PARTIE 1

CONDITIONS GENERALES COMMUNES A TOUS LES SCHEMAS

ARTICLE 1 - DEFINITIONS

1) L'"Accepteur" peut être tout commerçant, tout prestataire de services, toute personne exerçant une profession libérale, et d'une manière générale, tout professionnel vendant ou louant des biens ou des prestations de services, ou toute entité habilitée à recevoir des dons ou percevoir des cotisations susceptible d'utiliser un Système d'Acceptation reconnu par le(s) Schéma(s) dûment convenu(s) avec la Banque.

L'Accepteur dispose de toute liberté pour domicilier ses remises à l'encaissement auprès de l'établissement de crédit ou de paiement de son choix, membre du Schéma, et avec lequel il a passé un contrat pour ce faire.

L'Accepteur déclare disposer de toutes les informations déterminantes pour son consentement et que toutes ses demandes d'informations afférentes, notamment aux stipulations du présent Contrat et à la qualité des Parties, ont été satisfaites par la Banque.

2) Par "Marque", il faut entendre tout nom, terme, sigle, symbole matériel ou numérique ou la combinaison de ces éléments susceptible de désigner le Schéma.

Les Marques pouvant être acceptées entrant dans le champ d'application du présent Contrat sont CB, Visa et MasterCard.

3) Par "Banque", il faut entendre l'établissement de crédit habilité à organiser l'acceptation des Cartes portant la(les) Marque(s) du(des) Schéma(s) visé(s) en partie 2 du présent Contrat.

4) Par "Système d'Acceptation", il faut entendre les logiciels, protocoles et équipements conformes aux spécifications définies par chaque Schéma et nécessaires à l'enregistrement, à la transmission et au traitement sécurisé des ordres de paiement par Cartes portant l'une des Marques dudit Schéma. L'Accepteur 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.

5) Par "Règlement", il faut entendre le Règlement UE n°2015/751 du 29 avril 2015.

6) Par "Catégorie de carte", on entend les catégories de Carte suivantes:
- crédit ou carte de crédit,
- carte de débit,
- carte prépayée
- carte commerciale.

7) Par "Carte", on entend un instrument de paiement qui permet au payeur d'initier une opération de paiement. Elle porte une ou plusieurs Marques.

Lorsque la Carte 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), elle porte au moins l'une des mentions suivantes:
- crédit ou carte de crédit
- débit,
- prépayé,
- commercial,

ou l'équivalent dans une langue étrangère.

8) Par "Schéma", il faut entendre un ensemble de règles régissant l'exécution d'opérations de paiement liées à une carte tel que défini à l'article 2 du Règlement.

Les Schémas CB, Visa et MasterCard reposent sur l'utilisation de Cartes CB, Visa et MasterCard auprès des Accepteurs acceptant les Marques desdits Schémas, et cela dans le cadre des seules dispositions et procédures définies ou homologuées par lesdits Schémas.

9) Par "Contrat ", il faut entendre ensemble les Conditions Générales communes à tous les Schémas (partie 1), les dispositions spécifiques à chaque Schéma (partie 2) et les conditions particulières convenues entre les Parties (ci-après les "Conditions Particulières").

10) Par "Paiement à distance", il faut entendre 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.

11) Par "Paiements récurrents et/ou échelonnés" (ci-après les « Paiements Récurrents »), il faut entendre plusieurs opérations de paiement successives et distinctes (série d'opérations) ayant des montants et des dates déterminées ou déterminables et/ou à des échéances convenues entre l'Accepteur et le titulaire de la Carte.

12) Par "Parties", il faut entendre la Banque et l'Accepteur.

ARTICLE 2 - OBLIGATIONS DE L'ACCEPTEUR

L'Accepteur s'engage à:

2.1 Signaler au public de façon apparente sur les supports de vente chaque Marque qu'il accepte et chaque Catégorie de carte qu'il accepte ou refuse, et le montant minimum à partir duquel la Carte est acceptée.

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

2.2 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.

