CONDITIONS GENERALES D'ADHESION AUX SYSTÈMES D'ACCEPTATION DE PAIEMENT PAR CARTES

Les Conditions d'adhésion aux Systèmes d'Acceptation de paiement par cartes sont régies par :

- Les conditions particulières que l'Accepteur doit régulariser (« **Conditions Particulières** »)
- Les présentes conditions générales d'adhésion aux Systèmes d'Acceptation de paiement par cartes et leurs Annexes (ci-après « Conditions Générales »)

Les opérations de paiement de l'Accepteur sont garanties sous réserve du respect de l'ensemble des mesures de sécurité, en particulier celles visées dans les présentes Conditions Générales.

ARTICLE 1 : DÉFINITIONS

- «Accepteur» : désigne 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 dûment 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 l'Acquéreur ou lorsqu'il qu'il délivre des espèces dans le respect de la législation applicable (Casinos, Cercles de jeux privés référencés au Ministère de l'intérieur, Changeurs manuels et Prestataires de paiement).

- « Acquéreur » : CCF est qualifié d'Acquéreur dans le cadre de la collecte des transactions cartes de l'Accepteur en vue de leur règlement.

- « Carte », désigne toute Carte portant une Marque CB, Visa et MasterCard, Maestro, Electron, VPay. Une Carte est une solution de paiement que l'Acquéreur accepte. Elle peut être matérialisée par tout support physique ou dématérialisé.

  Lorsqu'elles sont émises dans l'Espace Économique Européen (EEE), les Cartes portent au moins l'une des mentions suivantes :
  - crédit ou carte de crédit,
  - débit,
  - prépayée,
  - commerciale

  Ou l'équivalent dans une langue étrangère.

  Les cartes prépayées sans puce ne portant pas les Marques CB, MasterCard, Maestro, Visa, Vpay, Electron, ne sont pas acceptées dans le Schéma CB. L'acceptation de ce type de carte doit faire l'objet d'un contrat spécifique avec l'émetteur de ces Cartes. Cette liste est valable à la date de signature des présentes et elle est évolutive. L'Accepteur sera informé de toute modification par tout moyen, sans que ce changement ne donne lieu à l'établissement d'un avenant.

- « Émetteur » : désigne un organisme financier ou assimilé qui met une Carte à la disposition de son client, le Titulaire de Carte.

- « Équipement Électronique » désigne tout dispositif de paiement qui comporte un système permettant l'acceptation d'un paiement par Carte comme par exemple un terminal de paiement électronique (ci-après « TPE »), ou une page de paiement sécurisée. Il doit être agréé selon des exigences définies par les Schémas de cartes.

- « Marque » désigne tout nom, terme, sigle, symbole matériel ou numérique ou la combinaison de ces éléments susceptible de désigner le Schéma. Les marques des Schémas pouvant être acceptées entrant dans le champ d'application du présent contrat sont : CB, Visa, MasterCard, Maestro, Electron, VPay, « Paiement de Proximité » désigne tout paiement réalisé au moyen d'un équipement électronique (« Equipement Electronique ») avec la présence physique du Titulaire de Carte.

- « Paiement pour la Location de Biens et Services » désigne un paiement comportant deux étapes :

  - L'acceptation initiale par le Titulaire de Carte de n'être débité qu'à l'issue du service ou de la prestation, du montant des frais réels de celle-ci dans les conditions définies aux présentes Conditions Générales,
  - L'exécution de l'opération de paiement intervenant après détermination de son montant.

  L'opération réalisée dans le cadre d'un Paiement pour la Location de Biens et Services doit respecter les conditions décrites dans les Conditions Générales, qui sont spécifiques aux Paiements de Proximité lorsqu'elle est réalisée dans ce contexte, ou bien celles de Vente à Distance Sécurisée lorsqu'elle se produit dans ce contexte.

- « Point d'Acception » désigne le lieu physique ou digital où l'Équipement Électronique est situé et où le paiement par Carte est réalisé.

«Schéma» désigne un Schéma de cartes de paiement au sens de l'article 2 du Règlement UE n°2015/751 du 29 avril 2015 (ci-après le « **Règlement** ») comme étant 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, qui est distinct de l'infrastructure ou du système de paiement qui assure son fonctionnement, et qui inclut toute organisation, toute entité ou tout organe décisionnel spécifique responsable du fonctionnement du Schéma. Les Schémas CB, Visa, MasterCard, reposent sur l'utilisation de Cartes CB, Visa, MasterCard auprès des Accepteurs et cela dans le cadre des seules dispositions et procédures définies ou homologuées par lesdits réseaux.

- « Système d'Acceptation », désigne tout dispositif permettant la réalisation et le dénouement complet d'une opération de paiement par Carte. Le Système d'Acceptation comprend l'ensemble des réseaux et systèmes informatiques conformes aux règles d'un Schéma qui assurent le transport et le traitement sécurisés des données entre l'Accepteur, l'Acquéreur, les entités de traitement et l'émetteur de la Carte (l' « Emetteur»). Le Système d'Acceptation englobe notamment les fonctions de validation de la Carte, d'authentification du Titulaire de Carte ou de l'utilisateur de l'application de paiement, ainsi que celles d'autorisation, de compensation et de règlement de l'opération de paiement par Carte.

- « Titulaire de Carte » désigne la personne dont le nom est mentionné sur la Carte.

- « Vente à Distance » désigne tout paiement réalisé au moyen d'un Équipement Électronique sans la présence physique du Titulaire de Carte et faisant suite au recueil par l'Accepteur des données Carte par courrier, téléphone, fax...

- « Vente à Distance Sécurisée », désigne tout paiement réalisé sans la présence physique du Titulaire de Carte et pour la réalisation duquel ce dernier saisit lui-même ses données Carte sur l'Equipement Electronique.

ARTICLE 2 : LES SCHÉMAS DE CARTES

Les Schémas de cartes reposent sur l'utilisation de Cartes pour la réalisation d'un paiement.

Lorsque l'Accepteur adhère aux Schémas de cartes, l'Accepteur s'engage à respecter les dispositions et procédures définies ou homologuées par lesdits Schémas.
Le rôle de l'Acquéreur se limite à appliquer les conditions techniques d'acceptation des Cartes et de remise des opérations, et ne s'étend pas à la mise en jeu de la garantie du paiement (telle que visée à l'article « Garantie du Paiement » des présentes Conditions Générales).

ARTICLE 3 : INFORMATION

L'Accepteur a la possibilité d'installer sur l'Équipement Électronique, des mécanismes automatiques qui effectuent la sélection prioritaire d'une Marque de carte ou d'un Schéma. Cependant, l'Accepteur ne peut pas s'opposer à ce que son client passe outre cette sélection.

ARTICLE 4 : OBLIGATIONS DE L'ACCEPTEUR

L'Accepteur s'engage à :

4.1 Assumer seul la responsabilité pleine et entière des services, des biens et produits de l'Acquéreur et du respect de la loi applicable à son Activité (notamment fiscales).

4.2 Respecter et faire respecter à ses prestataires installant sa solution de paiement l'ensemble des contraintes techniques et sécuritaires prévues aux présentes (notamment les Annexes « Référentiel sécuritaire accepteur » et « PCI DSS et risques acquéreurs »), et obtenir leur accord pour que l'Acquéreur puissions diligenter des audits chez eux.

4.3 Accepter que l'Acquéreur procède à des audits conformément à la clause d'audit de l'annexe « PCI DSS et risques acquéreurs ».

4.4 Utiliser un Équipement Électronique agréé par les Schémas de cartes et s'assurer de sa conformité notamment dans le temps en coopération avec l'Acquéreur.

4.5 Recueillir l'autorisation de toute entité ou tout organe décisionnel spécifique responsable du fonctionnement du Schémas de Cartes ou l'autorisation de l'Acquéreur avant de modifier les paramètres de fonctionnement de l'Équipement Électronique ou d'y installer de nouvelles applications.

4.6 Informer l'Acquéreur de tout changement impactant ses déclarations initiales (notamment type d'activité, sociétés prestataires, responsable sécurité...).

4.7 Ne pas exercer une activité de « Membre Service Provider (MSP) – Agrégateurs » qui consiste à assurer la collecte et le recouvrement des paiements effectués par Cartes pour des tiers, professionnels ou particuliers louant ou vendant des biens ou services sur Internet, vendant des espèces ou des Quasi-espèces ; ou encore, à réaliser

la gestion de leurs moyens de paiement. Le non-respect de cette obligation rendrait l'Accepteur pleinement responsable des conséquences dommageables liées à ces activités.

4.8 Afficher visiblement les informations suivantes :

- Les catégories et Marques de cartes que l'Accepteur pourrait acceptez ou refusez, en apposant les panonceaux, vitrophanies et enseignes fournis de façon apparente au Point d'Acceptation.
- Le montant minimum éventuel à partir duquel la Carte est acceptée afin que le Titulaire de Carte en soit préalablement informé.
- Les contraintes spécifiques figurant en Annexe et imposées par type de paiement.

4.9 Informer les Titulaires de Cartes des conditions imposées pour l'utilisation de leur Carte et recueillir leur acceptation explicite.

4.10 S'identifier clairement par son numéro d'identifiant commerçant et par son code activité (NAF/APE) que l'INSEE lui a attribué. Si l'activité de l'Accepteur a changé depuis l'attribution de ce code NAF/APE, ce dernier autorise l'Acquéreur à l'enregistrer sous un code correspondant à son activité actuelle principale ou secondaire. Si l'Accepteur n'est pas immatriculable ou est en cours d'immatriculation, il pourra dans certains cas utiliser un numéro d'identification spécifique, qui lui sera fourni par l'Accepteur lui permettant l'accès aux Schémas de cartes. L'Accepteur devra se faire immatriculer dans un délai maximum de six (6) semaines, sauf cas particulier ci-après :

- Accepteur situé à Monaco, Collectivités d'Outre-Mer, Accepteur situé hors de France,
- Accepteur exerçant une activité secondaire (exemple : garage exerçant à titre d'activité secondaire la location de voitures...),
- Certaines activités spécifiques (distributeur automatique de carburant, armée, artiste).

4.11 S'assurer que son client pourra sans difficulté vérifier et identifier, suite à un paiement, les opérations de paiement qu'il a effectuées sur son Point d'Acceptation (la dénomination commerciale connue du client de l'Accepteur) et le mode de paiement. L'Accepteur doit vérifier auprès de l'Acquéreur la conformité des informations transmises à son client. En cas d'achat de devises étrangères ou de chèques de voyage, l'Accepteur doit également s'assurer que son client pourra identifier le montant éventuel des commissions de change perçues et le montant de l'opération d'achat de Quasi-espèces.

4.12 N'accepter les paiements par Carte qu'en contrepartie de prestations réelles ou de dons, de la remise d'espèces ou de Quasi-espèces, et respecter le choix du Titulaire de Carte en ce qui concerne tant la Marque, que la catégorie de Carte, que le Schéma de cartes lors du paiement par Carte.

