerné et les procédures de sécurisation des ordres de paiement donnés à distance par les titulaires de Cartes proposées par la Banque.

2.12 Régler, conformément aux Conditions Particulières et/ou au barème tarifaire portant les principales Conditions Générales de Banque ou tout autre document convenu entre les Parties, les commissions, frais et, d'une manière générale, toute somme due au titre de l'acceptation des Cartes.

2.13 Faire son affaire personnelle des litiges liés à la relation sous-jacente qui existe entre lui et le titulaire de la Carte et de leurs conséquences financières.

2.14 A la demande de la Banque, selon les volumes d'opérations cartes acceptées, respecter les exigences du référentiel de sécurité PCI DSS figurant en annexe du présent Contrat.

Respecter les exigences du Référentiel Sécuritaire Accepteur annexé aux présentes ainsi que les exigences du Référentiel Sécuritaire PCI DSS annexé aux présentes et leurs mises à jour dont il peut prendre connaissance à l'adresse suivante : https://fr.pcisecuritystandards.org/minisite/env2/.

2.15 Respecter, pendant toute la durée du Contrat, les engagements pris à l'article « Eligibilité / Déclarations » de la partie I du Conditions Générales du Contrat.

2.16 Prévoir, dans ses relations contractuelles avec les tiers, tels que les prestataires de services techniques ou sous-traitants intervenant dans le traitement et le stockage des données de paiements sensibles liées à l'utilisation des Cartes, que ces derniers :

- s'engagent à respecter tant le Référentiel Sécuritaire PCI DSS que le Référentiel Sécuritaire Accepteur et leurs mises à jour et,

- acceptent que des audits soient réalisés dans leurs locaux et que les rapports puissent être communiqués, comme précisé à l'article 2.18 ci-dessous.

2.17 Permettre à la Banque et/ou au(x) Schéma(s) concerné(s) de faire procéder, dans les locaux du Client, aux frais de ce dernier, ou dans ceux des tiers visés à l'article 2.16 ci-dessus, à la vérification et au contrôle périodique par un tiers indépendant du fonctionnement des services de paiement hors Internet en fonction des risques de sécurité liés à l'Equipement Electronique utilisé. Cette vérification, appelée "procédure d'audit", s'inscrit dans le respect des procédures de contrôle et d'audit définies par le Schéma concerné

Le Client autorise la communication du rapport à la Banque et au(x) Schéma(s) concerné(s).

Au cas où le rapport remis aux Parties ou au Schéma concerné, par le tiers indépendant, à l'issue de la procédure d'audit révélerait un ou plusieurs manquements aux clauses du Contrat et/ou aux exigences du Référentiel Sécuritaire Accepteur et/ou du Référentiel Sécuritaire PCI DSS, la Banque pourra procéder, le cas échéant à la demande d'un Schéma, à une suspension de l'acceptation des Cartes par le Client dans les conditions de l'article « Suspension de l'acceptation », voire à une demande de résiliation du présent Contrat, dans les conditions prévues à l'article « durée et résiliation du contrat » de la Partie I des Conditions Générales du Contrat.

2.18 Informer immédiatement la Banque en cas de fonctionnement anormal de l'Equipement Electronique et/ou de toutes autres anomalies.

2.19 En cas de survenance d'un incident de sécurité majeur, notamment en cas de collecte et/ou d'utilisation frauduleuse des données, coopérer avec la Banque et les autorités compétentes le cas échéant. Le refus ou l'absence de coopération de la

part du Client pourra conduire la Banque à mettre fin au présent Contrat conformément à l'article « durée et résiliation du contrat » de la Partie I des Conditions Générales du Contrat.

