TOULOUSE 31
La banque proche & connectée

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, 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 :

1. crédit ou carte de crédit,
2. débit,
3. prépayé,
4. commercial,

ou l'équivalent dans une langue étrangère.

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

5. crédit ou carte de crédit,
6. carte de débit,
7. carte prépayée,
8. 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.

« **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:

9. 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;
10. 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;
11. 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 :

1. 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 ;

2. 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 ;
3. 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 ;
4. s'engager à signaler sans délai à la Banque toute modification relative à son activité (nature des biens et des services proposés) ;
5. 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 ;
6. 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 effectuées, vérifier avec la Banque la conformité des informations transmises pour identifier son Point de vente.

Les informations doivent indiquer une dénomination commerciale 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 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 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.

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 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 :

7. la référence lui permettant d'identifier l'opération de paiement,
8. le montant de l'opération de paiement exprimé dans la devise dans laquelle son compte est crédité,
9. 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 :

10. la période de validité (fin et éventuellement début),
11. 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 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.

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 : modalités annexes de fonctionnement

7.1 <u>Réclamation</u>

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 <u>Convention de preuve</u>

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 <u>Transaction crédit</u>

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 :

12. 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.
13. des modifications sécuritaires telles que :
    1. la suppression de l'acceptabilité de certaines Cartes,
    2. 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 : Durée et Résiliation 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.

10.2 La suspension peut être décidée en raison notamment :

14. 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),
15. d'une participation à des activités frauduleuses, notamment d'une utilisation anormale de Cartes perdu(e)s, volé(e)s ou contrefait(e)s,
16. 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,
17. 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,
18. de retard volontaire ou non motivé de transmission des justificatifs,
19. d'un risque aggravé en raison des activités du Client,
20. 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 prévention 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 Données à Caractère 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 <u>Secret bancaire</u>

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 <u>Protection des données à caractère personnel du Client</u>

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 <u>Protection des données à caractère personnel des titulaires de Cartes</u>

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 dispositif de sécurité) 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 :

1. 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 ;
2. mutuellement de tout incident de sécurité qui aurait pour conséquence une violation des données traitées dans le cadre du Contrat ;
3. 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 : Référencement

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 et répondre à ses éventuelles réclamations.
Dans ce dernier cas, le Client a aussi la possibilité, en écrivant à l'adresse de la Banque, de faire appel au Service Clients qui s'efforcera de trouver la meilleure solution à son différend.

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.

1. 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 :

1. VISA Inc. et VISA Europe
2. Mastercard Europe SA

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

1. Pour VISA Inc. et VISA Europe : Visa, V PAY, Visa Electron
2. Pour Mastercard Europe SA : Mastercard, Maestro.

Article 2 - Dispositions spécifiques aUx SCHEMAs visa et Mastercard

2.1 Obligations de la Banque

Par dérogation à l'article 4.6 de la partie I Conditions Générales, le Client 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.

3. 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 le Client 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 :

4. Les cartes sur lesquelles figure la Marque CB,
5. 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 :

6. à accepter les Cartes CB pour le paiement d'achats de biens ou de prestations de services offerts à sa clientèle et réellement effectués (à l'exclusion de toute délivrance d'espèces ou de tout titre convertible en espèces pour leur valeur faciale), 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.
7. 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.
8. 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 1.6 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.

6. 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 :

9. 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 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.
10. 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.

7. 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

8. 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.

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 donner 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 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 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 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.

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 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 donner 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 :

11. la référence lui permettant d'identifier l'opération de paiement,
12. le montant de l'opération de paiement exprimé dans la devise dans laquelle son compte est crédité,
13. 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 :

14. de réclamation du titulaire de la Carte qui conteste la réalité même ou le montant de l'opération de paiement et/ou,
15. 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 :

16. la période de validité suivant l'indication fournie par le titulaire de la Carte (fin et éventuellement début),
17. 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 :

18. 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.
19. Ne pas faire usage de la Carte pour s'octroyer une caution ou un dépôt de garantie.
20. Attribuer à l'occasion de l'initialisation de l'opération de paiement un numéro de dossier indépendant du numéro de carte.
21. Obtenir systématiquement une autorisation pour le montant maximal estimé connu et accepté par le titulaire de la Carte.
22. 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 :

23. le montant maximal estimé de la vente,
24. le numéro de dossier,
25. 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.

Articles 7 : dispositions communes à la Partie I des Conditions générales 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 des titulaires de Cartes, 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 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 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 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/