4.13 En cas de Paiement pour la Location de Biens et Services, ne pas faire usage de la Carte pour s'octroyer une caution ou effectuer un dépôt de garantie.

4.14 Attribuer à l'occasion de l'initialisation de l'opération de Paiement pour la Location de Biens et Services, un numéro de dossier indépendant du numéro de carte.

4.15 Ne pas réaliser une opération de paiement pour laquelle il n'a pas reçu le consentement du Titulaire de Carte

4.16 Ne pas transmettre à l'Acquéreur les enregistrements des opérations de paiement, dans les délais prévus dans les Conditions Particulières. Le délai maximum pour transmettre les enregistrements est de 6 (six) mois pour l'encaissement des opérations de paiement du Schéma de cartes CB.

4.17 Remettre au Titulaire de Carte ou lui transmettre un justificatif de l'opération de paiement par Carte comportant notamment le montant final de l'opération.

4.18 Dans le cas où l'Accepteur propose des opérations de paiements récurrentes ou échelonnées, il s'engage à respecter les règles relatives au stockage des données cartes, à informer clairement son client des modalités de paiement et à ne plus réaliser de paiements récurrents ou échelonnés dès lors que ce dernier a retiré son consentement.

4.19 Faire son affaire personnelle des litiges avec les Titulaires de Cartes concernant les achats, les réservations ou les locations de biens et services, la remise d'espèces dont l'achat a été réglé par Carte.

4.20 Régler les frais et commissions à l'Acquéreur prévues aux Conditions Particulières.

4.21 A effectuer des travaux de maintenance et de mise à niveau de son Système d'Acceptation conformément aux Conditions convenues avec l'Acquéreur. Ces travaux seront effectués dans le respect des règles définies dans l'annexe « PCI DSS et risques acquéreurs » et « l'annexe Référentiel sécuritaire accepteur ».

4.22 A prendre toutes mesures propres à assurer la garde de son Équipement Électronique et être vigilant quant à l'utilisation qui en est faite. Quels que soient ses modes de commercialisation, il s'engage à respecter les règles définies dans l'annexe « PCI DSS et risques acquéreurs » et l'annexe « Référentiel sécuritaire accepteur » qui ont été communiquées à l'Accepteur.

4.23 A informer immédiatement l'Acquéreur en cas de fonctionnement anormal de sa solution de paiement et de toutes autres anomalies (comme l'absence d'application des procédures de sécurisation des ordres de paiement, le dysfonctionnement du Système d'Acceptation, l'absence de reçu ou de mise à jour de la liste noire, l'impossibilité de réparer rapidement...).

ARTICLE 5 : CONDITIONS D'UTILISATION DE L'ÉQUIPEMENT ÉLECTRONIQUE

Les Schémas de Cartes informent tous les constructeurs connus et référencés par eux des mises à jour de logiciels jugées indispensables. L'Accepteur doit assurer l'installation, le fonctionnement, la maintenance et la mise à niveau de l'Équipement Électronique.

Dans le cadre de l'acceptation des Cartes, l'Accepteur doit :

5.1 Si l'Équipement Électronique appartient à l'Accepteur ou est loué à un tiers

5.1.1 Veiller à ce que sa police d'assurance couvre bien :
- les risques inhérents à la garde de cet Équipement Électronique ou des équipements annexes, dont l'Acquéreur ne saurait être responsable, ainsi que les dommages directs ou indirects résultant de leur destruction ou de leur altération,
- les dommages directs ou indirects sur les Cartes utilisées et sur les équipements annexes qui auraient pu être confiés à l'Accepteur.

5.1.2 Garantir à l'Acquéreur un libre accès à l'Équipement Électronique, tout comme au constructeur ou à toute personne désignée par l'Accepteur pour les différents travaux à effectuer sur l'appareil.

5.1.3 Ne pas utiliser l'Equipement Electronique à des fins illicites ou non autorisées et n'y apporter aucune modification de logiciel ayant un impact sur les Schémas de cartes sans accord préalable de l'Acquéreur. L'Equipement Électronique doit toujours être utilisé dans le respect des présentes Conditions générales.

5.1.4 Assurer, selon le mode d'emploi, les conditions de bon fonctionnement des Équipements Électroniques.

5.2 Si l'Équipement Électronique appartient à l'Acquéreur

L'Accepteur s'engage à :

5.2.1 Réserver dans le Point d'Acceptation, l'emplacement nécessaire à l'installation de l'Équipement Électronique.

5.2.2 Faire son affaire des travaux préalables à la mise en place des Équipements Électroniques (mise à disposition des prises électriques, téléphoniques, etc).

5.2.3 Garantir à l'Acquéreur un libre accès à l'Équipement Électronique, tout comme au constructeur ou à toute personne désignée par l'Acquéreur pour intervenir sur l'Équipement Électronique afin d'en assurer la maintenance, notamment lorsque la mise à jour de logiciels s'avère nécessaire.

5.2.4 Signer, à réception de l'Équipement Électronique, qu'il s'agisse d'une première installation ou d'un remplacement, le bordereau de prise en charge qui luis sera présenté. Ce document reprend les caractéristiques indispensables à l'identification de l'Equipement Electronique.

5.2.5 Ne pas utiliser l'Equipement Electronique à des fins illicites ou non autorisées, n'y apporter aucune modification si ce n'est dans le respect des dispositions des présentes Conditions générales.

5.2.6 Assurer, selon le mode d'emploi, les conditions de bon fonctionnement des Équipements Électroniques dont il a la garde.

5.2.7 Veiller à ce que sa police d'assurance couvre bien les risques inhérents à la garde des Equipements Electroniques ou des équipements annexes et dont l'Acquéreur ne saurait être responsable, ainsi que les dommages directs ou indirects résultant de leur destruction ou de leur altération.

5.2.8 Assumer toutes les obligations du dépositaire, conformément aux dispositions des articles 1927 et suivants du Code Civil.

5.2.9 Payer les frais de location ou de dépôt vente selon les présentes Conditions Particulières convenues avec l'Acquéreur. En outre, cette mise à disposition peut faire l'objet d'un contrat spécifique.

ARTICLE 6 : GESTION DE SITUATIONS SPÉCIFIQUES

6.1 Retrait à son titulaire d'une Carte faisant l'objet d'un blocage ou en opposition

Si conformément à nos procédures, l'Accepteur est conduit à retirer une Carte à son titulaire (le retrait ayant eu lieu notamment sur instruction du serveur d'autorisation en raison de la présence de la Carte sur la liste des Cartes faisant l'objet d'un blocage ou en opposition et/ou contrefaites, l'Accepteur devra utiliser la procédure de gestion et de renvoi des Cartes oubliées ou capturées disponible auprès de son conseiller.

6.2 Oubli d'une Carte par son titulaire

En cas d'oubli de sa Carte par le Titulaire de Carte, l'Accepteur peut la lui restituer dans un délai maximum de deux (2) jours ouvrables après la date d'oubli de la Carte, sur justification de son identité et après obtention d'un accord demandé selon la procédure de gestion et de renvoi des Cartes oubliées ou capturées qui lui est communiquée sur demande.

Au-delà de ce délai, l'Accepteur devra renvoyer la Carte à l'Acquéreur en utilisant la procédure de gestion et de restitution des Cartes oubliées ou capturées.

6.3 Transaction crédit

Le remboursement partiel ou total d'une transaction réglée par Carte doit, avec l'accord du Titulaire de Carte, être effectué au moyen de la Carte utilisée pour l'opération initiale.

6.4 Carte non signée

En cas de Carte non signée et si le panonceau de signature est présent sur la Carte, l'Accepteur doit demander au Titulaire de Carte de justifier de son identité et d'apposer sa signature sur le panonceau de signature prévu à cet effet au verso de la Carte et enfin vérifier la conformité de cette signature avec celle figurant sur sa pièce d'identité. Si le Titulaire de Carte refuse de signer sa Carte, l'Accepteur doit refuser le paiement par Carte.

ARTICLE 7 : LES OBLIGATIONS EN TANT QU'ACQUÉREUR

L'Acquéreur s'engage à :

7.1 Respecter le choix de l'Accepteur et celui du Titulaire de la Carte en ce qui concerne tant la Marque, que la catégorie de Carte, que le Schéma de cartes lors du paiement par Carte.

7.2 Inscrire l'Accepteur sur la liste des points d'acceptation habilités à recevoir des paiements par Cartes.

7.3 Préciser à l'Accepteur la liste et les caractéristiques des Cartes (marques et catégories) pouvant être acceptées et fournir l'Acquéreur à sa demande le fichier des codes émetteurs (BIN).

7.4 Indiquer à l'Accepteur les frais applicables aux Cartes acceptées, y compris les commissions d'interchange et les frais versés aux Schémas de cartes.

7.5 Créditer le compte de l'Accepteur des sommes qui lui sont dues selon les modalités prévues.

7.6 Ne pas débiter, au-delà du délai maximum de vingt-quatre (24) 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.

7.7 Adresser un relevé mensuel des frais d'encaissement carte de l'Accepteur mentionnant :
- les références s permettant d'identifier les opérations de paiement,
- les montants des opérations de paiement exprimés 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 commerçant ainsi que celui de la commission d'interchange.

L'Acquéreur peut demander que les informations soient regroupées par Marque de carte, application de paiement, catégorie de Carte et par taux de commission d'interchange.

7.8 L'Acquéreur indique les commissions de services à acquitter indiquées séparément pour chaque catégorie de Carte selon les différents niveaux de commission d'interchange.

ARTICLE 8 : PAIEMENT "SANS CONTACT"

8.1 Lorsque l'Accepteur bénéficie d'un Équipement Électronique disposant de la technologie « sans contact », ledit Équipement Électronique permet le paiement rapide « sans contact » par des Titulaires de Cartes avec une lecture à distance de la Carte ou du support sur lequel la Carte est enregistré, et sans frappe du code confidentiel.

8.2 L'Accepteur s'engage à signaler au public que le point d'acceptation permet les paiements « sans contact » par l'apposition de façon apparente sur l'Équipement Électronique, au niveau du lecteur « sans contact », d'un pictogramme.

8.3 En toutes circonstances, l'Accepteur doit se conformer aux directives qui apparaissent sur l'Équipement Électronique comme lorsqu'il est demandé de faire composer au Titulaire de Carte son code confidentiel ou mettre en œuvre la méthode d'authentification prévue et adaptée à la technologie applicable dans les meilleures conditions de confidentialité.

8.4 Le paiement en mode « sans contact » n'est pas accepté pour les Cartes des Schémas JCB et Discover même si l'Accepteur a souscrit un contrat avec JCB et Discover pour le paiement de proximité.

8.5 Lorsque le « sans contact » est réalisé par l'utilisation de la Carte physique, le montant unitaire maximum de chaque opération de paiement par Carte en mode « sans contact » est limité (à ce jour à 50 euros, ce plafond étant susceptible d'évoluer). Au-delà de ce montant unitaire maximum, la validation de l'opération par le Titulaire de Carte reste nécessaire. Lorsqu'il est réalisé par l'utilisation d'un autre support intégrant la Carte dématérialisée, le paiement est seulement soumis aux plafonds propres à la Carte.

