CONTRAT CADRE DE SERVICES DE PAIEMENT

PARTIE 1 - CONDITIONS PARTICULIERES

ARTICLE 1 : OBJET
Par les présentes, le Client bénéficie de l'ouverture d'un compte de paiement, ainsi que d'un service d'acquisition d'opérations de paiement, et demande à MONEXT, agissant tant pour son propre compte qu'en tant que représentant des Schémas, son adhésion aux systèmes de paiement par Cartes CB, Visa et MasterCard), selon les conditions du présent Contrat Cadre de Services de Paiement.
Il est expressément convenu que les termes en majuscule non spécifiquement définis au sein des présentes Conditions Particulières prennent le sens défini au sein des Conditions Générales et de leurs annexes, ci-après.

ARTICLE 2 : DUREE – RESILIATION
Le présent Contrat Cadre entre en vigueur à compter de sa signature, pour une durée indéterminée. Il remplace tout contrat en vigueur entre le Parties régissant les prestations visées en objet des présentes.
Il pourra être résilié, à tout moment, sans justification et sous réserve du dénouement des opérations en cours, par l'envoi à l'autre partie d'une lettre recommandée avec accusé de réception, moyennant le respect d'un préavis minimum de deux (2) mois en cas de résiliation à l'initiative de MONEXT, ou de trente (30) jours en cas de résiliation à l'initiative du Client. Le Client garde alors la faculté de continuer à adhérer au(x) Schema(s) avec tout autre acquéreur de son choix.

ARTICLE 3 : OUVERTURE DU COMPTE DE PAIEMENT
MONEXT ouvre dans ses livres, au nom du Client, en qualité de titulaire, un compte de paiement dont les caractéristiques lui seront communiquées par courrier ou email.
Ci-après désigné le « Compte ».
En application de l'article L522-4 du Code Monétaire et Financier, le Compte est exclusivement destiné à l'acquisition de paiements dont le montant est crédité sur le Compte, à l'exclusion notamment de tout placement de fonds, même temporaire, sur un produit d'épargne ou d'investissement.
Le Compte ne peut être utilisé que pour un usage professionnel ou une activité associative.

ARTICLE 4 : CONDITIONS LIEES A LA GARANTIE DE PAIEMENT
Les opérations de paiement du Client sont garanties sous réserve du respect des obligations visées au présent Contrat Cadre, notamment telles que listées ci-dessous. En cas de non-respect d'une seule de ces obligations, le Client s'expose à un risque de contestation du titulaire de la carte pendant le délai légal. Dans ce cas, MONEXT peut débiter le Compte sans préavis, le Client devant en assumer les conséquences.

4.1. Conservation des justificatifs après le paiement
Le Client s'engage à conserver pendant quinze (15) mois le justificatif d'une opération (journal de fond, courriel récapitulatif de la transaction, ticket de paiement).

4.2. Délai de communication des justificatifs à notre demande
Le Client doit communiquer les justificatifs dans les huit (8) jours calendaires suivant la demande de MONEXT, à défaut de quoi il s'expose à être débité définitivement du montant de la transaction concernée par un impayé.

4.3. Autorisation
D'un commun accord, les Parties fixent le seuil de demande d'autorisation, par carte, par jour et par point de vente, au premier centime d'euro.

4.4. Délai de remise des fichiers (ou enregistrements) des paiements
Le Client s'engage à transmettre les enregistrements des opérations au centre de traitement de MONEXT quotidiennement, par télécollecte automatique générée par l'Equipement Electronique. Passé ce délai, les transactions ne seront réglées que sous réserve de bonne fin d'encaissement.

4.5. Autres exclusions à la garantie de paiement
Les opérations de paiement ne sont pas garanties en cas :
- d'opération réalisée au moyen d'une carte non valide, périmée, volée ou annulée,
- de fraude avérée,
- de réponse négative à la demande d'autorisation ou de retour du dispositif 3D Secure indiquant que la transaction n'est pas garantie,
- de non-utilisation ou d'indisponibilité du dispositif 3D Secure.

4.6. Zone géographique d'acceptation et de situation géographique du commerçant
L'acceptation du paiement est limitée à l'Espace Economique Européen pour les paiements en euros. MONEXT se tient à la disposition du Client pour toute situation spécifique.

ARTICLE 5 : DATES DE VALEUR
Toute opération portée au crédit ou au débit du Compte sera inscrite sous un (1) à trois (3) jours ouvrés à compter de la réalisation de l'opération.
Par exception à ce qui précède, il est précisé que :
- le paiement des frais et commissions s'inscrira sur le Compte au jour prévu pour leur règlement ;
- les virements de restitution des fonds vers le compte bancaire professionnel du Client seront inscrits au jour d'émission dudit virement.

ARTICLE 6 : RELEVE DES FRAIS
MONEXT transmet par l'intermédiaire du coffre-fort électronique mis à disposition du Client dans le cadre des présentes, chaque année, un Relevé Annuel des Frais d'Encaissements Cartes (RAFEC) et, chaque mois, un Récapitulatif Mensuel des Frais d'Encaissement Carte (RMFEC). Les informations transmises sont regroupées par application (contact/sans contact) par marque, et par catégorie d'instrument de paiement (crédit/débit/...).

ARTICLE 7 : RESTITUTION DES FONDS PERÇUS
Par la présente, le Client donne mandat à MONEXT pour restituer par virement sur son compte bancaire professionnel, les fonds perçus sur le Compte dans le cadre du service d'acquisition des opérations de paiement, dans la limite de la réserve de roulement définie aux présentes.

ARTICLE 8 : LITIGES, FRAUDE ET SECURITE
Le Client déclare avoir pris connaissance de l'ensemble des mesures de sécurité imposées par le présent Contrat Cadre dont le Référentiel Sécuritaire Accepteur figurant en annexe.
En cas de fraude, le Client s'engage à mettre en œuvre, sans délai, les mesures sécuritaires appropriées et à coopérer avec MONEXT et/ou les Schémas, notamment si une alerte est émise par un Schéma et plus généralement pour toute autre demande de la part MONEXT.
Les Schémas peuvent appliquer des pénalités, notamment en cas de dépassement d'un taux de transactions frauduleuses et en cas de non-respect des règles visées à l'article « Gestion de Situations Spécifiques » des Conditions Générales. Le Client accepte d'emblée le débit de son Compte du montant de ces pénalités.

ARTICLE 9 : CONTACT
Pour toutes demandes d'informations, le Client peut contacter les services de MONEXT :
- par courrier à :

MONEXT - Services de Paiement
260, rue Claude Nicolas Ledoux Pôle d'Activités d'Aix-en-Provence CS 60507 13593 Aix-en-Provence Cedex 3 ;
- par e-mail à :

paymentservices.info@monext.net

***

PARTIE 2 - CONDITIONS GENERALES

ARTICLE PRELIMINAIRE - DEFINITIONS

• **« Accepteur » :** désigne tout commerçant, prestataire de services ou personne exerçant une profession libérale, utilisant un Système d'Acceptation. L'Accepteur dispose de toute liberté pour domicilier ses remises à l'encaissement auprès de l'établissement de crédit ou de paiement de son choix.

• **« Acquéreur » :** désigne tout établissement de crédit ou de paiement qui collecte les transactions cartes d'un Accepteur en vue de leur règlement.