2.3 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 (notamment télévision et téléphonie). A cet effet l'Accepteur organise la traçabilité adéquate des informations liées au paiement à distance.

2.4 Utiliser le Système d'Acceptation en s'abstenant 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 de moyens ou instruments de paiement, le non-respect de la protection des données à caractère personnel, des atteintes aux systèmes de traitement automatisé desdites 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 des dispositions relatives aux conditions d'exercice de professions réglementées.

2.5 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 2.4 ci-dessus.

2.6 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 en ligne. Les informations doivent indiquer une dénomination commerciale connue du titulaire de la Carte et permettre de dissocier ce mode de paiement par rapport aux autres modes de paiement (automate, règlement en présence physique du titulaire de la Carte, etc.).

2.7 Accepter les Paiements à distance sécurisés effectués avec les Cartes portant la(les) Marque(s) et Catégorie(s) de carte qu'il a choisi d'accepter ou qu'il doit accepter des Schémas en contrepartie d'actes de vente ou de prestations de services offerts à sa clientèle et qu'il fournit ou réalise lui-même, ou à titre de dons ou pour règlement du montant de cotisations.

2.8 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.

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

2.10 Régler, selon les Conditions Particulières convenues avec la Banque, les commissions, frais et d'une manière générale toute somme due au titre de l'acceptation des Cartes.

2.11 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 Accepteur annexé au présent Contrat que le Référentiel Sécuritaire PCI/DSS, acceptent que les audits visés à l'article 2.12 ci-dessous soient réalisés dans leurs locaux et que les rapports puissent être communiqués comme précisé audit article.

2.12 Permettre à la Banque de faire procéder, aux frais de l'Accepteur dans les locaux de l'Accepteur ou dans ceux des tiers visés à l'article 2.11 ci-dessus, à la vérification par un tiers indépendant du respect tant des clauses du présent Contrat que des exigences du Référentiel Sécuritaire Accepteur annexé au présent Contrat et/ou de celles 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.

L'Accepteur autorise la communication du rapport à la Banque et aux Schémas concernés.

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 Schéma peut procéder à une suspension de l'acceptation des Cartes portant ses Marques par l'Accepteur, voire à une demande de résiliation du présent Contrat telle que prévue à l'article 8 de la présente partie 1.

2.13 L'Accepteur doit respecter les exigences du Référentiel Sécuritaire Accepteur annexé au présent Contrat et celles du Référentiel Sécuritaire PCI/DSS dont il peut prendre connaissance à l'adresse suivante:
https://fr.pcisecuritystandards.org/minisite/en/
ou qui lui sera communiqué par la Banque à première demande.

2.14 Dans le cas où il propose des Paiements Récurrents, l'Accepteur s'engage à :
- respecter les règles relatives au stockage des données à caractère personnel ou liées à l'utilisation de la Carte définies par la délibération de la CNIL n°2013-358 du 14 novembre 2013,
- s'assurer que le titulaire de la Carte a consenti à ce que les données liées à sa Carte soient utilisées pour effectuer des Paiements Récurrents et, à ce titre, recueillir du titulaire de la Carte les autorisations et/ou mandats nécessaires à l'exécution des Paiements Récurrents et en conserver la preuve pendant 15 (quinze) mois à compter de la date du dernier paiement,
- donner une information claire au titulaire de la Carte sur les droits dont il dispose et notamment sur la possibilité de retirer à tout moment son consentement,
- ne plus initier de paiements dès lors que le titulaire de la Carte a retiré son consentement à l'exécution de la série d'opérations de paiement considérée

2.15 Faire son affaire personnelle des litiges liés à la relation sous-jacente qui existe entre lui et le titulaire de la Carte (litige commercial par exemple), et de leurs conséquences financières.

2.16 En cas de survenance d'un incident de sécurité majeur, notamment en cas de collecte/utilisation frauduleuse des données, coopérer avec la Banque et, le cas échéant, avec les autorités compétentes. Le refus ou l'absence de coopération de la part de l'Accepteur pourra conduire la Banque à résilier le présent Contrat conformément à l'article 8 de la présente partie 1.