8.6 Lorsqu'un certain nombre de paiements successifs par Carte en mode « sans contact » est atteint, la composition du code confidentiel sera exigée quel que soit le montant du paiement.

8.7 En cas d'opération « sans contact » permise par l'Équipement Électronique, l'opération de paiement est garantie dans les conditions visées à l'article « Garantie du paiement ».

8.8 L'Acquéreur ne pourra être tenu pour responsable de l'impossibilité d'utiliser la fonctionnalité « sans contact » en cas de dysfonctionnement du téléphone mobile et/ou de la carte SIM, de la carte micro SD ou de l'application de paiement.

ARTICLE 9 : RESPONSABILITÉ DE L'ACQUÉREUR

9.1 En cas de sinistre du fait de l'Acquéreur, celui-ci ne sera tenu qu'à la réparation des préjudices et dommages directs à l'exclusion de tout autre dommage tels que les dommages indirects, incidents ou immatériels et notamment les pertes de profits, les pertes ou les dommages causés aux données (dont les données clients), la perte d'une chance quelles qu'en soient les conséquences, la perte d'image ou l'atteinte à la réputation, que ces dommages soient prévisibles ou non.

9.2 Entre outre, les dommages et intérêts que l'Acquéreur pourrait devoir à l'Accepteur par année pour quelque cause que ce soit, ne pourront jamais excéder le montant total que l'Accepteur paye à l'Acquéreur au terme du présent Contrat pendant l'année civile précédant le sinistre (ou pour la première année du contrat, l'année du sinistre).

ARTICLE 10 : GARANTIE DU PAIEMENT

En cas de contestation du Titulaire de Carte pendant le délai légal, l'Acquéreur pourra débiter le compte de l'Accepteur sans préavis qui devra en assumer les conséquences.

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

Ainsi, l'autorisation donnée par le serveur d'autorisation ne vaut garantie que sous réserve du respect des autres mesures de sécurité, et notamment le contrôle du code confidentiel lorsqu'il est demandé.

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 en l'absence de contestation.

Par ailleurs, l'Emetteur devra aussi authentifier le Titulaire de Carte et autoriser la transaction.

Pour les opérations de paiement réalisées à l'aide d'une Carte émise hors de l'Espace Economique Européen, la garantie de paiement n'est pas acquise en cas de contestation du Titulaire de Carte liée à la relation sous-jacente.

ARTICLE 11 : INFORMATION SUR LES CONDITIONS COMPTABLES ET FINANCIÈRES

Les Conditions Comptables et Financières n'incluent pas les coûts inhérents aux communications téléphoniques (ou électroniques) liées au fonctionnement de l'Équipement Électronique nécessaire à l'exécution des présentes ; ces frais restants par ailleurs à la charge de l'Accepteur.

ARTICLE 12 : RÉCLAMATION ET CONVENTION DE PREUVE

12.1 Réclamation

Toute réclamation concernant le contrat doit être transmise à l'Acquéreur par écrit dans un délai maximum de six (6) mois à compter de la date de l'opération contestée, sous peine de forclusion (perte de vos droits).

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

12.2 Convention de preuve

De convention expresse les enregistrements électroniques émanant notamment du système d'information de l'Acquéreur (ou de celui des Schémas CB, Visa, MasterCard) font foi à moins que l'Accepteur démontre l'absence de fiabilité ou d'authenticité des documents produits.

ARTICLE 13 : MODIFICATIONS

13.1 L'Acquéreur peut, selon les modalités prévues aux Conditions Particulières, modifier les dispositions du présent Contrat.

L'Acquéreur peut notamment apporter :

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

13.2 Les nouvelles conditions entrent en vigueur au terme d'un délai de trente (30) jours à compter de l'information qui est faite à l'Accepteur concernant ces évolutions. Si l'Accepteur les refuse, il peut résilier le contrat dans ce délai de trente (30) jours. Ce délai est exceptionnellement réduit à cinq (5) jours calendaires lorsque l'Acquéreur constate dans le point de vente, une utilisation anormale de Cartes perdues, volées ou contrefaites.

Passé ces délais, l'Accepteur est réputé avoir accepté les modifications.

13.3 Si l'Accepteur ne respecte pas les nouvelles conditions techniques et sécuritaires, dans les délais requis, l'Acquéreur pourra résilier ou suspendre l'adhésion dans les conditions des articles ci-après.

13.4 L'Acquéreur peut à tout moment, et notamment en fonction de l'évolution du montant effectif du panier moyen que l'Acquéreur aura constaté, faire évoluer la tarification de l'Acquéreur figurant à l'article 6 des Conditions Particulières.

L'Accepteur en sera informé par tout moyen, au moins trente (30) jours avant la date d'entrée en vigueur des nouvelles dispositions. Si l'Accepteur les refuse, il pourra résilier le contrat dans ce délai de trente (30) jours. A défaut, le silence de l'Accepteur vaudra acceptation de ces nouvelles dispositions.

ARTICLE 14 : DUREE ET RESILIATION DU CONTRAT

14.1 Le présent Contrat est conclu pour une durée indéterminée. Il peut être résilié sans justification ni préavis selon les modalités prévues aux présentes et aux Conditions Particulières.

14.2 Toute cessation d'activité, cession ou mutation de son fonds de commerce, autorise l'Acquéreur à résilier immédiatement le 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 sa charge et pourront faire l'objet d'une déclaration de créances.

14.3 Après résiliation du présent Contrat, l'Accepteur pourra souscrire un nouveau contrat avec un autre acquéreur de son choix.

14.4 L'Accepteur s'engage lors de la résiliation à restituer à l'Acquéreur les dispositifs techniques et sécuritaires appartenant à l'Acquéreur et plus généralement tout document lui appartenant. Sauf si l'Accepteur a conclu d'autres contrats d'adhésion avec des Schémas de cartes, ce dernier devra retirer immédiatement de vos supports de communication tout signe d'acceptation des Cartes du Schéma concerné.

ARTICLE 15 : MESURES DE PRÉVENTION ET DE SANCTION

15.1 En cas de Transaction crédit abusive, par exemple sans vérifier l'existence préalable d'un paiement par carte bancaire, l'Acquéreur peut rendre indisponible la fonction Crédit sur l'Equipement Electronique.

En cas de manquement 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, l'Acquéreur pourra prendre des mesures de sauvegarde et de sécurité consistant, en premier lieu, en un avertissement valant mise en demeure précisant les mesures à prendre pour remédier au manquement ou résorber le taux d'impayés anormalement élevé constaté.

15.2 Si dans un délai de trente (30) jours, l'Accepteur n'a pas remédié au manquement ayant justifié l'avertissement ou n'avez pas mis en œuvre les mesures destinées à résorber le taux d'impayés constaté, l'Acquéreur se réserve le droit de procéder à une suspension, dans les conditions précisées à l'Article ci-dessous, 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.

15.3 De même, si dans un délai de trois (3) mois à compter de l'avertissement, l'Accepteur est toujours confronté à un taux d'impayés anormalement élevé, l'Acquéreur pourra résilier le présent Contrat de plein droit avec effet immédiat, sous réserve des opérations en cours, en le notifiant à l'Accepteur par lettre recommandée avec demande d'avis de réception.

15.4 Les Schémas peuvent appliquer des pénalités notamment en cas de non-conformité aux règles qu'ils édictent, en cas de dépassement d'un taux de transactions frauduleuses, ainsi qu'en cas de non-respect des mesures de sécurités

détaillées dans les Conditions Générales. L'Accepteur accepte d'emblée que l'Acquéreur puisse débiter sur son compte le montant de ces pénalités.

ARTICLE 16 : SUSPENSION ET RADIATION

L'Acquéreur peut (ou par représentation des Schémas) 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. Elle est précédée, le cas échéant, d'un avertissement, voire d'une réduction de son seuil de demande d'autorisation. Cette suspension est notifiée par tout moyen et doit être motivée. Son effet est immédiat.

Elle peut également intervenir à l'issu de la procédure d'audit visée à l'article 3 de l'annexe « PCI DSS et risques acquéreurs » au cas où le rapport révélerait un ou plusieurs manquements aux clauses du présent Contrat.

En outre, à la demande du Schéma de cartes, l'Acquéreur peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à une radiation de l'adhésion au Système d'Acceptation dudit Schéma de l'Accepteur. La radiation est notifiée par l'envoi d'une lettre recommandée et motivée, avec demande d'avis de réception. Son effet est immédiat.

La suspension ou radiation peut être décidée en raison notamment :
- du non-respect répété des obligations du présent contrat et du refus d'y remédier, notamment d'une utilisation non agréée de l'Equipement Electronique lui permettant d'accéder au Système d'Acceptation et d'un risque de dysfonctionnement important du Système d'Acceptation du Schéma ;
- d'une participation à des activités frauduleuses, notamment d'une utilisation anormale de Cartes perdues, volées ou contrefaites ;
- d'un refus d'acceptation répété et non motivé des Cartes du Schéma que l'Accepteur a choisi d'accepter ou qu'il doit accepter ;
- de plaintes répétées d'autres membres ou partenaires du Schéma et qui n'ont pu être résolues dans un délai raisonnable ;
- de retard volontaire ou non motivé de transmission des justificatifs ;
- d'un risque aggravé en raison de ses activités,
- d'une utilisation anormale ou détournée de l'Equipement Electronique ou du Système d'Acceptation.

L'Accepteur s'engage alors à restituer à l'Acquéreur les dispositifs techniques et sécuritaires lui appartenant et plus généralement tout document lui appartenant. Sauf si l'Accepteur a conclu d'autres contrats d'Adhésion avec des Schémas de cartes, il devra retirer immédiatement de ses supports de communication tout signe d'acceptation des Cartes du Schéma concerné.

La période de suspension est au minimum de six (6) mois, éventuellement renouvelable.
A l'expiration de ce délai, l'Accepteur peut demander à l'Acquéreur la reprise d'effet de son contrat ou souscrire un nouveau contrat avec un autre
Acquéreur de son choix.
En cas de comportement frauduleux de sa part ou de risque élevé de fraude, l'Acquéreur peut être immédiatement radié ou votre suspension pourra être convertie en radiation.

ARTICLE 17 : SECRET BANCAIRE ET PROTECTION DES DONNEES A CARACTERE PERSONNEL

17.1 Secret bancaire

L'Acquéreur à prendre toutes les précautions utiles pour que soient assurés la confidentialité et l'intégrité des données à caractère personnel traitées dans le cadre du présent Contrat.

L'Acquéreur s'assure de la mise en œuvre de dispositifs de protection et de contrôle des accès physiques et logiques pour protéger ces données.