ARTICLE 3 : OBLIGATIONS DE LA BANQUE

La Banque s'engage à :

3.1 Fournir au Client les informations le concernant directement sur le fonctionnement du/des Schéma(s) visé(s) dans la partie II des Conditions Générales du Contrat et son/leur évolution, les Catégories de cartes et les Marques dont il assure l'acceptation ainsi que les frais applicables à chacune des Catégories de cartes et Marques acceptées par lui, y compris les commissions d'interchange et les frais versés au(x) Schéma(s).

3.2 Respecter le choix de la Marque utilisée pour initier l'ordre de paiement conformément au choix du Client ou du titulaire de la Carte.

3.4 Indiquer au Client la liste et les caractéristiques des Cartes (Marques et Catégorie de Carte) pouvant être acceptées et lui fournir à sa demande le fichier des codes émetteurs (BIN).

3.5 Créditer le compte du Client des sommes qui lui sont dues, selon les modalités prévues dans les Conditions Particulières.

3.6 Ne pas débiter, au-delà du délai maximum de quinze (15) mois à partir de la date du crédit initial porté au compte du Client, les opérations non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.

3.7 Selon les modalités convenues avec le Client, communiquer au moins une fois par mois les informations suivantes :

- la référence lui permettant d'identifier l'opération de paiement,
- le montant de l'opération de paiement exprimé dans la devise dans laquelle son compte est crédité,
- le montant de tous les frais appliqués à l'opération de paiement et le montant de la commission de service acquittée par le Client et de la commission d'interchange.

Le Client peut demander à ce que les informations soient regroupées par Marque, Catégorie de carte et par taux de commission d'interchange applicable à l'opération.

3.8 Indiquer et facturer au Client les commissions de services à acquitter séparément pour chaque Catégorie de carte et chaque Marque selon les différents niveaux de commission d'interchange.

Le Client peut demander à ce que les commissions de services soient regroupées par Marque, Catégorie de carte et par taux de commission d'interchange applicable à l'opération.

ARTICLE 4 : GARANTIE DU PAIEMENT

Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées à l'article 5 ci-après sauf en cas :

- de réclamation du titulaire de la Carte qui conteste la réalité même ou le montant de l'opération de paiement et/ou,
- d'opération de paiement réalisée au moyen d'une Carte non valide, périmée ou bloquée.

A ce titre, le Client autorise expressément la Banque à débiter d'office son compte du montant de toute opération de paiement dont la réalité même ou le montant serait contesté par le titulaire de la Carte.

Toutes les mesures de sécurité sont indépendantes les unes des autres.

En cas de non-respect d'une seule de ces mesures, les opérations de paiement ne sont réglées que sous réserve de bonne fin d'encaissement, et ce en l'absence de contestations.

ARTICLE 5 : MESURES DE SECURITE

5.1 Lors du paiement, le Client s'engage à :

5.1.1 Effectuer tous les contrôles à partir des indications (numéro de Carte et date d'échéance) fournies par le client lors de la commande.

5.1.2 Contrôler la longueur (de 13 à 19 caractères) et la vraisemblance mathématique du numéro de la Carte au moyen de la méthode de calcul communiquée par la Banque. En cas de système de paiement interactif, bloquer la commande au bout de trois saisies erronées.

5.1.3 Vérifier l'acceptabilité de la Carte c'est-à-dire :

- la période de validité suivant l'indication fournie par le titulaire de la Carte (fin et éventuellement début),
- que la Marque (ou Catégorie de carte) utilisée est indiquée dans les Conditions Particulières et/ou figure dans la partie II des Conditions Générales du Contrat et/ou tout autre document ultérieur convenu entre les Parties.

5.1.4 Vérifier que le bon de commande est bien signé s'il s'agit d'une vente par correspondance.

5.1.5 Obtenir une autorisation d'un montant identique à l'opération.

5.2 Après le paiement, le Client s'engage à :

5.2.1 Transmettre à la Banque dans les délais et selon les modalités prévus dans les Conditions Particulières, les enregistrements électroniques des opérations et s'assurer que les opérations de paiement ont bien été portées au crédit du compte dans les délais et selon les modalités prévus dans les Conditions Particulières.