2.17 En cas de manquement de l'Accepteur aux dispositions du présent Contrat concernant les mesures de sécurité ou en cas de taux d'impayés constaté anormalement élevé ou d'utilisation anormalement élevée de Cartes volées, perdues ou contrefaites ayant entraîné , le cas échéant, l'application de pénalités par les Schémas à la Banque, indemniser la Banque du montant desdites pénalités versées par la Banque aux Schémas.

ARTICLE 3 - OBLIGATIONS DE LA BANQUE

La Banque s'engage à :

3.1 Fournir à l'Accepteur les informations le concernant directement sur le fonctionnement du(des) Schéma(s) visé(s) dans la partie 2 et son/leur évolution, les Catégories de carte et les Marques dont il assure l'acceptation ainsi que les frais applicables à chacune des Catégories de carte 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 de l'Accepteur ou du titulaire de la Carte.

3.3 Mettre à la disposition de l'Accepteur, selon les modalités convenues aux Conditions Particulières, les informations relatives à la sécurité des opérations de paiement, notamment l'accès au serveur d'autorisation.

3.4 Indiquer à l'Accepteur la liste et les caractéristiques des Cartes (Marques et Catégories de carte) pouvant être acceptées et lui fournir, à sa demande, le fichier des codes émetteurs (BIN).

3.5 Inscrire l'Accepteur dans la liste des accepteurs habilités à recevoir des paiements à distance sécurisés par Cartes.

3.6 Créditer le compte de l'Accepteur des sommes qui lui sont dues selon les modalités convenues aux Conditions Particulières.

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

3.8 Selon les modalités convenues avec l'Accepteur, 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 l'Accepteur et de la commission d'interchange.

L'Accepteur peut demander à ce que ces informations soient regroupées par Marque, application de paiement, Catégorie de carte et par taux de commission d'interchange applicable à l'opération.

3.9 Indiquer et facturer à l'Accepteur les commissions de services à acquitter séparément pour chaque Catégorie de carte et chaque Marque selon les différents niveaux de commission d'interchange.

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

ARTICLE 4 - GARANTIE DE PAIEMENT

4.1 Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées tant à l'article 5 de la présente partie 1 qu'en partie 2, ainsi qu'aux Conditions Particulières.

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

4.3 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.

ARTICLE 5 - MESURES DE SECURITE

5.1 **Lors du paiement**

L'Accepteur s'engage à :

5.1.1 Appliquer la procédure de sécurisation des ordres de paiement dont il peut obtenir les modalités d'application auprès de la Banque.

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

5.1.3 Vérifier l'acceptabilité de la Carte, c'est-à-dire:
- la période de validité (fin et éventuellement début),
- que la Marque utilisée est indiquée dans les Conditions Particulières ou figure à l'article 1 de la présente partie 1.

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

5.1.5 La garantie de paiement n'est pas acquise :

a) en cas d'opération de paiement donnée au moyen d'une Carte non éligible aux procédures de sécurisation des ordres de paiement visées aux présentes par décision des Schémas,

b) en cas de livraison de bien ou de prestation de service réalisée au-delà de 7 (sept) jours calendaires à compter de la date de l'opération de paiement, la nouvelle autorisation devant être recueillie par l'Accepteur étant alors obtenue sans mise en oeuvre des procédures de sécurisation des ordres de paiement visées aux présentes,

c) en cas d'opération de paiement initiée par l'Accepteur lui-même en utilisant les données de la Carte précédemment obtenues du titulaire notamment par téléphone, télécopie, courriel ou courrier,

d) en cas d'opération de paiement réalisée durant une période d'indisponibilité du dispositif de sécurisation des ordres de paiement,

e) en cas de fractionnement de l'opération de paiement par l'Accepteur,

f) au cas où l'Accepteur renonce à l'utilisation des procédures de sécurisation des ordres de paiement.