• **« Automate » :** désigne tout Equipement Electronique agréé par les Schémas (CB, Visa ou Mastercard), permettant la distribution automatique de biens et services, payables par carte.

• **« Equipement Electronique » :** désigne tout dispositif de paiement qui comporte un système permettant le contrôle du code confidentiel comme par exemple le Terminal de Paiement Electronique (ci -après « **TPE** »). Il doit être agréé selon des exigences définies par les Schémas de cartes (CB, Visa ou Mastercard).

• **« Carte » :** désigne une carte portant une des Marque définies aux Conditions particulières. Une Carte est une solution de paiement acceptée par MONEXT. Elle peut être matérialisée par tout support physique ou dématérialisée.
Lorsqu'elles sont émises dans l'Espace Economique Européen (EEE), les Cartes portent au moins l'une des mentions suivantes (ou leur équivalent dans une langue étrangère) :
- crédit ou carte de crédit,
- débit,
- prépayée,
- commerciale.

Les cartes prépayées sans puce ne portant pas les Marques CB, MasterCard, Maestro, Visa, Vpay et 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'Emetteur de ces 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 Cadre sont définies aux Conditions Particulières.

• **« Schéma » :** désigne un schéma de cartes de paiement qui pose un ensemble de règles régissant l'opération de paiement par carte tel que défini à l'article 2 du Règlement UE n°2015/751 du 29 avril 2015.
Les Schémas CB, Visa et MasterCard reposent sur l'utilisation de Cartes CB, Visa et MasterCard auprès des accepteurs et cela dans le cadre des seules dispositions et procédures définies ou homologuées par lesdits Schémas.

• **« 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 le Client, MONEXT, les entités de traitement et l'émetteur de la carte. Le Système d'Acceptation englobe notamment les fonctions de validation de la carte, d'authentification du titulaire de la 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.

CHAPITRE 1 - CONVENTION DE COMPTE

ARTICLE 1 : PIECES JUSTIFICATIVES

1.1. MONEXT, en qualité d'établissement de paiement réglementé, est assujettit à la réglementation relative à la lutte contre le blanchiment des capitaux et le financement du terrorisme (LCB-FT). A ce titre, MONEXT est tenue, pour toute ouverture d'un compte de paiement, d'identifier le client. Ainsi, pour ouvrir un compte, le Client doit fournir :

En qualité de personne morale :

• un extrait de Kbis datant de moins de trois (3) mois ou tout justificatif d'immatriculation au registre du commerce et des métiers ou équivalent pour les sociétés immatriculées à l'étranger ;

• un justificatif de domicile : quittance de loyer, facture de contrat d'eau, d'électricité ou de gaz, facture d'opérateur Telecom ou internet, … datant de moins de trois (3) mois.

• un exemplaire des statuts à jour, certifié conforme et daté par le dirigeant ;

• un justificatif d'auto-certification fiscale ;

• les états financiers du dernier exercice clos.

En qualité de mandataire sur les comptes, bénéficiaire effectif ou représentant légal :

• Si celui-ci est une personne physique :
- un justificatif d'identité : carte nationale d'identité ou passeport en cours de validité, carte de séjour française ou de résident français en cours de validité, permis de conduire de moins de quinze (15) ans ou document de demande d'asile remis par une préfecture ;
- un justificatif de domicile : dernier avis d'imposition sur le revenu ou quittance de loyer, facture de contrat d'eau, d'électricité ou de gaz, facture d'opérateur Telecom ou internet, … datant de moins de trois (3) mois.

• Si celui-ci est une personne morale :
- un extrait de Kbis datant de moins de trois (3) mois ou tout justificatif d'immatriculation au registre du commerce et des métiers ou équivalent pour les sociétés immatriculées à l'étranger ;
- un justificatif de domicile : quittance de loyer, facture de contrat d'eau, d'électricité ou de gaz, facture d'opérateur Telecom ou internet, … datant de moins de trois (3) mois.

Il est expressément précisé que MONEXT en conservera une copie numérisée.

1.2. En cas d'entrée en relation d'affaires à distance, l'article R.561-5-2 du Code Monétaire et Financier requiert la mise en œuvre de mesures de vigilance complémentaires dont la liste est gratuitement consultables par le client sur le site internet : www.legifrance.gouv.fr.
Dans ce cadre, MONEXT a choisi de mettre en œuvre des mesures de vérification et de certification du document d'identité pour les personnes physiques ou de l'extrait de registre officiel pour les personnes morales par un tiers indépendant du Client, ce que ce dernier reconnait et accepte.
Ces mesures sont applicables au Client et, le cas échéant, à toute personne agissant en qualité de mandataire sur les comptes, bénéficiaires effectifs ou représentant légal.

1.3. À tout moment, MONEXT se réserve le droit de demander tout document complémentaire, notamment concernant certaines opérations particulières, le défaut de fourniture de ces informations pouvant avoir des incidences sur l'exécution ou la poursuite du Contrat Cadre.

1.4. De même, tout au long de la relation d'affaires le Client s'engage à communiquer à MONEXT toute mise à jour ou information utile permettant de garantir l'exactitude des données d'identification le concernant.

ARTICLE 2 : FONCTIONNEMENT DU COMPTE

2.1. Opérations :

Le service de paiement proposé par MONEXT lui permet d'encaisser les fonds d'un payeur sur le Compte du Client en qualité de bénéficiaire. Ces fonds lui sont restitués par virement sur son compte bancaire professionnel, dans la limite de la réserve de roulement telle que déterminée à l'article « Constitution d'une Réserve de Roulement » des présentes.
Les opérations faites sur le Compte peuvent être rectifiées, notamment en cas d'erreur. En conséquence, le Client reconnait et accepte que toute écriture comptabilisée à tort sur son Compte soit contrepassée, soit une écriture au crédit pour corriger une écriture au débit et vice-versa.
Le solde du Compte peut devenir indisponible totalement ou partiellement, en raison de mesures légales ou réglementaires (exemples : gel des avoirs, saisies, Opposition à Tiers Détenteur, Avis à Tiers Détenteur, réquisition...) ou de soupçon de fraude et rendre impossible la réalisation de certaines opérations.

Par ailleurs, le Client s'engage à tenir MONEXT indemne en cas de contestation par un payeur de l'opération de paiement qu'il a initié.
Il est expressément précisé que le Compte ne pourra faire l'objet de prélèvement, ce que le Client reconnait et accepte. En conséquence, le Client s'engage à ne pas accepter d'autorisation de prélèvement sur le Compte ni transmettre le RIB du Compte à un tiers à cet effet.

2.2. Révocation d'un ordre de paiement :

Le Client ne pourra révoquer un ordre de paiement une fois que cet ordre aura été reçu par MONEXT.

2.3. Contestation d'une opération de paiement :

Toute opération anormalement débitée sur le Compte doit être signalée sans délai à MONEXT, en précisant si la contestation repose sur un défaut d'autorisation ou sur une mauvaise exécution. Tous les éléments de justification utiles doivent accompagner la contestation.
Conformément aux dispositions du second alinéa de l'article L. 133-24 du code monétaire et financier, les Parties conviennent que plus aucune contestation ne sera recevable passé un délai de quatre (4) mois suivant la date du débit opéré sur le Compte.
En cas de contestation de l'opération de paiement, MONEXT s'efforce immédiatement de retrouver trace de l'opération de paiement contestée et il notifie le résultat de ses vérifications au Client.