Le Client ne doit transmettre que les enregistrements électroniques des opérations pour lesquelles un ordre de paiement a été donné à son profit. Toute opération ayant fait l'objet d'une autorisation transmise par la Banque doit être obligatoirement remise à cette dernière.

5.2.2 Envoyer au titulaire de la Carte, à sa demande, un justificatif de l'opération de paiement.

5.2.3 Communiquer, à la demande de la Banque et dans les délais prévus dans les Conditions Particulières, tout justificatif des opérations de paiement.

5.2.4 Archiver et conserver, à titre de justificatif, pendant 15 mois, les bons ainsi que les relevés détaillés des commandes reçues des titulaires de Cartes.

5.2.5 Ne pas stocker sous quelque forme que ce soit le Cryptogramme visuel et / ou le numéro de la Carte de paiement.

5.2.6 Prendre toutes les précautions utiles pour que soient assurés la confidentialité et l'intégrité des données à caractère personnel du titulaire de la Carte qu'il est amené à recueillir à l'occasion de son activité et notamment lors de la réalisation d'une opération par Carte ainsi que le contrôle de l'accès à celles-ci et ce, conformément aux dispositions de la loi Informatique et Libertés.

5.2.7 Les mesures de sécurité énumérées ci-dessus pourront être modifiées et complétées pendant toute la durée du présent Contrat, selon la procédure prévue à l'article « Modifications » de la partie I des Conditions Générales du Contrat VADS.

ARTICLE 6 : PAIEMENT AVEC PREAUTORISATION

Le présent article s'applique lorsque le Client (i) utilise un Equipement Electronique muni de l'extension de service « Paiement avec Préautorisation » conforme aux spécifications en vigueur et, (ii) a choisi cette option dans les Conditions Particulières ou dans tout autre document convenu entre les Parties.

Lors d'une opération de paiement avec préautorisation, le titulaire d'une Carte donne son consentement à une opération de paiement en début de prestation pour un montant maximum convenu avec le Client et dont le montant définitif est déterminé à l'issue de la prestation.

Sauf disposition contraire prévue dans le présent article, l'ensemble des dispositions du présent Contrat sont applicables.

6.1 Au moment du consentement du titulaire de la Carte à l'opération de paiement, le Client s'engage cumulativement à :

- Recueillir l'acceptation du titulaire de la Carte d'être débité du montant final de la vente dont le montant maximal estimé lui est précisé.
- Ne pas faire usage de la Carte pour s'octroyer une caution ou un dépôt de garantie.
- Attribuer à l'occasion de l'initialisation de l'opération de paiement un numéro de dossier indépendant du numéro de carte.
- Obtenir systématiquement une autorisation pour le montant maximal estimé connu et accepté par le titulaire de la Carte.
- Fournir au titulaire de la Carte toutes les informations nécessaires lui permettant de raisonnablement déterminer le montant final de l'opération de paiement.

A défaut de respecter l'ensemble de ces engagements, l'opération ne sera pas garantie, même pour la fraction autorisée ou correspondant au montant du seuil de demande d'autorisation.

Une opération pour laquelle l'autorisation a été refusée par le serveur d'autorisation n'est jamais garantie.

6.2 Dans tous les cas où l'Equipement Electronique édite un ticket, mettre à disposition du titulaire de la Carte l'exemplaire qui lui est destiné sur lequel doit figurer notamment :

- le montant maximal estimé de la vente,
- le numéro de dossier,
- la mention de : "ticket provisoire" ou "préautorisation".

6.3 A l'exécution de l'opération de paiement, le Client s'engage à clôturer l'opération de paiement en recherchant via le numéro de dossier, l'opération de paiement initialisée lors du consentement et la finaliser pour le montant final de la vente connu et accepté par le titulaire de la Carte qui ne doit pas excéder la valeur du montant maximum autorisé par ce dernier.