Dans le cas où l'Accepteur proposerait le paiement par Carte pour règlement d'un abonnement, il est expressément stipulé qu'aucune opération de paiement n'est réalisée avec le dispositif de sécurisation des ordres de paiement donnés à distance et ne bénéficie de la garantie de paiement.

Avant toute livraison de bien ou prestation de service, la Banque conseille vivement à l'Accepteur de s'assurer, auprès du prestataire de services de paiement choisi par l'Accepteur pour gérer sa solution de paiement à distance, que tout ou partie des opérations de paiement n'est pas concernée par les cas visés aux paragraphes a) ou d) du présent article.

5.2 **Après le paiement**

L'Accepteur 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.

L'Accepteur ne doit transmettre que les enregistrements électroniques pour lesquels 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 précisant, entre autres, le mode de paiement utilisé.

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 L'Accepteur s'engage à ne stocker, sous quelque forme que ce soit, le cryptogramme visuel.

Les mesures de sécurité énumérées à l'article 5 ci-dessus pourront être modifiées et complétées pendant toute la durée du présent Contrat, selon la procédure prévue à l'article 7 de la présente partie 1.

ARTICLE 6 - MODALITES ANNEXES DE FONCTIONNEMENT

6.1 Réclamation

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

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

6.2 Convention de preuve

De convention expresse entre les Parties, les enregistrements électroniques constituent la preuve des opérations de paiement remises à l'Acquéreur.

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 l'Accepteur, à moins que ce dernier ne démontre l'absence de fiabilité ou d'authenticité des enregistrements produits par la banque ou le Schéma.

6.3 « Transaction crédit »

Le remboursement partiel ou total d'un achat d'un bien ou d'un service, d'un don ou d'une cotisation réglé(e) par Carte doit, avec l'accord de son titulaire, être effectué au titulaire de la Carte utilisée pour l'opération initiale.

L'Accepteur doit alors utiliser la procédure dite de « transaction crédit » et, dans le délai prévu dans les conditions convenues avec elle, 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 7 - MODIFICATIONS

7.1 La Banque peut modifier à tout moment les présentes Conditions Générales, les conditions spécifiques ainsi que les Conditions Particulières.

7.2 La Banque peut notamment apporter:

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

7.3 Les nouvelles conditions entrent généralement en vigueur au terme d'un délai minimum fixé à 1 (un) mois à compter de la notification sur support papier ou sur tout autre support durable.

7.4 Ce délai est exceptionnellement réduit à 5 (cinq) jours calendaires lorsque la Banque ou le Schéma concerné constate, dans le Point d'acceptation, une utilisation anormale de Cartes perdues, volées ou contrefaites.

7.5 Passés les délais visés au présent article, les modifications sont réputées acceptées par l'Accepteur s'il n'a pas résilié le présent Contrat. Elles lui sont dès lors opposables.

7.6 Le non-respect des nouvelles conditions techniques ou sécuritaires, dans les délais impartis, peut entraîner la résiliation du présent Contrat.

ARTICLE 8 - DUREE ET RESILIATION DU CONTRAT

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

L'Accepteur 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, 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. L'Accepteur 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 7 ci-dessus, elle ne peut intervenir qu'au-delà du délai prévu dans cet article pour l'entrée en vigueur de ces modifications.

8.2 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 9.2 ci-dessous.

Elle est notifiée par lettre recommandée avec demande d'avis de réception et doit être motivée. Son effet est immédiat.

8.3 Toute cessation d'activité de l'Accepteur, 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.

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

8.4 L'Accepteur 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, l'Accepteur s'engage à retirer immédiatement de ses supports de communication tout signe d'acceptation des Cartes ou Marques des Schémas concernés.

ARTICLE 9 - SUSPENSION DE L'ACCEPTATION

9.1 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 des Cartes portant certaines Marques par l'Accepteur. La suspension est précédée, le cas échéant, d'un avertissement à l'Accepteur, 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.

Elle peut également intervenir à l'issue d'une procédure d'audit telle que visée à l'article 2.12 de la présente partie 1, au cas où le rapport révélerait un ou plusieurs manquements tant aux clauses du présent Contrat qu'aux exigences du Référentiel Sécuritaire Accepteur annexé au présent Contrat et/ou du Référentiel Sécuritaire PCI/DSS.