2.4. Frais :

En contrepartie de la fourniture de services de paiement au Client, MONEXT percevra une rémunération dont le montant et les modalités sont fixées dans les Conditions Particulières Applicables au Compte de Paiement, infra.

2.5. Délais d'exécution :

Par convention, MONEXT s'engage à restituer les fonds perçus sur le Compte, hors commission et réserve de roulement, par virement selon un rythme déterminé d'un commun accord, dont l'exécution ne pourra excéder un (1) jour ouvrable. Les jours ouvrables sont du lundi au vendredi hors jours fériés bancaires.

2.6. Responsabilité opérationnelle de MONEXT :

MONEXT est responsable de la bonne exécution des opérations affectant le Compte que ce soit au crédit ou au débit. En cas d'opération mal exécutée, MONEXT n'est responsable que des opérations dont la mauvaise exécution lui est imputable. Si cette mauvaise exécution est imputable à un prestataire de services de paiement du payeur, MONEXT ne redevient responsable à l'égard du Client qu'à compter de la réception des sommes dues à destination du bénéficiaire, transmises par le prestataire de services de paiement du payeur. MONEXT porte alors les sommes reçues au crédit du Compte.
Dans le cas où la responsabilité de MONEXT serait engagée du fait d'une opération non exécutée, mal exécutée ou mal affectée, MONEXT met tout en œuvre, sans tarder, pour rétablir la situation du Compte telle qu'elle aurait dû être si la non-exécution, la mauvaise exécution ou la mauvaise affectation n'avait pas eu lieu.

2.7. Informations :

Un coffre-fort électronique est associé à l'ouverture du Compte dont les modalités figurent à l'article « Coffre-Fort Electronique » des présentes. Le Client est informé des opérations passées sur le Compte grâce à un relevé d'opérations.
Ce relevé est mis à disposition du Client une fois par mois si au moins une opération a été enregistrée depuis la date du précédent relevé dans le Coffre-Fort Electronique.
Il contient des informations détaillées des opérations de paiement enregistrées sur le Compte et notamment :

- la référence de l'opération de paiement ;
- le montant des frais appliqués par MONEXT ;
- la date de valeur du crédit ou du débit.

Il appartient au Client de vérifier les opérations enregistrées, de conserver ses relevés et de signaler toute anomalie ou difficulté d'accès dans les meilleurs délais. Sauf exceptions légales, le délai de contestation des opérations est de deux (2) mois. Au-delà, le Client est présumé avoir acceptées lesdites opérations, sauf s'il en apporte la preuve contraire.
MONEXT recommande au Client de conserver une copie de ses relevés, particulièrement avant la suppression de l'accès aux services fournis par MONEXT en cas de résiliation du Contrat Cadre.
Il est expressément précisé que le Client pourra demander à tout moment à MONEXT de lui fournir, sans frais, les termes du Contrat Cadre de service de paiement sur support papier ou un autre support durable.

2.8. Mandataires :

A l'ouverture du Compte, le Client transmet à MONEXT la liste des mandataires habilités à :

- réaliser toute opération sur le Compte ;
- prendre toute décision relative à l'utilisation du Compte (à l'exception de l'ouverture ou de clôture d'un compte) ;
- accéder à l'historique du Compte.

MONEXT se réserve la possibilité de demander la confirmation de certaines instructions avant de les exécuter.
Le Client peut mettre un terme à un mandat à tout moment par écrit adressé à MONEXT. Il prend nécessairement fin dans les cas suivants :

- la renonciation par le mandataire ;
- l'incapacité ou le décès du mandataire ;
- la révocation judiciaire ;
- la dissolution de la société ou une procédure collective.

MONEXT se réserve également la possibilité de prendre l'initiative de révoquer un mandat.
En pareil cas, il appartient au Client de s'assurer auprès de MONEXT que tout moyen d'accès au Compte par le mandataire ait été supprimé ou restitué.
Dans tous les cas, le Client reste totalement responsable de toute opération réalisée ou décision prise dans le cadre du mandat, jusqu'à ce que MONEXT ait été informé de son terme et des accès à clôturer ou modifier.
Le Client personne morale ne pourra en aucun cas désigner en tant que mandataire un tiers extérieur à ladite personne morale.

ARTICLE 3 : CONSTITUTION D'UNE RESERVE DE ROULEMENT (ROLLING RESERVE)

3.1. Eu égard aux exigences règlementaires applicables, MONEXT constituera sur le Compte une réserve de roulement. Celle-ci, d'un montant minimum obligatoire figurant sur le Compte, est destinée à la couverture de toute opération se présentant au débit du Compte afin que le solde de ce dernier ne puisse devenir négatif, conformément aux obligations réglementaires qui s'imposent aux établissements de paiement.
3.2. MONEXT déterminera le montant de la réserve de roulement associé au Compte et pourra, à sa convenance et à tout moment, faire évoluer le montant de cette dite réserve en tenant informé le Client.
3.3. La réserve de roulement peut être en partie consommée notamment du fait d'un impayé imputé sur le compte de paiement du Client. MONEXT est alors autorisé par le Client, ce qu'il reconnait et accepte, à reconstituer la réserve de roulement dès l'acquisition d'un paiement sur le Compte en ne restituant pas à celui-ci, par virement sur son compte bancaire professionnel, la quotepart correspondante au montant consommé de la réserve de roulement.
3.4. A titre exceptionnel, si la réserve de roulement est totalement consommée du fait d'un ou plusieurs impayé(s) dont le montant unitaire ou cumulé lui est supérieur, MONEXT couvrira l'insuffisance de la réserve de roulement afin que le compte de paiement ne présente pas un solde négatif. MONEXT est alors titulaire d'une créance à l'égard du Client, correspondante à la couverture de l'insuffisance de la réserve de roulement. Cette créance est à valoir sur la prochaine ou les prochaines opération(s) d'acquisition de paiement, ce que le client reconnait et accepte pleinement.
3.5. Dès l'acquisition d'un paiement sur le Compte, le Client autorise expressément, par le présent Contrat Cadre, MONEXT à prélever sur le montant du ou des paiement(s) acquis le montant de la couverture de l'insuffisance de la réserve de roulement, au titre du remboursement de la créance envers MONEXT, et à ne pas lui restituer les montants acquis jusqu'à due concurrence du montant de la réserve de roulement initiale, au titre de la reconstitution de la réserve de roulement.

ARTICLE 4 : PROTECTION DES FONDS DES CLIENTS

Les fonds acquis par MONEXT pour le compte du Client dans le cadre des présentes sont protégés par MONEXT conformément à la législation en vigueur.

A ce titre, MONEXT assure notamment la séparation des fonds des Clients dans un compte affecté spécialement à cette fin ouvert dans un établissement de crédit français, de sorte qu'ils ne pourront jamais servir à régler les dettes de MONEXT en cas d'insolvabilité ou en cas de retrait d'agrément en sa qualité d' « établissement de paiement » et resteront insaisissables par des éventuels créanciers de MONEXT.