De convention expresse, l'Accepteur autorise l'Acquéreur à stocker le cas échéant des données secrètes ou confidentielles le concernant et à les communiquer à des entités impliquées dans le fonctionnement des Systèmes de paiement aux seules finalités de traiter les opérations de paiement, de prévenir des fraudes et de traiter les réclamations, qu'elles émanent des Titulaires de Cartes ou d'autres entités.

17.2 Protection des données à caractère personnel

L'Accepteur peut avoir accès à différentes données à caractère personnel à l'occasion de l'exécution du présent contrat, dont il doit garantir la sécurité et la confidentialité conformément aux dispositions du présent contrat et au Règlement général sur la protection des données 2016/679 du 27 avril 2016 (« RGPD »). Dans le cadre du présent contrat, l'Accepteur ne peut utiliser ces données à caractère personnel que pour l'exécution des ordres de paiement. En tant que responsable de traitement au sens du chapitre IV du RGPD, il devra respecter les obligations prévues par le RGPD sous peine d'engager sa seule responsabilité. Les données personnelles recueillies et traitées dans le présent contrat par CCF en tant que responsable de traitement ont un caractère obligatoire dans le cadre de sa conclusion. A défaut l'adhésion ne pourra être réalisée.

Les informations personnelles collectées seront principalement utilisées par CCF pour assurer l'ouverture et la gestion des produits et services souscrits, la gestion du risque opérationnel et de lutte contre le blanchiment des capitaux et le financement du terrorisme, la lutte contre la fraude fiscale, la détection et prévention de la corruption, la prévention des impayés, la réalisation de sondages et d'enquêtes de satisfaction, la réalisation d'études statistiques, la gestion, prévention et détection de la fraude et la gestion des plateformes internet.

Certains traitements, tels que la prospection commerciale, sont soumis au consentement préalable qui peut être donné soit à la souscription de nos produits soit ultérieurement sur l'espace de la banque en ligne. Ce consentement peut être retiré à tout moment en se rendant sur l'espace de la banque en ligne ou en s'adressant à nos conseillers. Par exception, sauf opposition de la part de la personne concernée, CCF pourra être amené à lui adresser des offres de produits et services dès lors qu'ils sont similaires à ceux déjà souscrits en se fondant sur l'intérêt légitime que pourrait avoir CCF à adresser de telles offres.

Les données collectées sont conservées pour une durée qui est strictement nécessaire à la bonne exécution du traitement. CCF prend en compte les différentes finalités pour lesquelles les données sont collectées, les personnes concernées par la collecte et le respect d'obligations légales ou règlementaires.

CCF prend, au regarde de la nature des données personnelles et des risques que présentent les traitements, les mesures techniques, physiques et organisationnelles nécessaires pour préserver la sécurité des données personnelles et empêcher qu'elles ne soient modifiées, supprimées ou que des tiers non autorisés y aient accès.

CCF choisit des sous-traitants ou des prestataires qui présentent des garanties en termes de qualité, de sécurité, de fiabilité et de ressources pour assurer la mise en œuvre de mesures techniques et organisationnelles y compris en matière de sécurité des traitements.

Pour sécuriser les transferts hors de l'Union européenne, le CCF peut par exemple mettre en place des clauses contractuelles types définies par la Commission européenne afin d'encadrer les flux. Ces clauses seront accompagnées de mesures complémentaires, techniques de sécurité informatique et organisationnelles.

Sur les informations collectées, toute personne concernée dispose notamment de droits d'accès, de rectification, d'opposition, d'effacement, de limitation du traitement, d'un droit de portabilité des données la concernant, d'un droit de retrait de son consentement notamment à des fins de prospection commerciale et d'un droit de formuler des directives spécifiques et générales concernant la conservation, l'effacement et la communication de ses données post-mortem qui peuvent être exercés en s'adressant par courrier électronique à l'adresse dpo@ccf.fr ou par courrier à l'attention du CCF – Délégué à la protection des Données – 103, rue de Grenelle Paris 75007.

Si la personne concernée estime, après nous avoir contactés, que ses droits « Informatique et Libertés » ne sont pas respectés, une réclamation peut être adressée à la CNIL à l'adresse suivante : Commission nationale de l'informatique et des libertés - 3 Place de Fontenoy - TSA 80715 - 75334 Paris CEDEX 07 ou sur le site www.cnil.fr/fr/plaintes.

Pour en savoir plus sur l'ensemble de ses droits et plus largement sur la gestion des informations personnelles, il conviendra de se reporter à notre « Politique de protection des données personnelles » disponible sur https ://www.ccf.fr/protection-des-données/.

ARTICLE 18 : NON RENONCIATION

Même si l'une ou l'autre Partie n'exige pas à un moment quelconque l'exécution stricte d'une disposition du présent Contrat ceci 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 19 : LOI APPLICABLE : TRIBUNAUX COMPETENTS

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

ARTICLE 20 : LANGUE DU PRÉSENT CONTRAT

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

ANNEXE : Spécificités du Schéma de Cartes CB

ARTICLE 1 : DISPOSITIONS RELATIVES AUX CARTES CB ET APPLICATION DE PAIEMENT CB

Sont utilisables dans le Schéma de cartes et dans le cadre du présent Contrat :

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

ARTICLE 2 : TRANSMISSION DES ENREGISTREMENTS

L'Accepteur doit transmettre à l'Acquéreur les enregistrements des opérations de paiement, dans les délais prévus dans les Conditions Particulières. 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 de cartes.

ARTICLE 3 : ÉQUIPEMENT ÉLECTRONIQUE AGRÉÉ

L'Accepteur doit utiliser obligatoirement un Équipement Électronique agréé CB et s'assurer à cette occasion qu'il est en cours de validité (qu'il n'a pas atteint ou dépassé la date de fin de vie telle que définie dans la notification d'agrément adressée par GIE CB). A cet effet, l'Accepteur peut prendre information de la date de fin de vie auprès de la documentation du GIE CB (notamment en consultant son site internet).

ARTICLE 4 : MESURE DE PREVENTION ET DE SANCTION DANS LE CADRE DE LA VENTE À DISTANCE SÉCURISÉE

4.1 Mesures de prévention et de sanction que l'Acquéreur peut mettre en œuvre

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

Si dans un délai de trente (30) 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, l'Acquéreur peut soit procéder à une suspension de l'adhésion, dans les conditions précisées à l'article "Suspension et Radiation" des Conditions Générales, 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.

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

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

En cas de manquement 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 sont ventilées les remises en paiement entre plusieurs Acquéreurs CB de sorte qu'aucun de ceux-ci n'est en mesure d'avoir une vision globale de son taux d'impayés), le GIE CB peut prendre des mesures de sauvegarde et de sécurité consistant en :

- La suspension de son acceptation des Cartes CB. 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 l'Accepteur 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.

- La radiation de son adhésion au Système d'Acceptation du 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. Cette radiation est notifiée par l'envoi d'une lettre recommandée et motivée, avec demande d'avis de réception.

4.3 L'Accepteur alors restituer à l'Acquéreur les dispositifs techniques et sécuritaires et les documents en sa possession dont l'Acquéreur est propriétaire et à retirer immédiatement de son établissement tout signe d'acceptation des Cartes du Schéma CB.

4.4 La période de suspension est au minimum de six (6) mois, éventuellement renouvelable. A l'expiration de ce délai, l'Accepteur peut demander à l'Acquéreur la reprise d'effet de son Contrat ou souscrire un nouveau Contrat d'adhésion 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 l'Acquéreur ou par le GIE CB et portant sur le respect des bonnes pratiques en matière de vente ou de prestations réalisées à distance et des mesures de sécurité visées dans l'annexe « Paiement à distance ».

ARTICLE 5 : PROTECTION DES DONNEES A CARACTERE PERSONNEL

Au titre de l'acceptation en paiement par Carte CB, le GIE CB traite les données à caractère personnel de l'Accepteur (qui concernent notamment son identité et ses fonctions).
Ces données à caractère personnel font l'objet de traitements afin de permettre :

- la lutte contre la fraude et la gestion des éventuels recours en justice, conformément aux missions définies dans les statuts du GIE CB ;
- de répondre aux obligations réglementaires ou légales notamment en matière pénale ou administrative liées à l'utilisation de la Carte.

L'Accepteur peut exercer les droits prévus au chapitre III du Règlement (UE) 2016/679 du 27 avril 2016 et détaillés à l'article « Secret bancaire et protection des données à caractère personnel » des Conditions Générales par courriel à l'adresse : protegezvosdonnees@cartes-bancaires.com.

Pour toute question en lien avec la protection des données à caractère personnel traitées par le GIE CB, l'Accepteur peut :

- Consulter la Politique de protection des données à caractère personnel du GIE CB accessible à : www.cartes-bancaires.com/protegezvosdonnees ;
- Contacter le Délégué à la protection des données désigné par le GIE CB par courriel à : protegezvosdonnees@cartes-bancaires.com.

ANNEXE : Paiement à distance

ARTICLE 1 : LES OBLIGATIONS DE L'ACCEPTEUR

L'Accepteur déclare connaître les lois et règlements 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 (TV, téléphonie mobile, ordinateur...).
L'Accepteur reconnait devoir se conformer à ces dispositions ou à celles qui pourront intervenir et qu'il doit commercialiser les produits ou prestations de services faisant l'objet d'une vente à distance en respectant les lois et règlements applicables.

Dans le cadre d'une Vente à Distance Sécurisée, l'Accepteur s'engage à :

1.1. Utiliser les procédures de sécurisation des ordres de paiement donnés à distance par les Titulaires de Cartes dans le respect desdispositions légales, réglementaires et professionnelles applicables, notamment et sans limitation, les dispositions relatives aux ventes et prestations réalisées à distance et au commerce électronique (informations des utilisateurs, délais d'exécution des prestations...) ainsi que les bonnes pratiques commerciales telles que définies notamment par les codes de conduite applicables à son activité.

1.2. 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, 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 des dispositions relatives aux conditions d'exercice de professions réglementées et de façon plus générale l'ensemble des textes applicables à son activité et toute vente illicite.

1.3. Garantir l'Acquéreur, ainsi que les Schémas de cartes le cas échéant, contre toute conséquence dommageable pouvant résulter du manquement de vos obligations contractées au titre des présentes.

1.4. Utiliser obligatoirement un Système d'Acceptation conforme aux spécifications définies par les Schémas de cartes et les procédures de sécurisation des ordres de paiement donnés à distance par les Titulaires de Cartes.

1.5. Faire son affaire des litiges commerciaux et de leurs conséquences financières pouvant survenir avec des Titulaires de Cartes notamment lors de l'exercice par ces derniers de leur droit de rétractation et concernant des biens et des services dont l'achat a été réglé par Carte au titre du présent contrat.

1.6. Utiliser obligatoirement un Système d'Acceptation conforme aux spécifications définies par les Schémas de cartes, au Référentiel sécuritaire accepteur figurant en annexe et au Protocole 3D Secure dans le cadre d'un paiement transmis par internet.