9.2 La suspension peut être décidée en raison notamment:

- 9.2.1 du non-respect répété des obligations du présent Contrat et du refus d'y remédier, ou d'un risque de dysfonctionnement important du Système d'Acceptation du Schéma,
- 9.2.2 d'une participation à des activités frauduleuses, notamment d'une utilisation anormale de Cartes perdues, volées ou contrefaites,
- 9.2.3 d'un refus d'acceptation répété et non motivé des Cartes et/ou des Catégories de carte du Schéma qu'il a choisi d'accepter ou qu'il doit accepter,
- 9.2.4 de plaintes répétées d'autres membres ou partenaires d'un Schéma et qui n'ont pu être résolues dans un délai raisonnable,
- 9.2.5 de retard volontaire ou non motivé de transmission des justificatifs,
- 9.2.6 d'un risque aggravé en raison des activités de l'Accepteur.

9.3 L'Accepteur 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 tout signe d'acceptation des Cartes du Schéma concerné.

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

ARTICLE 10 - MESURES DE PREVENTION ET DE SANCTION PRISES PAR LA BANQUE

10.1 En cas de manquement de l'Accepteur 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 perdues, volées ou contrefaites, la Banque peut prendre des mesures de sauvegarde et de sécurité consistant, en premier lieu, en un avertissement à l'Accepteur valant mise en demeure précisant les mesures à prendre pour remédier au manquement ou résorber le taux d'impayés anormalement élevé constaté.

10.2 Si, dans un délai de 30 (trente) jours, l'Accepteur 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'acceptation des Cartes dans les conditions précisées à l'article 9 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.

10.3 De même, si dans un délai de 3 (trois) mois à compter de l'avertissement, l'Accepteur 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 11 - SECRET BANCAIRE ET PROTECTION DES DONNEES A CARACTERE PERSONNEL

Conformément aux dispositions de la loi n°78-17 du 6 janvier 1978 modifiée relative à l'informatique, aux fichiers et aux libertés, il est précisé que les données à caractère personnel recueillies aux présentes sont obligatoires pour la conclusion du présent Contrat et son exécution et, qu'à ce titre, elles feront l'objet d'un traitement dont le responsable est la Banque, ce qu'acceptent les personnes sur lesquelles portent lesdites données.

Ces données ainsi que l'ensemble des données à caractère personnel détenues par la Banque dans le cadre des opérations réalisées par les signataires des présentes pourront être utilisées pour les besoins de gestion de ces opérations, d'octroi de crédit, de détection et d'évaluation du risque, de sécurité et de prévention des impayés, de lutte contre la fraude et le blanchiment d'argent, et des actions commerciales de la Banque et des sociétés du Groupe HSBC.

Elles pourront être communiquées aux sociétés dudit groupe ou à des tiers, notamment sous-traitants, partenaires, les Schémas visés en partie 2, sociétés pour lesquelles la Banque intervient dans le cadre d'opérations de courtage situés en France ou à l'étranger, notamment dans des Etats n'appartenant pas à l'Union Européenne, pour l'exécution du présent Contrat ou pour répondre aux obligations légales, fiscales ou réglementaires de la Banque.

Dans le cadre d'un transfert vers des pays tiers à l'Union européenne (actuellement l'Inde, la Chine, l'Égypte, la Malaisie, le Sri Lanka, les Philippines ou les États-Unis sont des pays destinataires à des fins de sous-traitance), des règles assurant la protection des données ont été mises en place et peuvent être consultées sur le site www.hsbc.fr. La liste mise à jour des pays destinataires des données est également consultable sur le même site.

Les personnes susvisées consentent à ce que lesdites données soient communiquées dans les conditions décrites ci-dessus et délient la Banque du secret professionnel.