ARTICLE 5 : COFFRE-FORT ELECTRONIQUE

5.1. Le Client dispose d'un accès à un coffre-fort électronique rattaché au Compte lui permettant de :

- conserver et archiver les documents bancaires, sous format électronique, dans un centre de stockage hautement sécurisé, pendant la durée légale de conservation (variable selon la nature du document - durée minimale conseillée 10 ans) ;
- consulter en ligne à tout moment les documents bancaires ;
- télécharger ou imprimer lesdits documents.

5.2. Sauf accord contraire des Parties, les documents suivants sont déposés dans le coffre-fort électronique, ce dépôt ayant valeur d'une transmission au Client :

- les relevés de Compte ;
- les Relevés Annuel des Frais d'Encaissements Cartes (RAFEC) et Récapitulatif Mensuel des Frais d'Encaissement Carte (RMFEC).
- le présent Contrat Cadre de Services de Paiement.

ARTICLE 6 : CLOTURE DU COMPTE

6.1. Le Compte pourra être clôturé par l'une ou l'autre des Parties en procédant à la résiliation du Contrat Cadre dans les conditions définies aux articles « Durée – Résiliation » des Conditions Particulières et de présentes Conditions Générales.

6.2. Par exception à ce qui précède, le Compte pourra être clôturé et le Contrat résilié, sans préavis, à l'initiative de MONEXT dans les cas suivants :

- de position créancière non autorisée ;
- de déclaration inexacte ou frauduleuse ;
- de risque avéré de fraude
- de non-respect par le Client à l'une des obligations mise à sa charge au titre des présentes ;
- de fonctionnement anormal du Compte ;
- de comportement répréhensible de la part du Client ;
- de non-respect par le Client de ses obligations légales ou réglementaires vis-à-vis de MONEXT comme par exemple un refus de communiquer des documents ;
- d'incidents de paiement répétés ;
- de Compte inactif ;
- de décès ;
- de liquidation judiciaire ;
- de dissolution de la société ;

le Client restant, le cas échéant, redevable de dédommagements en cas de préjudices.

6.3. À la clôture du Compte, son solde devient immédiatement exigible, à l'exception de la réserve de roulement destinée à assurer une provision suffisante du Compte pour liquider les opérations en cours et ce jusqu'à l'apurement de celles-ci. En outre, si le Client est en situation créancière vis-à-vis de MONEXT à la date de clôture, MONEXT se réserve le droit de procéder au recouvrement de ladite créance par tout moyen à sa disposition, de manière amiable et/ou judiciaire.

6.4. La réserve de roulement est contractuellement restituée par virement sur le compte bancaire professionnel du bénéficiaire indiqué à MONEXT lors de l'entrée en relation ou lors de la dernière mise à jour des documents de connaissance client selon le rythme suivant :

- à date de résiliation + trois (3) mois : 50% de la réserve de roulement ;
- à date de résiliation + six (6) mois : 25% de la réserve de roulement ;
- à date de résiliation + douze (12) mois : 25% de la réserve de roulement qui est dès lors totalement restituée (fermeture définitive).

Jusqu'à fermeture définitive du Compte l'ensemble des conditions tarifaires prévues aux présentes sont applicables.

6.5. Compte Inactif :

Sans manifestation de la part du Client, ni opération pendant douze (12) mois, ou encore si aucun de ses ayants-droit ne s'est manifesté dans les douze (12) mois suivant son décès, le Compte sera considéré comme inactif. Au terme d'un délai de 10 ans à compter de sa dernière manifestation ou opération (ou d'un délai de 3 ans à compter du décès), MONEXT procédera à la clôture du Compte et au versement du solde global en résultant à la Caisse des dépôts et consignations. Le Client, ses représentants, ou ses ayants-droit connus, en seront préalablement informé(s). Par prescription acquisitive trentenaire, cette somme sera définitivement acquise à l'État.

6.6. En cas de Décès ou de Procédure Collective :

Si le Client est une personne physique et que MONEXT est informé de son décès, le Compte et le coffre-fort électronique sont bloqués. Le compte sera liquidé sur justification des droits des héritiers ou instruction du notaire. Le contenu du coffre-fort électronique leur sera mis à disposition sur un support externe. Si le Client est une personne morale, en cas de sauvegarde ou de redressement judiciaire, MONEXT suivra les instructions de l'administrateur judiciaire. Si une liquidation judiciaire est prononcée, l'ensemble de vos engagements devient de plein droit immédiatement exigible, et notamment une éventuelle position créancière.

6.7. La clôture du compte, quelle qu'en soit la cause, entraine la résiliation du présent Contrat Cadre.

ARTICLE 7 : AGREMENT

MONEXT est agréé en qualité d'établissement de paiement sous le numéro d'enregistrement 17028. A ce titre, MONEXT est soumis au contrôle de l'Autorité de Contrôle Prudentiel et de Résolution (ACPR) en ce qui concerne le respect des dispositions législatives et réglementaires. Cet agrément est consultable sur le site de l'ACPR, via le Registre de Agents Financiers (REGAFI) ou en écrivant à :

Autorité de contrôle prudentiel et de résolution - Direction du contrôle des pratiques commerciales - 75436 PARIS CEDEX 09

CHAPITRE 2 - ADHESION AUX SCHEMAS DE CARTES

ARTICLE 8 : LES SCHEMAS DE CARTES

Les Schémas de cartes reposent sur l'utilisation de Cartes pour le paiement de biens ou de services.

Lorsque le Client adhère aux Schémas de cartes (CB, MasterCard ou Visa), il s'engage à respecter les dispositions et procédures définies ou homologuées par lesdits Schémas.

Lorsque MONEXT représente les Schémas (CB, Visa MasterCard), cette représentation concerne l'ensemble des dispositions relatives aux conditions techniques d'acceptation des Cartes CB, Visa ou MasterCard et celles relatives à la remise des opérations à MONEXT, et non la mise en jeu de la garantie du paiement visée à l'article « Garantie du Paiement » des présentes Conditions Générales.

ARTICLE 9 : INFORMATION

Le Client a la possibilité d'installer sur l'équipement utilisé au point de vente, des mécanismes automatiques qui effectuent la sélection prioritaire d'une Marque de carte ou d'un Schéma. Cependant, il ne peut pas s'opposer à ce que ses propres clients passent outre cette sélection.

ARTICLE 10 : OBLIGATIONS DU CLIENT

Le Client s'engage à :

10.1. Connaître et respecter les lois et règlements applicables, ainsi que les bonnes pratiques commerciales applicables à ses activités, telles que définies notamment dans les codes de conduite, tant dans l'exécution du présent Contrat Cadre que dans la commercialisation de ses produits ou services.

10.2. Assumer seul la responsabilité pleine et entière de ses produits et services et garantir MONEXT contre toute incidence dommageable résultant de leur commercialisation, notamment en cas de litige avec des titulaires de Cartes concernant des biens et

des services dont l'achat a été réglé par Carte, ou 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 à distance.

10.3. Respecter et faire respecter à chacun de ses prestataires intervenant sur 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 MONEXT puisse diligenter des audits chez eux.