Lorsqu'une opération de paiement avec préautorisation est réalisée, l'article 5.1.5 ci-dessus n'est pas applicable

ARTICLE 7 : DISPOSITIONS COMMUNES A LA PARTIE I DES CONDITIONS GENERALES DU CONTRATS

Trouvent à s'appliquer dans le cadre des présentes conditions de fonctionnement de l'Option d'acceptation en paiement à distance par cartes de paiement **hors Internet**, les dispositions suivantes de la partie I des Conditions Générales du Contrat :

Article 7 : Modalités annexes de fonctionnement

Article 8 : Modifications

Article 9 : Durée et Résiliation du Contrat

Article 10 : Suspension de l'acceptation

Article 11 : Mesures de prévention et de sanction prises par la Banque

Article 12 : Secret Bancaire et Protection des Données à Caractère Personnel

Article 13 : Référencement

Article 14 : Non renonciation

Article 15 : Titre – Permanence

Article 16 : Loi applicable et tribunaux compétents

Article 17 : Langue du Contrat

Article 18 : Domiciliation

Article 19 : Renseignement – Réclamation

Article 20 : Démarchage bancaire et financier

Article 21 : Lutte contre le blanchiment des capitaux, le financement du terrorisme, la corruption et la fraude – Respect des sanctions internationales.

ANNEXE 1 : REFERENTIEL SECURITAIRE ACCEPTEUR

Les exigences constituant le Référentiel Sécuritaire Accepteur sont présentées ci-après :

EXIGENCE 1 (E1) : GERER LA SECURITE DU SYSTEME COMMERCIAL ET D'ACCEPTATION AU SEIN DE L'ENTREPRISE

Pour assurer la sécurité des données des opérations de paiement et notamment, des données personnelles des titulaires de Cartes et des données de paiement sensibles liées à la Carte, une organisation, des procédures et des responsabilités doivent être établies.

En particulier, un responsable de la sécurité du système commercial et d'acceptation doit être désigné. Il est chargé, entre autres, d'appliquer la législation sur la protection des données à caractère personnel et du secret bancaire dans le cadre de leur utilisation et de leur environnement.

Les détenteurs de droits d'usage des informations et du système doivent être identifiés et sont responsables de l'attribution des droits d'accès au système.

Le contrôle du respect des exigences de sécurité relatives au système commercial et d'acceptation doit être assuré.

Une organisation chargée du traitement des incidents de sécurité, de leur suivi et de leur historisation doit être établie.

EXIGENCE 2 (E2) : GERER L'ACTIVITE HUMAINE ET INTERNE

Les obligations et les responsabilités du Personnel quant à l'utilisation des données bancaires et confidentielles, à leur stockage et à leur circulation en interne ou à l'extérieur doivent être établies. Il en est de même pour l'utilisation des postes de travail et du réseau interne comme du réseau Internet.

Les obligations et les responsabilités du Personnel quant à la protection des données bancaires et confidentielles doivent être établies. L'ensemble de ces règles doit s'appliquer à tous les personnels impliqués : salariés de l'entreprise et tiers.

Le Personnel doit être sensibilisé aux risques encourus, notamment sur la divulgation d'informations confidentielles, l'accès non autorisé aux informations, aux supports et aux documents.

Le Personnel doit être régulièrement sensibilisé aux risques particuliers liés à l'usage des moyens informatiques (postes de travail en réseau, serveurs, accès depuis ou vers Internet) et notamment, à l'introduction de virus.

Il convient que le Personnel reçoive une formation appropriée sur l'utilisation correcte du système d'exploitation et du système applicatif commercial et d'acceptation.

EXIGENCE 3 (E3) : GERER LES ACCES AUX LOCAUX ET AUX INFORMATIONS

Tout dispositif (équipement réseau, serveur, …) qui stocke ou qui traite des données relatives à une opération de paiement et notamment, des données de paiement sensibles liées à la Carte du titulaire de la Carte doit être hébergé dans un local sécurisé et répondre aux exigences édictées par les règles et recommandations de la CNIL.