Les personnes sur lesquelles portent les données à caractère personnel ci-dessus recueillies auront le droit d'en obtenir communication auprès de la Banque (Direction Expérience Client HSBC en France, HSBC Continental Europe, 38 avenue Kléber, 75116 Paris), d'en exiger, le cas échéant, la rectification, de s'opposer à leur utilisation à des fins de prospection, notamment commerciale.

Les titulaires de Cartes sur lesquels des données à caractère personnel ont été recueillies doivent pouvoir disposer desdits droits de communication, de rectification ou d'opposition auprès de l'Accepteur. A cet égard, l'Accepteur s'engage d'ores et déjà à leur permettre d'exercer ces droits.

ARTICLE 12 - NON RENONCIATION

Le fait pour l'Accepteur ou pour la Banque de ne pas exiger à un moment quelconque l'exécution stricte d'une disposition du présent Contrat ne peut en aucun cas être considéré comme constituant de sa part une renonciation, quelle qu'elle soit, à l'exécution de celle-ci.

ARTICLE 13 - IMPRÉVISION

Sans préjudice des autres stipulations du présent contrat, en cas de changement de circonstances imprévisible entraînant un risque d'exécution excessivement onéreuse du contrat, les parties s'engagent à entrer en négociation afin de trouver une solution raisonnablement satisfaisante pour les parties et consentent à ne pas se prévaloir des dispositions de l'article 1195 du Code civil. À défaut d'accord entre les parties dans un délai de 8 (huit) jours calendaires à compter de l'entrée en négociation, le présent Contrat sera résilié de plein droit.

ARTICLE 14 - AUTONOMIE DES DISPOSITIONS

Chaque stipulation du présent Contrat est divisible et si une stipulation est ou devient illégale, nulle ou inopposable, l'application de cette stipulation sera alors écartée, toutes les autres stipulations continuant à produire leurs effets.

ARTICLE 15 - LOI APPLICABLE / TRIBUNEAUX 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 16 - LANGUE DU PRESENT CONTRAT

Le présent Contrat est le contrat original rédigé en langue française qui est le seul qui fait foi.

PARTIE 2

DISPOSITIONS SPECIFIQUES A CHAQUE SCHEMA

DISPOSITIONS SPECIFIQUES AUX SCHEMAS VISA ET MASTERCARD

ARTICLE 1 - FONCTIONNEMENT DES SCHEMAS

Les entités responsables des Schémas Visa et MasterCard sont:
- VISA Inc.et VISA Europe ,
- MasterCard International Inc.

Les Schémas reposent sur l'utilisation des Cartes portant les Marques suivantes:
- Pour VISA Inc. et VISA Europe:
  - Visa
  - VPAY
  - ELECTRON
- Pour MasterCard International Inc.:
  - MasterCard
  - Maestro

ARTICLE 2 - OBLIGATION DE LA BANQUE

Par dérogation à l'article 3.7 de la partie 1 du présent Contrat, 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 de l'Accepteur les opérations de paiement non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.

ARTICLE 3 - 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.

DISPOSITIONS SPECIFIQUES AU SCHEMA CB

ARTICLE 1 - DEFINITION DU SCHEMA CB

Le Schéma CB repose sur l'utilisation de Cartes portant la Marque CB (ci-après les « Cartes CB ») auprès des Accepteurs 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 4 de la partie 1.

ARTICLE 2 - DISPOSITIONS 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.

ARTICLE 3 - DISPOSITIONS SUR l'ACCEPTATION DE CARTES CB

En complément des dispositions de la partie 1, l'Accepteur 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 (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 ou 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 de l'Accepteur, dans les locaux de l'Accepteur ou dans ceux des tiers visés à l'article 2.12 de la partie 1, 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'adhésion, voire à une radiation du Schéma CB telle que prévue à l'article 4 ci-après.

  L'Accepteur autorise la communication du rapport à la Banque et au GIE CB.

ARTICLE 4 - RECLAMATION

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

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

ARTICLE 5 - SUSPENSION DE L'ADHESION ET RADIATION DU SCHEMA CB

5.1 Le GIE CB peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à une suspension de l'adhésion au Schéma CB. Elle est précédée, le cas échéant, d'un avertissement à l'Accepteur, voire d'une réduction de son seuil de demande d'autorisation. Cette suspension est notifiée par tout moyen. Son effet est immédiat.