1.7. Présenter sur son site internet les informations suivantes :

- la description détaillée des biens et / ou des services qu'il propose à la vente,
- le pays de localisation de son activité,
- la devise de paiement,
- des conditions générales d'utilisation informant les Titulaires de Cartes notamment :
  - du dispositif prévu pour la livraison des biens et / ou des services et les restrictions d'exportations,
  - du dispositif prévu pour le retour des biens et / ou des services et le remboursement aux Titulaires de Cartes associé,
  - d'un contact pouvant répondre aux questions des Titulaires de Cartes et ses coordonnées par mail ou par téléphone,
  - dans le cas où il propose un mode de facturation par des paiements récurrents par Cartes, le site doit expliquer comment le Titulaire de Carte peut faire cesser la vente des biens et / ou des services et la facturation associée.

ARTICLE 2 : LES MESURES DE SÉCURITÉS

2.1. Lors du paiement, l'Accepteur s'engage à :

2.1.1 Appliquer la procédure décrite dans les Conditions Particulières,

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

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

- la période de validité (fin et éventuellement début),
- la catégorie et la marque de la Carte utilisée qui doivent être indiquées dans les Conditions Particulières ou dans les Conditions Générales.

2.1.4 Demander obligatoirement une autorisation d'un montant identique à l'opération,

2.1.5 Contrôler (ou faire contrôler) le cryptogramme visuel donné par le Titulaire de Carte.

2.2. Suivre et respecter la procédure d'authentification demandée par l'Emetteur.

Après une opération de paiement, l'Accepteur s'engage à :

2.3. Transmettre à l'Acquéreur dans les délais et selon les modalités prévues dans les Conditions Particulières, les enregistrements électroniques des opérations et s'assurer qu'ils ont bien été portés au crédit de son compte dans les délais et selon les modalités prévues aux Conditions Particulières. L'Accepteur 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 doit être obligatoirement remise à l'Acquéreur.

2.4. Envoyer au Titulaire de Carte, lorsqu'il le demande, un ticket précisant, entre autres, le mode de paiement par Carte utilisée.

ANNEXE : Paiement pour la Location de Biens et Services

Dans le cadre d'un Paiement pour la Location de Biens et Services en Vente à Distance Sécurisé ou en Paiement de Proximité, en plus des conditions énoncées dans l'annexe « Paiement en vente à distance » ou « Paiement de Proximité », l'Accepteur s'engage à respecter les conditions suivantes :

ARTICLE 1 : NE PAS FAIRE USAGE DE LA CARTE POUR S'OCTROYER UNE CAUTION OU UN DÉPÔT DE GARANTIE

L'Accepteur s'engage à ne pas faire usage de la carte pour s'octroyer une caution ou un dépôt de garantie.

ARTICLE 2 : SUITE A LA CONCLUSION DE LA CONVENTION DE LOCATION, L'ACCEPTEUR S'ENGAGE À:

2..1 Recueillir l'acceptation du Titulaire de Carte d'être débité du montant des frais réels de la location dont le montant estimé lui est précisé. S'associer à un numéro de dossier à l'opération de paiement de la location ainsi initialisée.

2.2 Obtenir une autorisation d'un montant identique à celui connu et accepté par le Titulaire de la Carte

2.3 Remettre au Titulaire de Carte l'exemplaire du ticket (dématérialisé le cas échéant) qui lui est destiné sur lequel doit figurer notamment :

- le montant des frais estimés de la prestation de location,
- le numéro de dossier,
- la mention de : « ticket provisoire » ou « pré-autorisation ».

ARTICLE 3 : APRÈS L'EXÉCUTION DE L'OPÉRATION DE PAIEMENT, L'ACCEPTEUR S'ENGAGE À :

Clôturer l'opération de paiement, à l'issue de la location ou dans les 30 jours calendaires après l'opération, en recherchant via le numéro de dossier, l'opération de paiement initialisée lors de la mise à disposition du bien et la finaliser pour le montant final des frais réels connu et accepté par le Titulaire de Carte qui ne doit pas excéder la valeur du montant autorisé par ce dernier.

ANNEXE : Paiement de Proximité

ARTICLE 1 : LORS D'UN PAIEMENT DE PROXIMITÉ L'ACCEPTEUR S'ENGAGE À :

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

- la présence de la Marque sur la Carte ou de la Marque des cartes acceptées conformément à l'article 1 des Conditions Générales,
- le cas échéant l'hologramme sauf pour les Cartes portant la Marque V Pay,
- la présence de la puce sur les cartes CB,
- la Marque et catégorie de Carte définies à l'article 1 des Conditions Générales,
- le cas échéant, la période de validité (fin et éventuellement début).

1.2 Utiliser l'Equipement Electronique, respecter les indications affichées sur son écran et suivre les procédures dont les modalités techniques lui ont été indiquées.

L'Équipement Électronique doit notamment :

- après la lecture de la puce de la Carte lorsqu'elle est présente :
  - permettre le contrôle du code confidentiel lorsque la puce le lui demande,
  - vérifier :
    - le code émetteur de la Carte (BIN),
    - le code service,
    - la date de fin de validité de la Carte.

- lorsque la puce n'est pas présente sur une Carte, après lecture de la piste ISO 2, vérifier :
  - le code émetteur de la Carte (BIN),
  - le code service,
  - la date de fin de validité de la Carte.

1.3 Contrôler le numéro de la Carte par rapport à la dernière liste des Cartes faisant l'objet d'un blocage ou d'une opposition que l'Acquéreur a diffusé, pour le Point d'Acceptation concerné et selon les Conditions Particulières convenues avec l'Acquéreur.

1.4 Lorsque la puce le demande à l'Équipement Électronique, faire composer par le Titulaire de Carte, dans les meilleures conditions de confidentialité, son code confidentiel. La preuve de la frappe du code confidentiel est apportée par le certificat qui doit figurer sur le ticket émis par le Terminal de Paiement Électronique (ci-après « Ticket TPE »).

Lorsque le code confidentiel n'est pas vérifié, l'opération n'est réglée que sous réserve de bonne fin d'encaissement, même en cas de réponse positive à la demande d'autorisation.

1.5 Obtenir une autorisation d'un montant identique à l'opération sous-jacente :

- lorsque le montant de l'opération en cause, ou le montant cumulé des opérations réglées au moyen de la même Carte, dans la même journée et pour le même Point d'Acceptation, dépasse celui du seuil de demande d'autorisation fixé dans les Conditions Particulières convenues avec l'Acquéreur, et ceci quelle que soit la méthode d'acquisition des informations,
- lorsque l'Équipement Électronique ou la Carte à puce déclenche une demande d'autorisation, indépendamment du seuil de demande d'autorisation fixé dans les Conditions Particulières convenues avec l'Acquéreur.

A défaut d'obtention d'une autorisation ou l'autorisation a été refusée par le serveur, l'opération ne sera pas garantie.

Lorsque la puce n'est pas présente sur une Carte, l'autorisation doit être demandée en transmettant l'intégralité des données de la piste ISO 2.

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

Une demande de capture de Carte, faite par le serveur d'autorisation, annule la garantie pour toutes les opérations faites postérieurement le même jour et avec la même Carte, dans le même Point d'Acceptation.

1.6 Faire signer le Ticket TPE dans tous les cas où l'Equipement Electronique le demande.

1.7 Lorsque la signature est requise et que la Carte comporte un panonceau de signature, vérifier attentivement la conformité de celle-ci avec celle qui figure sur ledit panonceau.

Pour une Carte sur laquelle ne figure pas le panonceau de signature, vérifier la conformité de la signature utilisée avec celle qui figure sur la pièce d'identité présentée par le Titulaire de la Carte.

1.8 Dans tous les cas où l'Équipement Électronique édite un Ticket TPE, remettre au Titulaire de la Carte l'exemplaire qui lui est destiné.

ARTICLE 2 : APRÈS UN PAIEMENT, l'ACCEPTEUR DEVRA :

2.1 Transmettre dans les délais et selon les modalités prévues dans les Conditions Particulières, les enregistrements électroniques des opérations, et l'Accepteur s'assure qu'ils ont bien été portés au crédit du compte dans les délais et selon les modalités prévues dans les Conditions Particulières. Toute opération ayant fait l'objet d'une autorisation doit obligatoirement être remise à l'Acquéreur.

2.2 Archiver et conserver, à titre de justificatif, pendant une durée de quinze (15) mois requis par les règles des Schémas de cartes de paiement après la date de l'opération :

- un exemplaire du Ticket TPE comportant, lorsqu'elle est requise, la signature du Titulaire de la Carte,
- l'enregistrement magnétique représentatif de l'opération ou le journal de fond lui-même.

2.3 Communiquer, à la demande de l'Acquéreur et dans les délais prévus dans les Conditions Particulières, tout justificatif des opérations de paiement.

2.4 Ne pas stocker, sous quelque forme que ce soit, aucune des données cartes ci-après :

- le cryptogramme visuel,
- la piste magnétique dans son intégralité,
- le code confidentiel.

ANNEXE : Référentiel sécuritaire accepteur

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

Exigence 1 (E1)
Gérer la sécurité du Système 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 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 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)
Gérer l'activité 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 d'Acceptation.

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 opération de paiement et notamment, des données du Titulaire de 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 Système d'Acceptation

Les règles de sécurité relatives aux accès et sorties depuis et vers le Système 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)
Contrôler l'accès au Système 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 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)
Gérer les accès autorisés au Système 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 d'Acceptation 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 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)
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 d'Acceptation.
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 (E10)
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 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 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 d'Acceptation

La protection et l'intégrité des éléments de l'opération de paiement 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 d'Acceptation doit décrire les moyens mis en place pour répondre à cette exigence.

Exigence 14 (E14)
Protéger la confidentialité des données bancaires

Les données du Titulaire de 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.
Les données bancaires et à caractère personnel relatives à une opération de paiement, et notamment les données du Titulaire 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 dispositions de la loi Informatique et Libertés et aux recommandations de la CNIL. Il en est de même pour l'authentifiant de l'Accepteur et les éléments secrets servant à chiffrer.
Le dossier de sécurité propre au Système d'Acceptation 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.

ANNEXE : PCI DSS et risques acquéreurs

ARTICLE 1 : RÈGLES À RESPECTER

L'Accepteur doit respecter les dispositions du « Référentiel Sécuritaire Accepteur » figurant en Annexe et les exigences de sécurité PCI DSS (il est possible de se référer également au site officiel : http://fr.pcisecuritystandards.org/minisite/en/).
L'Accepteur doit se conformer aux obligations, règles et directives applicables émises par les Schémas de cartes.
En conséquence, l'Accepteur a l'interdiction notamment de stocker ou communiquer, sous quelque forme que ce soit, les données d'authentification du Titulaire de Carte (numéro de carte, cryptogramme visuel, date d'échéance, code confidentiel, la piste magnétique dans son intégralité, ainsi que toute autre donnée qui serait considérée comme sensible et sujette à l'application des mesures du « Référentiel Sécuritaire Accepteur »).
L'Accepteur a l'obligation, auprès de l'Acquéreur, de la bonne réalisation de ses obligations et en fournir les documents associés sur simple demande de l'Accepteur.