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

10.5. Utiliser un Equipement Electronique agréé par les Schémas de cartes et s'assurer de sa conformité notamment dans le temps en interrogeant MONEXT. Ne pas modifier les paramètres de son fonctionnement et ne pas y installer de nouvelles applications notamment en acceptant l'intervention de tiers, sans avoir au préalable obtenu l'autorisation de MONEXT.

10.6. Recueillir l'autorisation des Schémas de cartes ou de MONEXT avant de modifier les paramètres de fonctionnement de l'Equipement Electronique et/ou Automate ou d'y installer de nouvelles applications.

10.7. Informer MONEXT de tout changement impactant ses déclarations initiales (notamment type d'activité, sociétés prestataires, responsable sécurité…) et, plus généralement, de toute modification des conditions d'exercice de ses activités susceptible d'avoir un impact sur ses obligations aux termes des présentes.

10.8. 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, la vente illicite, 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 ou des dispositions relatives aux conditions d'exercice de professions réglementées.

10.9. Ne pas exercer une activité de « Member Service Provider (MSP) – Agrégateurs » qui consiste à assurer la collecte et le recouvrement des paiements effectués par Cartes CB, Visa ou MasterCard pour des tiers, professionnels ou particuliers, vendant des biens ou services sur Internet ou à réaliser la gestion de leurs moyens de paiement. Le non-respect de cette obligation rendrait le Client pleinement responsable des conséquences dommageables liées à ces activités.

10.10. Accepter les Cartes pour le paiement d'achats de biens ou de prestations de services offerts à sa clientèle, auquel le porteur a effectivement et expressément consenti, même lorsqu'il s'agit d'articles vendus ou de prestations fournies à titre de promotion ou de soldes.

10.11. Appliquer aux Porteurs de Cartes les mêmes prix qu'à l'ensemble de sa clientèle. En tout état de cause, ne faire supporter, directement ou indirectement, aucun frais supplémentaire au Porteur de Carte, du seul fait qu'il utilise sa Carte comme mode de paiement.

10.12. Afficher visiblement les informations suivantes :

- les catégories et Marques de cartes acceptées ou refusées par le Client, en apposant les panonceaux, vitrophanies et enseignes fournis à cet effet, de façon apparente à l'extérieur et à l'intérieur de son point d'acceptation ou sur tout autre support adapté en cas de vente à distance (par exemple son site internet) ;
- le montant minimum éventuel à partir duquel la Carte est acceptée afin que le titulaire de la Carte ou utilisateur d'application de paiement en soit préalablement informé ;
- les contraintes spécifiques figurant en annexe et imposées par type de paiement.

10.13. Informer les titulaires de Cartes des conditions imposées pour l'utilisation de leur Carte.

10.14. S'identifier clairement par son numéro d'identifiant commerçant et par son code activité (NAF/APE) attribué par l'INSEE. Si son activité a changé depuis l'attribution de ce code NAF/APE, le Client autorise MONEXT à l'enregistrer sous un code correspondant à son activité actuelle principale ou secondaire. Si le Client n'est pas immatriculable, il peut dans certains cas utiliser un numéro d'identification spécifique, fourni par MONEXT, permettant l'accès aux Schémas. Le Client doit se faire immatriculer dans un délai maximum de six (6) semaines, sauf cas particulier ci-après :

- Client situé dans une Collectivités d'Outre-Mer ou hors de France,
- Client exerçant une activité secondaire (exemple : garage exerçant à titre d'activité secondaire la location de voitures…),
- pour certaines activités spécifiques (distributeur automatique de carburant, armée, artiste).

10.15. S'assurer que ses propres clients pourront sans difficulté vérifier et identifier suite à un paiement, les opérations de paiement qu'ils ont initiées chez le Client, son point de vente, sa dénomination commerciale et le mode de paiement. Le Client devant vérifier, auprès de MONEXT, la conformité des informations transmises à ses propres clients.

10.16. N'accepter les paiements par Carte qu'en contrepartie de prestations réelles ou de dons et respecter le choix du titulaire de la Carte en ce qui concerne tant la Marque, que la catégorie de Carte ou le Schéma lors du paiement par Carte.

10.17. Ne pas réaliser une opération de paiement pour laquelle il n'a pas reçu le consentement exprès du titulaire de la Carte.

10.18. Transmettre les enregistrements des opérations de paiement, dans les délais prévus aux Conditions Particulières.

10.19. Dans le cas où il propose des opérations de paiements récurrents ou échelonnées (attention cette forme de paiement est exclue lorsque l'achat ou la prestation de service est soumise à conditions), le Client s'engage à respecter les règles relatives au stockage des données cartes, à informer clairement ses propres clients des modalités de paiement et à ne plus réaliser de paiements récurrents ou échelonnés dès lors que ce dernier a retiré son consentement.

10.20. Régler, selon les Conditions Particulières conclue avec MONEXT, les commissions, frais et d'une manière générale toute somme due au titre du présent Contrat Cadre.

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

10.22. Prendre toutes mesures propres à assurer la garde de son Equipement Electronique et/ou Automate et être vigilant quant à l'utilisation qui en est faite. Quels que soient les modes de commercialisation, le Client doit respecter les règles définies dans les annexes « PCI DSS et risques acquéreurs » et « Référentiel sécuritaire accepteur ».

10.23. Informer immédiatement MONEXT en cas de fonctionnement anormal de du Système d'Acceptation ou de toutes autres anomalies (absence d'application des procédures de sécurisation des ordres de paiement, dysfonctionnement du Système d'Acceptation, absence de reçu ou de mise à jour de la liste noire, impossibilité de réparer rapidement , ...).

10.24. Garantir MONEXT, ainsi que les Schémas le cas échéant, contre toute conséquence dommageable pouvant résulter du manquement de ses obligations contractées au titre des présentes.

ARTICLE 11 : OBLIGATIONS DE MONEXT

11.1. Fournir la documentation (dont les procédures) concernant l'acceptation des paiements et l'accès au serveur d'autorisation, que le Client doit respecter obligatoirement. Ces informations figurent notamment dans les Conditions Particulières ou en annexes.

11.2. Respecter le choix du Client 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.

11.3. Inscrire le Client sur la liste des points d'acceptation habilités à recevoir des paiements par Cartes.

11.4. Préciser au Client la liste et les caractéristiques des Cartes (Marques et catégories) pouvant être acceptées et lui fournir sur demande le fichier des codes émetteurs (BIN).

11.5. Communiquer au Client les frais applicables aux Cartes acceptés, y compris les commissions d'interchange et les frais versés aux Schémas.

11.6. Créditer le Compte du Client des sommes qui lui sont dues selon les modalités prévues aux présentes.
11.7. Ne pas débiter, au-delà du délai maximum de vingt-quatre (24) mois à partir de la date du crédit initial porté au Compte, les opérations non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.
11.8. Adresser les relevés mensuels et annuels des frais d'encaissement carte.
11.9. Indiquer au Client les commissions de services à acquitter séparément pour chaque catégorie de Carte selon les différents niveaux de commission d'interchange.