Elle peut être décidée en raison notamment :

- d'une utilisation anormale de Cartes perdues, volées ou contrefaites,
- d'un risque de dysfonctionnement important du Schéma CB.

5.2 L'Accepteur s'engage alors à restituer à l'Acquéreur 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.

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

5.4 A l'expiration de ce délai, l'Accepteur 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 en paiement à distance sécurisé par cartes de paiement 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 la Banque, et portant sur le respect des bonnes pratiques en matière de vente ou prestations réalisées à distance visées à l'article 2.3 de la partie 1 et des mesures de sécurité visées à l'article 5 de la partie 1.

5.5 En cas de comportement frauduleux de la part de l'Accepteur, il peut être immédiatement radié du Schéma CB ou la suspension être convertie en radiation.

Les exigences présentées ci-après constituent le référentiel sécuritaire de la Banque qui doit être respecté à tout moment par l'Accepteur.

Exigence 1 (E1) - Gérer la sécurité du système commercial et de paiement au sein de l'entreprise

Pour assurer la sécurité des données des transactions et notamment, des données du porteur de Carte, une organisation, des procédures et des responsabilités doivent être établies par l'Accepteur.

En particulier, un responsable de la sécurité du système commercial et de paiement doit être désigné. Il est chargé, entre autres, d'appliquer la législation sur la protection des données à caractère personnel et des données bancaires 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 de paiement 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) - Gérer l'activité humaine et interne

Les obligations et les responsabilités du personnel de l'Accepteur 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 de l'Accepteur 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.

Les personnels de l'Accepteur doivent être sensibilisés aux risques encourus, notamment sur la divulgation d'informations confidentielles, l'accès non autorisé aux informations, aux supports et aux documents. Ils doivent être régulièrement sensibilisés 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 les personnels de l'Accepteur reçoivent une formation appropriée sur l'utilisation correcte du système d'exploitation et du système applicatif commercial et de paiement.

Exigence 3 (E3) - Gérer les accès aux locaux et aux informations

Tout dispositif (équipement réseau, serveur, ...) qui stocke ou qui traite des données relatives à une transaction, et notamment des données du porteur de la Carte, doit être hébergé dans un local sécurisé et répondre aux exigences édictées par les recommandations de la Commission Nationale de l'Informatique et des Libertés (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 système commercial et de paiement

Les règles de sécurité relatives aux accès et sorties depuis et vers le système commercial et de paiement 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 de paiement 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 oeuvre 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) - Contrôler l'accès au système commercial et de paiement

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 de paiement.

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) - Gérer les accès autorisés au système commercial et de paiement

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 accès au système commercial et de paiement

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 être le pare-feu, 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) - Contrôler 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 de paiement.

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

Exigence 9 (E9) - Appliquer les correctifs de sécurité (patches de sécurité) 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 (E l0) - Gérer 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'intégrité des logiciels applicatifs relatifs au système commercial et de paiement

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 traçabilité des opérations 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'intégrité des informations relatives au système commercial et de paiement

La protection et l'intégrité des éléments de la transaction doivent être assurés 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 de paiement doit décrire les moyens mis en place pour répondre à cette exigence.

Exigence 14 (E14) - Protéger la confidentialité des données bancaires

Les données du porteur de Carte ne peuvent être utilisées que pour exécuter l'ordre de paiement et les réclamations.

Le cryptogramme visuel d'un porteur de Carte ne doit en aucun cas être stocké par le commerçant.

Les données bancaires et à caractère personnel relatives à une transaction, et notamment les données du porteur de 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 recommandations de la Commission Nationale de l'Informatique et des Libertés (CNIL).

Il en est de même pour l'authentifiant du commerçant et les éléments secrets servant à chiffrer.

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

Exigence 15 (E15) - Protéger la confidentialité des identifiants/authentifiants des utilisateurs et des 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.