ARTICLE 2 : RECOURS À DES TIERS

Dans ses relations contractuelles avec les tiers, tels que les prestataires de services techniques ou les sous-traitants intervenant dans le traitement et le stockage des données liées à l'utilisation des cartes, l'Accepteur s'assure que ces derniers s'engagent à respecter le référentiel de sécurité PCI DSS et les mesures du « Référentiel Sécuritaire Accepteur ».
L'Accepteur doit tenir informé l'Acquéreur du nom et des coordonnées des sous-traitants auxquels l'Accepteur fait appel dans le cadre de la mise en œuvre de sa solution de paiement.

ARTICLE 3 : CLAUSE D'AUDIT

L'Acquéreur pourra procéder dans les locaux de l'Accepteur ou ceux de ses prestataires, tout comme les Schémas, à la vérification par un tiers indépendant du respect tant des clauses du présent Contrat que des exigences figurant en annexe ainsi que des exigences de sécurité PCI DSS. Cette vérification, appelée « procédure d'audit », peut intervenir à tout moment dès la conclusion du présent Contrat.
L'Accepteur autorise que ces rapports que soit communiqués à l'Acquéreur, ainsi qu'aux Schémas de cartes.
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 ses engagements, chacun de ces Schémas pourra procéder à une suspension de l'adhésion, voire à une radiation du Schéma telle que prévue dans les Conditions Générales.
L'Accepteur est tenu d'informer l'Acquéreur immédiatement et de suivre intégralement ses instructions s'il en a connaissance ou s'il soupçonne que des données de transactions sont (ou ont été) accessibles à des tiers ou sont (ou peuvent être) utilisées abusivement par des tiers. L'Accepteur fournit dans ce cas sans délai, de sa propre initiative ou à la demande à l'Acquéreur, toutes les informations (telles que les données de transaction) en vue du traitement du dossier.
L'Accepteur est tenu d'apporter tout son concours à l'enquête et de suivre intégralement toutes les instructions s'il soupçonne ou constate que des données de transaction erronées, falsifiées ou volées ont été utilisées dans son commerce, ou l'utilisation de données compromises ou d'autres actes et/ou transactions frauduleux à partager les résultats de l'enquête avec des tiers tels que les Schémas de cartes.
L'Accepteur est tenu de ne commettre aucun acte pouvant nuire à une enquête éventuelle ou influencer négativement les résultats d'une telle enquête. Par « actes », on entend notamment l'extinction de systèmes ou la suppression de fichiers.
L'Acquéreur pourra aussi bloquer les fonds « suspects ».
L'Accepteur accepte d'être facturé des éventuelles pénalités qui pourraient lui être appliquées par les Schémas de cartes en cas de compromission de données du fait de manquements ou d'actes et de faits relevant de sa responsabilité notamment après un audit.

ARTICLE 4 : INVENTAIRE DES TERMINAUX DE PAIEMENT ÉLECTRONIQUE

L'Accepteur doit établir un inventaire des TPE et de leurs caractéristiques. L'inventaire doit au minimum lister la marque, le modèle, le numéro de série, l'emplacement physique de chaque TPE. La mise à jour de ces informations est requise dès lors qu'un changement intervient.
L'Accepteur doit vérifier périodiquement (une revue mensuelle est préconisée) l'exactitude de ces informations.
En cas de présence anormale d'un TPE il doit le signaler immédiatement à l'Acquéreur.

ARTICLE 5 : ENTRÉE EN RELATION ET SUIVI DE LA RELATION

Sur demande de l'Acquéreur, l'Accepteur devra l'informer par le biais du formulaire « Fiche d'Identification Accepteur » :

- Des informations relatives aux types d'activités réalisées, aux coordonnées des sous-traitants auxquels il fait appel dans le cadre de la mise en œuvre de sa solution de paiement, aux applications de paiement utilisées, ...

- De tout changement intervenant en cours d'exécution du présent contrat et pouvant impacter ses déclarations initiales.

ARTICLE 6 : ACTIVITÉS ILLÉGALES OU INTERDITES

L'Accepteur s'engage à ne pas exercer une activité de type :

- pornographie infantile,
- vente illégale de drogues comprenant notamment les produits dérivés du cannabis (fleurs et graines de chanvre, produits ou de liquides contenant du cannabidiol – CBD - à un taux supérieur à celui autorisé par la loi),
- sites Internet de jeux d'argent en fonction de la juridiction en cours dans le pays émetteur,
- vente de marchandises contrefaites ou en violation des droits de propriétés,
- pornographie « agressive » : bestialité, viol, mutilation, …
- agrégateur qui traite les transactions d'un autre commerçant et les communique à l'Acquéreur sans l'indiquer dans l'opération de paiement,
- cyberlocker proposant des services d'hébergement ou de téléchargement de données,
- commerce en marketing direct de services pour adultes (sexshop, striptease, pornographie…) par téléphone,
- vente de tabac en Vente à distance et Vente à Distance Sécurisée,
- sites pour adultes (films, « streaming ») en Vente à Distance et Vente à Distance Sécurisée,
- vente de crypto-monnaies (bitcoin et crypto actifs).

Ou plus généralement toute autre activité punie par la loi.

ARTICLE 7 : RISQUES DE FRAUDE

En cas d'alerte de fraude, l'Accepteur s'engage à mettre en œuvre les solutions proposées par l'Acquéreur, telle que l'activation du protocole 3D Secure, afin de réduire la fraude ainsi que le taux de fraude au sein du Point d'Acceptation.
Lorsqu'une activité frauduleuse est constatée, l'Acquéreur pourra contacter l'Accepteur, venir dans ses locaux ou lui communiquer des instructions à suivre. En cas de refus de sa part, l'Accepteur supportera d'emblée l'ensemble des frais liés à la fraude qui n'aura pu être évitée.
Les pénalités appliquées par les Schémas de cartes seront facturées et seront débitées directement sur le compte de l'Accepteur.

ARTICLE 8 : ACTIVITÉS À HAUTS RISQUES

L'Accepteur doit demander l'autorisation et obtenir l'accord préalable de l'Acquéreur et écrit, avant d'exercer des activités notamment telles que définies à hauts risques par les Schémas de cartes dans les documents « Mastercard Security Rules » et « Visa Global Brand Protection Programme ».
Les domaines d'activités précisés ci-dessous sont donnés à titre indicatif et peuvent évoluer dans le temps :

- grossiste en produits pharmaceutiques en Vente à Distance et Vente à Distance Sécurisée,
- détaillant de produits pharmaceutiques en Vente à Distance et Vente à Distance Sécurisée,
- agence de voyages en marketing direct par courriers, mails ou par téléphone,
- commerce en marketing direct hors services pour adultes et agences de voyages,
- vente de cigarettes électroniques en Vente à Distance et Vente à Distance Sécurisée,
- sites pour adultes : sextoys, lingerie… en Vente à distance et Vente à Distance Sécurisée,
- paris, vente de jetons de casino et jeux de hasard en Vente à Distance et Vente à Distance Sécurisée,
- vente d'armes,
- vente de titres à risque élevé en Vente à Distance Sécurisée,
- vente de produits dérivés du cannabis (produits ou e-liquides contenant du cannabidiol – CBD - à un taux autorisé par la loi).

En cas de réponse favorable à la demande de l'Accepteur, ce dernier devra fournir les documents et informations mentionnés dans l'Annexe « Activités à Haut Risques » qui seront communiquées et autoriser à débiter annuellement par l'Acquéreur à l'Accepteur sur son compte des frais correspondants à l'enregistrement de son activité à hauts risques auprès des Schémas de cartes. L'Acquéreur pourra lui communiquer le montant de ces frais sur simple demande.
A noter qu'en cas de volume d'impayés trop important détecté par les programmes « Visa Chargeback Monitoring Program » et Mastercard « Excessive Chargeback Program », l'Accepteur sera alors considéré comme exerçant une activité à Haut Risques et sera soumis à l'ensemble de ces obligations, notamment à un enregistrement de son activité à Haut Risques auprès des Schémas de cartes ainsi qu'au paiement des frais correspondants.

ARTICLE 9 : PENALITES ET RÉSILIATION

En cas de manquement à l'une de ces obligations, l'Accepteur s'expose à des pénalités en provenance des Schémas de cartes ainsi qu'à la résiliation du présent Contrat.
En cas de survenance d'un incident de sécurité majeur, notamment en cas de violation des données, l'Accepteur devra coopérer avec l'Acquéreur et les autorités compétentes le cas échéant. Le refus ou l'absence de coopération de la part de l'Accepteur pourra entraîner la résiliation du présent Contrat.
La résiliation du Contrat lui alors notifiée par l'envoi d'une lettre recommandée, avec demande d'avis de réception. Son effet est immédiat.

NOTICE D'INFORMATION ET DE SENSIBILISATION

INTRODUCTION AUX PROGRAMMES DE GESTION DE RISQUES

L'augmentation des paiements par carte bancaire a vu augmenter de manière significative le vol de données électroniques et d'informations de paiement.
Pour maîtriser les taux de fraude et garantir la confiance des clients dans le système de paiement, les principaux Schémas de Cartes bancaires ont développé un ensemble de programmes de gestion de risques auxquels les Acquéreurs et les Accepteurs sont parties prenantes. Ce guide a pour objectif d'expliquer aux Accepteurs la manière dont ils doivent appliquer les bonnes pratiques réglementaires.

PROGRAMMES DE GESTION DE RISQUES

1.1 Quels sont les objectifs du programme de bonnes pratiques PCI DSS ?
PCI DSS - Payment Card Industry Data Security Standard, est un ensemble de bonnes pratiques de sécurité qui visent à réduire les risques de vol ou d'usurpation de données de cartes de paiement. Le respect de ces bonnes pratiques réduit le risque d'être victime d'une compromission de données, protège l'activité, la réputation et augmente la confiance que des clients placent à disposition de l'Accepteur.

1.2 Qui doit informer l'Accepteur en cas de changement de mode de vente, ou de nature des biens, produits et services vendus ?
Le Contrat conclu avec l'Acquéreur identifie son activité principale selon la classification « Code NAF » normalisée de l'INSEE, et selon son type de mode de vente : Paiement de proximité ou Vente à distance sécurisée.
Toute évolution du mode de vente devra faire l'objet d'une déclaration préalable à l'Acquéreur. Par évolution du mode de vente, on entend :

- Modification du canal de vente (évolution de vente via TPE vers Vente à distance sécurisée).
- Modification des biens, produits et services vendus.