ARTICLE 12 : GESTION DE SITUATIONS SPECIFIQUES
12.1. Retrait à son titulaire d'une Carte faisant l'objet d'un blocage ou en opposition :
Si le Client est conduit à retirer une Carte à son titulaire, conformément aux procédures définies par MONEXT (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), il doit suivre la procédure de gestion et de renvoi des Cartes oubliées ou capturées disponible sur demande.
Pour toute capture de Carte faisant l'objet d'un blocage ou en opposition et/ou contrefaite et sur instruction de l'Equipement Electronique et/ou Automate, une prime pourra être versée au Client ou à toute personne indiquée par lui et exerçant une activité au sein de son établissement.
12.2. Oubli d'une Carte par son titulaire :
En cas d'oubli de sa Carte par le titulaire, le Client 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 communiquée sur demande. Au-delà de ce délai, le Client doit renvoyer la Carte à MONEXT en utilisant la procédure de gestion et de restitution des Cartes oubliées ou capturées.
12.3. Transaction crédit :
Le remboursement partiel ou total d'une transaction réglée par Carte doit, avec l'accord de son titulaire, être effectué au titulaire de la Carte utilisée pour l'opération initiale. Le Client doit pour cela utiliser la procédure dite de « transaction crédit », et effectuer la remise correspondante. Le montant de la « transaction crédit » ne doit pas dépasser le montant de l'opération initiale.
12.4. Carte non signée :
En cas de Carte non signée et si le panonceau de signature est présent sur la Carte, le Client doit demander au titulaire 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 la Carte refuse de signer sa Carte, le Client doit refuser le paiement par Carte.

ARTICLE 13 : PAIEMENT « SANS CONTACT »
Les membres des Schémas peuvent mettre à disposition de leurs clients une Carte équipée de la technologie « sans contact » et/ou un instrument de paiement disposant de la technologie « Mobile sans contact » (ci-après l'« Instrument de Paiement »). L'Instrument de Paiement est constitué d'un logiciel de paiement mobile en mode « sans contact » intégré pour partie dans l'élément sécurisé d'un téléphone mobile pour partie dans le téléphone mobile lui-même, et permettant de réaliser quelle que soit la Marque du Schéma des opérations de paiement. L'utilisateur de l'Instrument de Paiement (ci-après l'« Utilisateur ») est le titulaire du compte sur lequel fonctionne l'Instrument de Paiement.
En cas d'utilisation d'un Equipement Electronique disposant de la technologie dite « sans contact » ou mobile « sans contact » par le Client, les Parties conviennent des stipulations suivantes :

- L'Equipement Electronique permet le paiement rapide d'achats de biens ou de prestations de services par des titulaires de Cartes ou des Utilisateurs avec une lecture à distance de la Carte/de l'Instrument de Paiement et sans frappe du code confidentiel.
- Le Client s'engage à signaler au public le point d'acceptation de paiement « sans contact » par l'apposition sur l'Equipement Electronique d'un pictogramme apparent permettant d'identifier le paiement « sans contact ».

En toutes circonstances, le Client doit se conformer aux directives qui apparaissent sur l'Equipement Electronique.

- Le montant unitaire maximum de chaque opération de paiement en mode « sans contact » est limité à ce jour à trente (30) euros (sous réserve d'évolution de ce montant). Lorsqu'un certain nombre de règlements successifs en mode « sans contact » est atteint, le Client peut être amené à passer en mode « contact » même pour une opération d'un montant inférieur au montant unitaire maximum d'une opération en mode « sans contact ».
- Lorsque l'Equipement Electronique le demande, le Client doit faire composer par l'Utilisateur de l'Instrument de Paiement son code confidentiel ou mettre en œuvre la méthode d'authentification prévue et adaptée à la technologie applicable dans les meilleures conditions de confidentialité.
- En cas d'opération « sans contact » permise par l'Equipement Electronique, l'opération de paiement est garantie même si le code confidentiel n'est pas vérifié, dans les conditions visées à l'article « Garantie du Paiement » ci-dessous.
- MONEXT ne peut être tenue pour responsable de l'impossibilité d'utiliser le mode « 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.
- Lorsque l'opération de paiement de proximité est réalisée à l'aide d'un Instrument de Paiement, l'article « Gestion de Situations Spécifiques » et l'alinéa 7 de l'article « Obligation de MONEXT » des présentes Conditions Générales ne sont pas applicables.

ARTICLE 14 : GARANTIE DU PAIEMENT
Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité définies au Contrat Cadre, notamment en annexes. 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.
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 la Carte liée à la relation sous-jacente.

ARTICLE 15 : INFORMATION SUR LES CONDITIONS COMPTABLES ET FINANCIERES
Les conditions comptables et financières n'incluent pas les coûts inhérents aux communications téléphoniques (ou électroniques) liées au fonctionnement de l'Equipement Electronique nécessaire à l'exécution des présentes ; ces frais restants à la charge du Client.

ARTICLE 16 : MESURES DE PREVENTION ET DE SANCTION
16.1. En cas de "transaction crédit" abusive, notamment réalisée sans vérifier l'existence préalable d'un paiement par carte bancaire, MONEXT se réserve le droit de rendre indisponible la fonction Crédit sur le terminal de paiement.
16.2. En cas de manquement aux stipulations du présent Contrat Cadre ou aux lois en vigueur ou en cas de constat d'un taux d'impayés anormalement élevé ou d'utilisation anormale de Cartes/Instruments de Paiement perdues, volées ou contrefaites, MONEXT se réserve le droit de 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.
16.3. Si dans un délai de trente (30) jours, le Client n'a pas remédié au manquement ayant justifié l'avertissement ou n'a pas mis en œuvre les mesures destinées à résorber le taux d'impayés constaté, MONEXT pourra soit procéder à une suspension, dans les conditions précisées à l'article « Suspension et Radiation » ci-dessous, soit résilier de plein droit avec effet immédiat, sous

réserve du dénouement des opérations en cours, le présent Contrat Cadre par lettre recommandée avec avis de réception.
16.4. De même, si dans un délai de trois (3) mois à compter de l'avertissement, le Client est toujours confronté à un taux d'impayés anormalement élevé, MONEXT se réserve le droit de résilier le présent Contrat Cadre de plein droit avec effet immédiat, sous réserve des opérations en cours, par notification adressée au Client par lettre recommandée avec avis de réception.

ARTICLE 17 : SUSPENSION ET RADIATION
MONEXT peut (directement 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/Instruments de Paiement. Elle est précédée, le cas échéant, d'un avertissement, voire d'une réduction du seuil de demande d'autorisation du Client. 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 « Clause d'Audit » de l'annexe « PCI DSS et risques acquéreurs » au cas où le rapport révélerait un ou plusieurs manquements aux clauses du présent Contrat Cadre.
En outre, à la demande du Schéma de cartes, MONEXT peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à une radiation de l'adhésion du Client au Système d'Acceptation dudit Schéma. 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 d'un des motifs suivants notamment :
• du non-respect répété des obligations du présent Contrat Cadre et du refus d'y remédier, notamment d'une utilisation non agréée de l'Equipement Electronique permettant au Client 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/Instruments de Paiement perdues, volées ou contrefaites ;
• d'un refus d'acceptation répété et non motivé des Cartes/Instruments de Paiement du Schéma que le Client a choisi ou 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 des activités du Client ;
• d'une utilisation anormale ou détournée de l'Equipement Electronique ou du Système d'Acceptation.
Dans ce cas, le Client s'engage à restituer à MONEXT les dispositifs techniques et sécuritaires et plus généralement tout document, information confidentielle ou donnée appartenant à MONEXT. Le Client doit retirer immédiatement de ses supports de communication et de son lieu de vente, tout signe d'acceptation des Cartes du Schéma concerné, sauf s'il a conclu d'autres contrats d'adhésion avec des Schémas de cartes.
La période de suspension est au minimum de six (6) mois, éventuellement renouvelable. A l'expiration de ce délai, le Client peut demander à MONEXT la reprise d'effet du Contrat Cadre ou souscrire un nouveau contrat avec un acquéreur de son choix.
En cas de comportement frauduleux de la part du Client ou de risque élevé de fraude, ce dernier pourra être immédiatement radié ou sa suspension pourra être convertie en radiation.