Les petits matériels ou supports informatiques sensibles doivent être rendus inaccessibles à des tiers en période de non utilisation. Notamment, les cartouches de sauvegarde doivent être stockées dans un coffre.

Dans le cas où ces petits matériels ou supports informatiques sensibles ne sont plus opérationnels, ils doivent être obligatoirement détruits et la preuve de leur destruction doit être établie.

La politique d'accès aux locaux sensibles doit être formalisée et les procédures doivent être établies et contrôlées.

EXIGENCE 4 (E4) : ASSURER LA PROTECTION LOGIQUE DU SYSTEME COMMERCIAL ET D'ACCEPTATION

Les règles de sécurité relatives aux accès et sorties depuis et vers le système commercial et d'acceptation doivent être établies et leur respect doit être contrôlé.

Seul le serveur supportant l'application commerciale doit être accessible par les internautes.

Le serveur de base de données client ainsi que le serveur hébergeant le système d'acceptation ne doivent être accessibles que par le serveur commercial front-office et seulement par l'intermédiaire d'un pare-feu.

Les accès internes des utilisateurs comme des administrateurs à ces mêmes serveurs doivent se faire par l'intermédiaire du pare-feu.

L'architecture réseau doit être organisée de manière à ce que les règles de sécurité définies soient mises en œuvre et contrôlées.

Le pare-feu doit être mis à jour systématiquement lorsque des vulnérabilités sont identifiées sur ses logiciels (logiciel pare-feu et logiciel d'exploitation) et corrigeables.

Le serveur supportant le pare-feu doit être doté d'un outil de contrôle de l'intégrité.

Le pare-feu doit assurer l'enregistrement des accès et des tentatives d'accès dans un journal d'audit. Celui-ci doit être analysé quotidiennement.

EXIGENCE 5 (E5) : CONTROLER L'ACCES AU SYSTEME COMMERCIAL ET D'ACCEPTATION

Le principe d'autorisation d'utilisation du système doit être défini et reposer sur la notion d'accès des classes d'utilisateurs aux classes de ressources : définition des profils d'utilisateurs et des droits accordés.

Les responsabilités et rôles quant à l'attribution, l'utilisation et le contrôle doivent être identifiés. Notamment, les profils, les droits et les privilèges associés doivent être validés par les propriétaires des informations et du système commercial et d'acceptation.

Les droits des utilisateurs et des administrateurs ainsi que de leurs privilèges, doivent être gérés et mis à jour conformément à la politique de gestion des droits.

EXIGENCE 6 (E6) : GERER LES ACCES AUTORISES AU SYSTEME COMMERCIAL ET D'ACCEPTATION

Aucune ouverture de droits ne peut se faire en dehors des procédures d'autorisation adéquates. Les autorisations données doivent être archivées et contrôlées régulièrement.

Outre les accès clients, tout accès au système commercial et de paiement doit se faire sur la base d'une identification et d'une authentification.

L'identification doit être nominative y compris pour les administrateurs et les personnels de maintenance. Les droits accordés à ceux-ci doivent

être restreints aux opérations qui leur sont autorisées.

L'utilisation de codes d'identification attribués à des groupes ou des fonctions (process techniques comme l'alimentation automatique des signatures antivirales) n'est autorisée que si elle est appropriée au travail effectué.

Les changements de situation (changement de poste, départ, …) des personnels doivent systématiquement entraîner un contrôle des droits d'accès attribués.

La suppression des droits d'accès doit être immédiate en cas de départ d'une personne.

Le contrôle d'accès doit être assuré au niveau réseau par le pare-feu, au niveau système par les systèmes d'exploitation des machines accédées et au niveau applicatif par le logiciel applicatif et par le gestionnaire de base de données.