1.3 Existe-il des catégories de produits, biens et services dont la vente est interdite ou limitée ?
Les activités suivantes sont interdites par les Schémas de Cartes ou par CCF et ne pourront pas faire l'objet d'un contrat d'acceptation :

- pornographie infantile,
- vente illégale de drogues comprenant notamment les produits dérivés du cannabis (fleurs et graines de chanvre, produits ou e-liquides contenant du cannabidiol – CBD - à un taux supérieur à celui autorisé par la loi),
- sites Internet de jeux d'argent en fonction de la juridiction en cours dans le pays émetteur,
- vente de marchandises contrefaites ou en violation des droits de propriétés,
- pornographie « agressive » : bestialité, viol, mutilation ...
- agrégateur qui traite les transactions d'un autre commerçant et les communique à l'Acquéreur sans l'indiquer dans l'opération de paiement,
- cyberlocker proposant des services d'hébergement ou de téléchargement de données,
- commerce en marketing direct de services pour adultes (sexshop, striptease, pornographie...) par téléphone,
- vente de tabac à distance ou par e-commerce,
- sites pour adultes (films, « streaming ») en Vente à distance et Vente à distance sécurisée,
- vente de crypto-monnaies (bitcoin et crypto actifs).
-

Toute autre activité punie par la loi est également interdite d'opération.

Par ailleurs, les activités suivantes sont jugées « à risques » car susceptibles de générer des montants d'impayés plus élevés :

- grossiste en produits pharmaceutiques en Vente à Distance et Vente à Distance Sécurisée,
- détaillant de produits pharmaceutiques en Vente à Distance et Vente à Distance Sécurisée,
- agence de voyages en marketing direct par courriers, mails ou par téléphone,
- commerce en marketing direct hors services pour adultes et agences de voyages,
- vente de cigarettes électroniques en Vente à distance et Vente à Distance Sécurisée,
- sites pour adultes : sextoys, lingerie... en Vvente à distance et Vente à Distance Sécurisée,
- paris, vente de jetons de casino et jeux de hasard en Vente à distance et Vente à Distance Sécurisée,
- vente d'armes,
- vente de titres à risque élevé en Vente à distance sécurisée,
- vente de produits dérivés du cannabis (produits ou e-liquides contenant du cannabidiol – CBD - à un taux autorisé par la loi).

Sans être interdites, ces activités devront faire l'objet d'une déclaration préalable à l'Acquéreur et d'un suivi particulier par celui-ci.

Ces listes sont susceptibles d'évoluer selon la législation en vigueur.

1.4 Quels sont les différents niveaux d'exigences de la norme PCI-DSS ?
Les exigences définies par la norme PCI-DSS varient proportionnellement au nombre de transactions à traiter selon une classification comportant 4 niveaux (*voir le tableau ci-après*).

Niveau de Commerçant Accepteur PCI DSS	**Volumes de transactions**	**Mesures requises pour être conforme**
Niveau 1	Plus de 6 millions de transactions par an (tous canaux confondus).	- Audit sur-site chaque année par un auditeur QSA. - Scan trimestriel de vulnérabilités réalisé par une société ASV.
Niveau 2	Entre 1 et 6 millions de transactions par an (tous canaux confondus).	- Audit sur-site chaque année par un auditeur QSA ou ISA. - Scan trimestriel de vulnérabilités réalisé par une société ASV.
Niveau 3	Entre 20.000 et 1 million de transactions e-commerce par an.	- Questionnaire d'auto-évaluation annuel (SAQ). - Scan trimestriel de vulnérabilités réalisé par une société ASV.
Niveau 4	Tous les autres commerçants Accepteurs.	- Questionnaire d'auto-évaluation annuel recommandé (SAQ).

1.5 Quelles sont les risques en cas compromission des données ?
Si l'Accepteur détecte ou soupçonne une intrusion non autorisée dans un réseau ou tout type de perte de données de Titulaires de cartes, il est essentiel de signaler les détails de l'incident à l'Acquéreur dans les plus brefs délais.
En cas de non-respect de la réglementation en vigueur ou de compromission de données importantes, des mesures pouvant donner lieu à des pénalités financières ou à la fermeture du Contrat pourraient être appliquées.

Paiement en Vente à Distance Sécurisée

L'ensemble des informations précisées ci-après ne concernent que les Accepteurs ayant souscrit un contrat de Vente à Distance Sécurisée.

1.6 Quelles sont vos obligations en tant qu'Accepteur ?

Dès lors que l'Accepteur manipule, transmet ou stocke des données de Cartes (et ce, quel que soit son canal de paiement : point de vente physique, e-commerce, téléphone ...) ou qu'un fournisseur de services s'en charge pour lui, il est soumis à une mise en conformité à PCI DSS.

Les données de Cartes concernées par PCI DSS sont :

- le numéro de la carte,
- la date d'expiration et le nom du porteur,
- le cryptogramme visuel.

1.7 Qu'est-ce qu'un questionnaire SAQ ?

Le questionnaire d'auto-évaluation (Self Assessment Questionnaire - SAQ) est un outil de validation de la conformité PCI DSS utilisé et rempli par les Accepteurs eux-mêmes.

Il existe plusieurs types de SAQ qui dépendent de la nature de l'environnement de paiement (le SAQ applicable à une installation comportant un seul TPE, sera différent d'un SAQ applicable à un E-Commerçant).

Les Questionnaires SAQ sont disponibles en ligne à l'adresse suivante :
https://www.pcisecuritystandards.org/security_standards/documents.php (section « SAQs »).

Le tableau ci-après présente les questionnaires SAQ disponibles et leurs modalités d'utilisations :

Version du SAQ	Description	Proximité	Vente à distance sécurisée	Vente à distance (téléphone, courrier…)
A	Paiement Carte non présente (e-commerce ou commerce par courrier ou téléphone), sous-traitance de toutes les fonctions de données des Titulaires de Cartes auprès d'un fournisseur de services conforme à PCI DSS. Aucune manipulation/transmission/ stockage de données de cartes sur l'environnement de l'Accepteur. *Applicable seulement aux activités E-commerce.Exemple : Commerçant Accepteur exerçant une activité de E-commerce avec sous-traitance auprès d'un fournisseur certifié des fonctions de paiement, redirection vers le fournisseur par méthode Iframe ou HTTP Redirect.*		X	X
A-EP	PaiementE-commerce, sous-traitance de toutes les fonctions de données des Titulaires de carte auprès d'un fournisseur de services conforme à PCI DSS, le site web ne reçoit pas directement des données de cartes mais il peut impacter la sécurité de la transaction de paiement. Aucune manipulation / transmission / stockage de données de cartes sur l'environnement de l'Accepteur. *Applicable seulement aux activités E-commerce.Exemple : Commerçant Accepteur exerçant une activité de E-commerce avec sous-traitance auprès d'un fournisseur certifié des fonctions de paiement, redirection vers le Fournisseur par méthode Direct Post ou Javascript.*		X	
D	Tous les autres Accepteurs non pris en compte dans les descriptions des SAQ précédentes.	X	X	X

1.8 Qu'est-ce qu'un scan de vulnérabilités ?

Un scan de vulnérabilités est une revue de tous les sites et systèmes accessibles depuis Internet, qui permet de vérifier que ceux-ci sont protégés contre les menaces externes telles que : accès illégitimes, hacking, virus, etc.

Le scan de vulnérabilités doit être réalisé chaque trimestre. Il est non intrusif et cible l'ensemble de vos équipements réseaux, systèmes et applicatifs. Il est mené par une entreprise certifiée en tant qu'Approved Scanning Vendor (ASV) et assure à l'Accepteur que son environnement offre un niveau de protection adéquat.

La liste des vendeurs ASV est accessible en ligne à l'adresse suivante :
https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

1.9 Qu'est-ce qu'un audit sur-site mené par un QSA ?

Si l'Accepteur est éligible à un audit sur-site, il doit recourir aux services d'une société accréditée en tant que Qualified Security
Assessor (QSA) qui validera chaque année la conformité PCI DSS de son environnement.

La liste des sociétés accréditées QSA est accessible en ligne à l'adresse suivante :
https://www.pcisecuritystandards. org/approved_companies_providers/qualified_security_assessors.php

1.10 Par où commencer ?

Le standard PCI DSS est accessible en ligne gratuitement sur le site : http://fr.pcisecuritystandards.org/minisite/en/

Il est recommandé de démarrer une analyse d'écart PCI DSS à l'aide du questionnaire d'auto-évaluation (SAQ) qui correspond à l'environnement de paiement de l'Accepteur et de se rapprocher d'un vendeur ASV pour démarrer les scans de vulnérabilité trimestriels. L'Accepteur obtiendra alors de la visibilité sur son niveau de conformité PCI DSS.

S'il s'avère que certaines exigences PCI DSS ne sont pas opérationnelles, il devra développer un plan de mise en conformité couvrant chaque élément non conforme. Ce plan comportera une indication du temps estimé pour chaque action. Les Accepteurs de niveaux 1, 2 et 3 devront transmettre chaque trimestre ce plan à leur Acquéreur

en utilisant l'outil « Approche par Priorités » disponible sur le site ci-dessous, ce qui démontrera ainsi les progrès réalisés et réduira les risques de pénalités pour « non-conformité ».
https://www.pcisecuritystandards.org/documents/Prioritized_Approach_for_PCI_DSS_v20.xls
Lorsque l'Accepteur aura finalisé la mise en conformité, il devra valider sa conformité au standard PCI DSS par le biais de la méthode qui correspond à son niveau de commerçant Accepteur (chaque année : audit annuel sur-site ou auto-évaluation et scan ASV trimestriel), transmettre ces éléments à l'Acquéreur et maintenir son niveau de conformité dans le temps.

1.11 Quelles sont les actions que l'Accepteur peut mener en urgence pour réduire les risques sur son environnement et simplifier sa mise en conformité PCI DSS ?

Le moyen le plus simple pour augmenter la sécurité des données de paiement de ses clients est de ne pas stocker ces données.

Si cela s'avérait indispensable, alors :

- Stockez les données de paiement sur des composants informatiques sécurisés et conformes aux exigences du standard PCI DSS.
- Ne pas conserver sous format électronique ou papier les données de paiement « très sensibles » comme le Cryptogramme Visuel.
- Recourir aux services de fournisseurs de services de paiement conformes au standard PCI DSS et utiliser des applications de paiement certifiées PA-DSS.

Paiement de Proximité

L'ensemble des informations précisées ci-après ne concernent que les Accepteurs équipés de TPE.

1.11 Le commerçant est un Accepteur en Paiement de Proximité. Est-il soumis à la conformité PCI DSS ?

Dès lors qu'il manipule, transmet, ou est au contact de données de cartes bancaires, la conformité de son environnement au Standard PCI DSS est requise.

Cependant, les menaces auxquelles il est confronté en tant que point de vente physique étant différentes de celles d'un marchand E-Commerce, le mécanisme de vérification de sa conformité PCI DSS est allégé. Il n'aura pas l'obligation de faire valider sa conformité PCI DSS chaque année par un auditeur externe ni à remonter l'état de conformité PCI DSS à l'Acquéreur.