CHAPITRE 3 - STIPULATIONS DIVERSES

ARTICLE 18 : DUREE ET RESILIATION
18.1. Le Contrat Cadre est conclu pour la durée prévue aux Conditions particulières. Il peut être résilié selon les modalités prévues aux présentes et aux Conditions Particulières.
18.2. En cas de manquement par l'une des Parties à l'une quelconque des obligations lui incombant aux termes des présentes, la Partie lésée aura la possibilité de résilier le Contrat Cadre par anticipation et sans formalité judiciaire. La résiliation interviendra dans un délai de quinze (15) jours ouvrés après mise en demeure notifiée par lettre recommandée avec accusé de réception à la Partie défaillante, indiquant l'intention de faire jouer la présente clause et restée en tout ou partie sans effet, sans préjudice des éventuels recours intentés par la Partie lésée et notamment en dommages et intérêts.
18.3. Toute cessation d'activité, cession ou mutation du fonds de commerce du Client, autorise MONEXT à résilier immédiatement le Contrat Cadre sous réserve du dénouement des opérations en cours.
Dans le cas où, après résiliation du Contrat Cadre, il se révèlerait des impayés, ceux-ci seront à la charge du Client et pourront faire l'objet d'une déclaration de créances.
18.4. Lors de la résiliation, le Client s'engage à restituer à MONEXT les dispositifs techniques et sécuritaires et plus généralement tout document, information confidentielle ou donnée appartenant à MONEXT. Le Client doit retirer immédiatement de ses supports de communication et de son lieu de vente, tout signe d'acceptation des Cartes du Schéma concerné, sauf s'il a conclu d'autres contrats d'adhésion avec des Schémas de cartes.

ARTICLE 19 : MODIFICATIONS
19.1. MONEXT se réserve le droit de modifier les stipulations du présent Contrat Cadre, afin notamment d'apporter :
• des modifications techniques telles que l'acceptation de nouvelles Cartes, des modifications de logiciel, le changement de certains paramètres, la remise en l'état du Système d'Acceptation à la suite d'un dysfonctionnement, etc…
• des modifications sécuritaires telles que :
- la suppression de l'acceptabilité de certaines Cartes ;
- la suspension de de l'adhésion à un Schéma de carte ;
- la modification du seuil d'autorisation.
• des modifications tarifaires, notamment en cas de modification des frais pratiqués par les schémas de carte ou en cas d'évolution des données déclarées par le client dans l'article « Données en entrée du service » des Conditions Particulières.
19.2. Les nouvelles conditions entrent en vigueur au terme d'un délai de deux (2) mois à compter de l'information du Client concernant ces évolutions. Ce délai peut exceptionnellement être réduit à cinq (5) jours calendaires si MONEXT constate une utilisation anormale de Cartes perdues, volées ou contrefaites dans le point de vente du Client.
19.3. En cas de refus, le Client peut notifier à MONEXT sa volonté de mettre fin au Contrat Cadre par courrier recommandé avec accusé de réception. Ainsi le Contrat Cadre sera automatiquement résilié à la date prévue pour l'entrée en vigueur des nouvelles conditions. A défaut, le silence du Client vaut acceptation des nouvelles conditions.
19.4. Le non-respect des nouvelles conditions techniques et sécuritaires, dans les délais impartis, peut entraîner la résiliation ou la suspension l'exécution du présent Contrat Cadre dans les conditions des articles « Durée et Résiliation du Contrat Cadre » et « Mesures de Prévention et de Sanction » ci-après.
19.5. Toutes dispositions législatives ou réglementaires qui rendraient nécessaire la modification de tout ou partie du Contrat Cadre seront applicables sans préavis dès leur date d'entrée en vigueur.

ARTICLE 20 : SECRET BANCAIRE
De convention expresse, le Client autorise MONEXT à traiter et stocker, le cas échéant, des données confidentielles et protégées par le secret professionnel le concernant et à les communiquer à des entités impliquées dans le fonctionnement du Système d'Acceptation 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.
A l'occasion de l'exécution des ordres de paiement donnés par Carte, MONEXT accède à des données à caractère personnel concernant les titulaires de Cartes.
MONEXT utilise ces données pour exécuter des ordres de paiement et pour respecter ses obligations légales et règlementaires. Dans le cadre des opérations de paiement ces données seront transmises aux Schémas de cartes et aux prestataires de MONEXT en vue de l'exécution des ordres de paiement.
Le Client s'engage, quant à lui, à traiter les données personnelles de ses propres clients en toute conformité avec les réglementations française et européenne, ainsi qu'avec les

recommandations de la CNIL, et à permettre aux personnes concernées d'exercer leurs droits d'accès, de rectification et d'opposition auprès de ses services.

ARTICLE 21 : DONNEES PERSONNELLES

Dans le cadre de l'exécution du présent Contrat Cadre et des services associés, MONEXT, en sa qualité de responsable de traitement, est amené à collecter, traiter, conserver, archiver et supprimer des données personnelles, dans les conditions ci-dessous définies. Les orientations de MONEXT relatives à la protection des données personnelles sont également décrites dans sa Politique des données personnelles disponible sur demande.

Il est expressément convenu que les termes non spécifiquement définis au sein du présent Contrat Cadre prennent le sens défini par le Règlement Général sur la Protection des Données Personnelles (RGPD) 2016/679 du 27 Avril 2016.

21.1. Les Données Personnelles traitées par MONEXT

Catégories de données personnelles traitées par MONEXT :

Sont principalement traitées, dans le cadre de la relation contractuelle ou commerciale avec le Client, les catégories de données personnelles suivantes :

- données personnelles déclaratives : c'est-à-dire celles que MONEXT peut être amené à recueillir directement auprès du Client ou celles collectées indirectement auprès de tiers avec lesquels MONEXT a un lien contractuel ;
- données personnelles liées au fonctionnement du service ;
- données personnelles provenant d'informations publiques ;
- données personnelles inférées ou calculées par MONEXT dans le cadre de ses obligations réglementaires.

Les informations relatives aux témoins ou traceurs de connexion (cookies) sont consultables dans la Politique des données personnelles ou sur le site de MONEXT.

Fondements justifiant la collecte de données personnelles :

Conformément à la réglementation relative à la protection des données, MONEXT collecte des données personnelles et met en œuvre un traitement respectant les droits de ses clients :

- sur la base de l'exécution du Contrat Cadre, pour respecter ses obligations légales ou règlementaires ;
- sur la base du consentement lorsque celui-ci est requis ;
- ou quand cela est justifié par ses intérêts légitimes.