Les tentatives d'accès doivent être limitées en nombre.

Les mots de passe doivent être changés régulièrement.

Les mots de passe doivent comporter au minimum 8 caractères dont des caractères spéciaux.

EXIGENCE 7 (E7) : SURVEILLER LES ACCES AU SYSTEME COMMERCIAL ET D'ACCEPTATION

Les accès et tentatives d'accès au système doivent être enregistrés dans des journaux d'audit.

L'enregistrement doit comporter au minimum la date et l'heure de l'accès (ou tentative) et l'identification de l'acteur et de la machine.

Les opérations privilégiées comme la modification des configurations, la modification des règles de sécurité, l'utilisation d'un compte administrateur doivent également être enregistrées.

Les systèmes assurant l'enregistrement doivent au minimum avoir la fonction de pare-feu pour le système supportant la base de données Clients ainsi que celui supportant la base de données Paiements.

Les journaux d'audit doivent être protégés contre des risques de désactivation, modification ou suppression non autorisées.

Les responsabilités et rôles quant à l'audit des données enregistrées sont identifiés. Celui-ci doit être effectué quotidiennement.

EXIGENCE 8 (E8) : CONTROLER L'INTRODUCTION DE LOGICIELS PERNICIEUX

Les procédures et les responsabilités de gestion ayant trait à la protection anti-virus et à la restauration des données et des logiciels en cas d'attaque par virus doivent être définies et formalisées.

L'installation et la mise à jour régulière des logiciels de détection et d'élimination des virus doivent être effectuées sur la totalité des machines ayant accès au système commercial et d'acceptation.

La vérification anti-virus doit être exécutée quotidiennement sur la totalité des machines.

EXIGENCE 9 (E9) : APPLIQUER LES CORRECTIFS DE SECURITE (PATCHES DE SECURITE) SUR LES LOGICIELS D'EXPLOITATION

Les correctifs de sécurité doivent être systématiquement appliqués sur les équipements de sécurité et les serveurs applicatifs frontaux pour fixer le code lorsque des vulnérabilités pourraient permettre des accès non autorisés et non visibles.

Ces correctifs doivent être appliqués sur la base d'une procédure formelle et contrôlée.

EXIGENCE 10 (E10) : GERER LES CHANGEMENTS DE VERSION DES LOGICIELS D'EXPLOITATION

Une procédure d'installation d'une nouvelle version doit être établie et contrôlée.

Cette procédure doit prévoir entre autres, des tests de non régression du système et un retour arrière en cas de dysfonctionnement.

EXIGENCE 11 (E11) : MAINTENIR L'INTEGRITE DES LOGICIELS APPLICATIFS RELATIFS AU SYSTEME COMMERCIAL ET D'ACCEPTATION

Il convient d'établir les responsabilités et les procédures concernant les modifications opérationnelles touchant aux applications.

Les modifications apportées aux logiciels applicatifs doivent faire l'objet d'une définition précise.

La demande de modification doit être approuvée par le responsable fonctionnel du système.

Les nouvelles versions de logiciels applicatifs doivent être systématiquement soumises à recette et approuvées par le responsable fonctionnel de l'application concernée avant toute mise en production.

EXIGENCE 12 (E12) : ASSURER LA TRAÇABILITE DES OPERATIONS TECHNIQUES (ADMINISTRATION ET MAINTENANCE)

Les opérations techniques effectuées doivent être enregistrées de manière chronologique, dans un cahier de bord pour permettre la reconstruction, la revue et l'analyse en temps voulu des séquences de traitement et des autres activités liées à ces opérations.

EXIGENCE 13 (E13) : MAINTENIR L'INTEGRITE DES INFORMATIONS RELATIVES AU SYSTEME COMMERCIAL ET D'ACCEPTATION

La protection et l'intégrité des éléments de l'opération de paiement doivent être assurées ainsi lors de leur stockage et lors de leur routage sur les réseaux (internes ou externes). Il en est de même pour les éléments secrets servant à chiffrer ces éléments.