1.12 Quelles précautions doit-il prendre pour assurer la sécurité de des Paiements de Proximité ?

Les menaces qui touchent les points de vente physique ciblent avant tout les terminaux de paiement (TPE). Pour se protéger, il est vivement recommandé d'appliquer les bonnes pratiques suivantes :

- Utiliser des TPE conformes à « PCI PED » (demander à son fournisseur de matériel).
- Faites appel à des prestataires certifiés par l'Acquéreur. L'Accepteur doit se rapprocher de son conseiller pour en connaître la liste.
- Ranger en lieu sûr (dans un tiroir sous le comptoir, dans une salle fermée à clé) les reçus commerçants sur lesquels le numéro de Carte, la date d'expiration sont inscrits. Ces reçus sont à conserver sur une durée d'un an.
- Appliquez des autocollants (par exemple le nom de sa société) sur ses TPE pour détecter toute substitution de terminal.
- Ne laisser pas le TPE facilement accessible et sans surveillance, pour éviter qu'ils ne soient manipulés, modifiés et piratés.
- Maintenir à jour un inventaire des numéros de série, marque, modèle, localisation physique de chacun des TPE.
- Inspecter périodiquement vos TPE, leurs connexions, et vérifiez que leurs caractéristiques correspondent à son inventaire.
- N'autoriser l'accès physique aux TPE qu'aux mainteneurs préalablement autorisés et clairement identifiés par leur carte professionnelle.

D'une manière générale, il est vivement recommandé que d'utiliser le questionnaire SAQ correspondant à son environnement de paiement, pour auto-évaluer et améliorer ses pratiques opérationnelles le cas échéant.

1.13 Qu'est-ce qu'un questionnaire SAQ ?

Le questionnaire d'auto-évaluation (SAQ, Self Assessment Questionnaire) est un outil de validation de la conformité PCI DSS utilisé par les Accepteurs qui n'ont pas l'obligation de mener un audit sur-site chaque année.

Il existe plusieurs types de SAQ qui dépendent de la nature de l'environnement de paiement. Les versions de SAQ qui correspondent à des activités de proximité sont les suivants :

Version de SAQ	Description
B	Accepteur utilisant des périphériques d'impression uniquement, ou des TPE autonomes à ligne directe, sans stockage électronique de données de titulaires de carte. *Exemple : Commerçant Accepteur disposant de TPE RTC.*
B-IP	Accepteur utilisant uniquement des TPE autonomes certifiés PTS, avec une connexion IP vers le processeur de paiement, sans stockage électronique de données de cartes. *Exemple : Commerçant Accepteur disposant de TPE certifiés PTS avec liaison IP vers le processeur de paiement.*
C-VT	Accepteur qui saisit manuellement une transaction unitaire à travers un clavier dans une solution basée sur un terminal virtuel Web hébergée chez un fournisseur de services certifié PCI DSS, sans stockage électronique de données de titulaires de carte. *Exemple : Commerçant Accepteur disposant d'une interface de saisie des transactions hébergée chez un fournisseur certifié.*
C	Accepteur possédant des systèmes d'application de paiement connectés à Internet, sans stockage électronique de données de titulaires de carte. *Exemple : Commerçant Accepteur disposant d'une application de paiement reliée au processeur par Internet.*
D	Tous les autres Accepteurs non décrits dans les descriptions des SAQ ci-dessus.

Les Questionnaires SAQ sont disponibles en ligne à l'adresse suivante :
https://www.pcisecuritystandards.org/security_standards/documents.php (section « SAQs »).

Régimes spécifiques : hôtels, compagnies aériennes

1.14 L'Accepteur est un hôtelier. Comment doit-il valider sa conformité PCI DSS ?

Les hôteliers évoluent dans un paysage de risques spécifiques, ils sont soumis à un régime particulier. Les critères qu'ils doivent respecter s'ils acceptent exclusivement les paiements de proximité pour valider leur conformité sont les suivants :

- L'hôtel doit être de niveau 4.
- L'hôtel doit confirmer qu'il ne fait pas de stockage électronique de données d'authentification sensibles (Cryptogramme Visuel, Code PIN, données de la piste) avant ou après l'autorisation.
- L'hôtel confirme que les transactions « no-show » (Le No-show s'applique quand un client ayant réservé une chambre
  ne se présente pas à l'hôtel le jour d'arrivée prévu sans avoir au préalable annulé sa réservation auprès de l'hôtel. Dans ce cas, la première nuit de la réservation est facturée par l'hôtel par une facture « no-show) sont conduites conformément à la réglementation - Visa Europe Operating Regulations, à savoir produire un reçu comportant les informations suivantes :
  - Montant de la nuitée facturée et des taxes applicables.
  - Nom du Titulaire de la Carte débité.
  - Numéro de la Carte (de préférence n'afficher que les six premiers et les quatre derniers chiffres du numéro)
  - La date d'expiration de Carte
  - La mention « No-Show » sur la ligne de signature du reçu.
- L'hôtel fournit chaque année à son acquéreur une liste des fournisseurs de services qui stockent, traitent ou transmettent des données de Cartes.
- L'hôtel confirme qu'il n'utilise pas de mots de passe par défaut sur ses systèmes (en particulier sur les systèmes de
  gestion type PMS (Property Management System qui gère les activités opérationnelles de l'hôtel : réservation, facturation depuis les terminaux points de vente (restauration, bar, boutique, spa, et/ou depuis les systèmes de gestion de téléphonie/Internet/TV payante), gestion des débiteurs, gestion de la relation client).
  L'hôtelier doit confirmer chaque année le respect de ces points à son Acquéreur.

Les hôteliers qui ne s'inscrivent pas dans ces critères devront mettre leur environnement en conformité à PCI DSS.

1.15 L'Accepteur est une compagnie aérienne. Comment doit-il valider sa conformité PCI DSS ?

Les compagnies aériennes, au titre de leur activité d'émission de billets, sont soumises elles aussi à la mise en conformité PCI DSS de leurs environnements. Toutefois, du fait de la complexité générale de leur système d'information, un régime dérogatoire leur est proposé.

Ainsi, les compagnies aériennes processant plus de 50.000 transactions cartes par an doivent fournir à leur Acquéreur un plan de mise en conformité à PCI DSS adressant la conformité au plus tard au 31/12/2017. La compagnie aérienne doit communiquer chaque année l'évolution de son plan d'action à son Acquéreur.

Les compagnies aériennes n'atteignant pas ce volume de transactions n'ont pas d'obligations spécifiques, elles doivent néanmoins appliquer les pratiques « de bon sens » pour sécuriser leurs environnements.

Frais liés aux encaissements par Carte

1.17 Le Règlement UE 2015/751 du Parlement européen et du Conseil relatif aux commissions d'interchange pour les opérations de Paiement liées à une Carte du 29 avril 2015 a pour objectif :

- de faciliter le bon fonctionnement des paiements par Carte dans l'Union Européenne (physiquement ou sur Internet),
- de fixer des règles permettant de co-badger les Cartes ou les applications de paiement (comme l'apposition sur la même Carte de plusieurs marques, par exemple CB et Visa, CB et MasterCard®…)
- et de sélectionner la Marque à utiliser au moment du paiement.

Le législateur européen entend ainsi parvenir à une concurrence loyale et efficace dans tous les Etats de l'Union Européenne sur le marché des services de paiement.

Au 1er janvier 2022, l'Union Européenne compte 27 Etats membres : Allemagne, Autriche, Belgique, Bulgarie, Chypre, Croatie, Danemark, Espagne, Estonie, Finlande, France, Grèce, Hongrie, Irlande, Italie, Lettonie, Lituanie, Luxembourg, Malte, Pays-Bas, Pologne, Portugal, République tchèque, Roumanie, Slovaquie, Slovénie et Suède.

Le règlement est en vigueur depuis le 9 décembre 2015 mais l'entrée en vigueur effective de certaines des dispositions s'est étalée jusqu'au 9 décembre 2016. Les nouvelles règles suivantes ont notamment été définies.

1.18 Information relative aux commissions

A compter du 9 juin 2016, l'Accepteur doit être informé des frais liés aux encaissements par Carte qui lui sont facturés.

Les liés aux encaissements par Carte sont composés de :

- La commission d'Interchange : commission que se facturent les banques et/ou établissements de paiement et qui est refacturée du fait de l'utilisation des Cartes comme moyen de paiement ;
- La commission de service commerçant : commission facturée en contrepartie de la prestation bancaire ;
- La commission systèmes monétiques : commission facturée à la banque de l'Accepteur par les réseaux (CB, MasterCard®, Visa) qui est incluse dans la commission de service commerçant.

Le montant de la commission d'Interchange diffère en fonction du type de Carte.

Interchange	
Débit et Prépayé*	0,20 %
Crédit*	0,30 %
Commercial*	0,90 %

** voir définitions ci-dessous*

Pour une meilleure personnalisation de l'information, l'Accepteur un Relevé Annuel des Frais d'Encaissements Cartes (RAFEC) ainsi qu'un Récapitulatif Mensuel des Frais d'Encaissements (RMFEC) qui comprend les informations déjà délivrées dans le RAFEC mais aussi le détail des frais liés à l'acceptation des Cartes de paiement. Cette information est entièrement gratuite.

A terme l'Accepteur n'aura plus l'obligation d'accepter toutes les Cartes. L'Accepteur également en mesure d'opter pour des conditions plus favorables à une marque de Cartes de paiement plutôt qu'à une autre. Les différentes marques de Cartes de paiement sont par exemple CB, Visa, MasterCard®, Maestro**…**

Les Cartes de paiement se différencient aussi en termes de catégories. **Depuis le 9 juin 2016, ces catégories ont changé de nom et leurs définitions sont précisées :**

- Les Cartes à débit immédiat deviennent des Cartes de **débit.** Ce sont des Cartes de paiement dont les montants sont débités sur le compte du porteur moins de 48h après que les transactions ont été réalisées.
- Les Cartes à débit différé deviennent des Cartes de **crédit.** Ce sont des Cartes dont les montants sont débités de façon différée sur le compte du Titulaire de Carte, avec ou sans intérêts. C'est une définition plus large que celle dont l'Acquéreur a l'habitude en France. Les Cartes de crédit incluent également les Cartes avec paiement en plusieurs fois sans frais, les Cartes de crédit à la consommation, les Cartes de crédit renouvelable (dites « revolving »).
- Les Cartes utilisées à des fins professionnelles deviennent des Cartes **commerciales**. Elles sont utilisées à des fins de dépenses professionnelles. Ce sont, par exemple, les Cartes dites « cartes professionnelles », « Cartes d'entreprise » ou « Cartes d'achat ».
- Les Cartes **prépayées** sont des Cartes permettant de disposer d'une somme d'argent limitée. Elles sont exclusivement réservées aux particuliers. Ce sont par exemple les « Cartes cadeaux » ou « Cartes rechargeables ».

Ces mentions apparaîtront progressivement au recto des Cartes bancaires.

1.19 Choix de la Marque au moment du paiement

Le Titulaire de Carte pourra choisir, au moment de son achat dans son Point d'Acceptation, la Marque qu'il souhaite utiliser pour son achat (CB, Visa, MasterCard®, Maestro**…**). L'Accepteur pourra programmer une sélection automatique mais le choix définitif lui revient.