Le dossier de sécurité propre au système commercial et d'acceptation doit décrire les moyens mis en place pour répondre à cette exigence.

EXIGENCE 14 (E14) : PROTEGER LA CONFIDENTIALITE DES DONNEES BANCAIRES

Les données de paiement sensibles liées à la Carte du Titulaire de la Carte ne peuvent être utilisées que pour exécuter l'ordre de paiement et pour traiter les réclamations. Le cryptogramme visuel d'un Titulaire de Carte ne doit en aucun cas être stocké par l'Accepteur CB.

Les données bancaires et à caractère personnel relatives à une opération de paiement, et notamment les données de paiement sensibles liées à la Carte du Titulaire de la Carte doivent être protégées lors de leur stockage et lors de leur routage sur les réseaux internes et externes au site d'hébergement conformément aux dispositions de la loi Informatique et Libertés et aux recommandations de la CNIL. Il en est de même pour l'authentifiant de l'Accepteur CB et les éléments secrets servant à chiffrer.

Le dossier de sécurité propre au système commercial et d'acceptation doit décrire les moyens mis en place pour répondre à cette exigence.

EXIGENCE 15 (E15) : PROTEGER LA CONFIDENTIALITE DES IDENTIFIANTS - AUTHENTIFIANTS DES UTILISATEURS ET ADMINISTRATEURS

La confidentialité des identifiants - authentifiants doit être protégée lors de leur stockage et de leur circulation.

Il convient de s'assurer que les données d'authentification des administrateurs ne puissent être réutilisées.

Dans le cadre d'une intervention extérieure pour maintenance, les mots de passe utilisés doivent être systématiquement changés à la suite de l'intervention.

ANNEXE 2 : REFERENTIEL SECURITAIRE PCI-DSS

Les exigences constituant le Référentiel Sécuritaire PCI-DSS sont organisées autour d'un ensemble de douze (12) familles d'exigences regroupant deux cent cinquante (250) règles réparties en six (6) grands domaines présentés ci-après :

1° *Mettre en place et gérer un réseau sécurisé*

1ère exigence	Installer et gérer une configuration de pare-feu afin de protéger les données des titulaires des Cartes
2ème exigence	Ne pas utiliser les paramètres par défaut du fournisseur pour les mots de passe et les autres paramètres de sécurité du système

2° *Protéger les données des titulaires de Cartes*

3ème exigence	Protéger les données des titulaires de Cartes stockées
4ème exigence	Crypter la transmission des données des titulaires de Cartes sur les réseaux publics ouverts

3° *Disposer d'un programme de gestion de la vulnérabilité*

5ème exigence	Utiliser et mettre à jour régulièrement un logiciel antivirus
6ème exigence	Développer et gérer des applications et systèmes sécurisés

4° *Mettre en œuvre des mesures de contrôle d'accès efficaces*

7ème exigence	Limiter l'accès aux données des titulaires de Cartes aux cas de nécessité professionnelle absolue
8ème exigence	Attribuer une identité d'utilisateur unique à chaque personne disposant d'un accès informatique
9ème exigence	Limiter l'accès physique aux données des titulaires de Cartes

5° *Surveiller et tester régulièrement les réseaux*

10ème exigence	Suivre et surveiller tous les accès aux ressources du réseau et aux données des titulaires de Cartes
11ème exigence	Tester régulièrement les systèmes et procédures de sécurité

6° *Disposer d'une politique en matière de sécurité de l'information*

12ème exigence	Disposer d'une politique régissant la sécurité de l'information

L'intégralité des exigences du Référentiel Sécuritaire PCI-DSS, ainsi que leurs mises à jour sont disponibles à l'adresse internet suivante : http//fr.pcisecuritystandards.org/minisite/en/