Durée de conservation des données personnelles :

Les données personnelles sont conservées conformément à la durée nécessaire aux finalités pour lesquelles elles sont collectées, soit pendant la durée du Contrat Cadre augmentée des prescriptions légales, soit pour assurer le respect des obligations légales, réglementaires ou reconnues par la profession auxquelles MONEXT est tenu.

Les principales durées de conservation des données personnelles sont précisées dans la Politique des données personnelles.

Destinataires des données personnelles

Les données personnelles collectées par MONEXT, ainsi que les données personnelles recueillies auprès de tiers par MONEXT bénéficient d'un niveau de protection identique. À ce titre, elle s'assure que seules les personnes habilitées peuvent y accéder.

Les données peuvent être communiquées aux sociétés du groupe Crédit Mutuel Arkéa, à leurs prestataires, aux partenaires de MONEXT ainsi qu'aux autorités administratives ou judiciaires lorsque cette communication est nécessaire à l'exécution du Contrat Cadre ou autorisée par la loi.

MONEXT n'est pas responsable des traitements de données personnelles autorisés par le Client auprès de tiers tels que, par exemple, les applications d'agrégation de compte bancaire ou les réseaux sociaux. Il appartient au Client de se référer aux Politiques de protection des données de ces tiers pour vérifier les conditions des traitements réalisés ou exercer ses droits au titre de ces traitements.

21.2. Les Finalités des Traitements

Les données personnelles collectées seront utilisées pour :

- gérer la souscription et le fonctionnement du service, et au besoin, mettre en œuvre des actions de recouvrement ;
- classifier les clients en termes de risque, lutter contre la fraude et mettre en œuvre l'ensemble des obligations réglementaires (gestion de la fiscalité, lutte anti-blanchiment, abus de marché, lutte anti-corruption, échanges automatiques et obligatoires de renseignements relatifs aux comptes financiers...) ;
- réaliser des études statistiques et mener des actions d'optimisation de la relation commerciale en analysant les données collectées.

21.3. Les Mesures de Sécurité

La réglementation impose à MONEXT d'assurer un haut niveau de sécurité et de confidentialité sur les données personnelles de ses clients. La conservation, l'exploitation ou la transmission de ces données s'effectue ainsi dans le cadre de règles et procédures strictes.

MONEXT prend, au regard de la nature des données personnelles et des risques que présentent les traitements, les mesures techniques, physiques et organisationnelles nécessaires pour préserver la sécurité et la confidentialité des données personnelles et empêcher qu'elles ne soient déformées, endommagées ou que des tiers non autorisés y aient accès. MONEXT 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, MONEXT peut par exemple mettre en place des clauses types définies par la Commission Européenne afin d'encadrer les flux. Des mesures complémentaires de sécurité informatique peuvent également être mises en œuvre.

21.4. Exercice des Droits des Personnes Concernées

En matière de données personnelles, les personnes physiques dont les données font l'objet d'un traitement dans le cadre des présentes disposent, conformément à la règlementation applicable, d'une série de droits dédiés, tels que :

- Un droit d'accès, de rectification, d'opposition, de limitation, d'effacement et de portabilité de leurs données personnelles.
- Un droit à définir des instructions concernant la conservation, l'effacement et la communication de leurs données personnelles, après leur décès.
- Un droit de réclamation auprès de la CNIL.

Les demandes d'exercice de ces droits doivent être transmises à l'adresse suivante : paymentservices.rgpd@monext.net.

ARTICLE 22 : PROPRIETE INTELLECTUELLE

Le présent Contrat Cadre n'entraine aucun transfert de propriété d'une Partie au profit d'une autre. Chacune des Parties conservera la propriété des logiciels, ainsi que des méthodes, du savoir-faire et des outils, qui lui sont propres et/ou qui lui ont servi à exécuter ses prestations contractuelles ou qu'elle y aurait inclus à titre onéreux ou gratuit. MONEXT reste propriétaire de toutes les créations réalisées pour l'exécution du présent Contrat Cadre.

MONEXT déclare détenir, sur les matériels, les logiciels et les progiciels, les droits ou autorisations nécessaires pour fournir au Client les prestations, objet du Contrat Cadre.

Pour les besoins exclusifs du Contrat Cadre et dans les limites de sa durée, MONEXT accorde au Client, une licence d'utilisation sur les éléments mis à sa disposition dans le cadre de l'exécution du Contrat Cadre, non-exclusive, personnelle, et limitée, sans possibilité de sous-licencier, vendre, céder, distribuer ces droits. Le Client s'interdit de copier, décompiler ou modifier lesdits éléments.

Le Client déclare, pour sa part, détenir, les droits ou autorisations nécessaires pour utiliser les données qu'il transmet pour traitement, tel que prévu par le Contrat Cadre. MONEXT dispose sur ces données d'un droit d'usage gratuit, non exclusif, non cessible et non transmissible, valable pour la seule durée et aux seules fins d'exécution du Contrat Cadre. En tout état de cause, le Client autorise expressément MONEXT à utiliser ses noms commerciaux, logos et marques dans le cadre de prestations de personnalisation ou promotionnelles et/ou à titre de référence commerciale.

Le Client garantit MONEXT contre toute action en contrefaçon, réclamation ou revendication relative à l'utilisation de ces éléments.

ARTICLE 23 : RESPONSABILITE DE MONEXT

23.1. La responsabilité de MONEXT ne saurait en aucun cas être engagée notamment :

- en cas de 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 ;
- en cas de force majeure, telle que définie par le code civil ;
- pour tout manquement du Client aux obligations définies au présent Contrat Cadre ;
- du fait de l'utilisation des codes confidentiels et/ou des identifiants du Client, sauf preuve contraire apportée par ce dernier, toute utilisation des identifiants ou codes confidentiels est réputée constituer une utilisation des espaces du Client et des services associés, ce que le Client déclare accepter expressément. En conséquence, le Client est réputé et demeure seul responsable de l'usage qui pourrait en être fait par un tiers et des risques y afférents ;
- en cas de manquement résultant directement ou indirectement d'une cause indépendante de la volonté de MONEXT, notamment d'une panne ou d'une indisponibilité totale ou partielle des réseaux téléphonique et Internet ou des systèmes globaux de traitement des données ;
- en cas de mauvaise utilisation par le Client des extranets et des services associés.

23.2. Il est expressément entendu qu'en tout état de cause, en cas de mise en jeu de la responsabilité de MONEXT, cette dernière ne saurait excéder six (6) fois le montant mensuel facturé par MONEXT au Client au titre du présent Contrat Cadre, calculé sur les douze (12) derniers mois précédent l'incident.

ARTICLE 24 : RECLAMATION

24.1. En cas de difficulté dans le fonctionnement du Compte ou pour formuler une réclamation, MONEXT peut être contactée :

- par courrier à : **MONEXT - Services de Paiement**, 260, rue Claude Nicolas Ledoux Pôle d'Activités d'Aix-en-Provence CS 60507 13593 Aix-en-Provence Cedex 3 ;
- par e-mail à l'adresse : paymentservices.info@monext.net.

24.2. Toute réclamation concernant le Contrat Cadre doit être adressée à MONEXT par écrit dans un délai maximum de six (6) mois à compter de la date de l'opération contestée, sous peine de forclusion.
Ce délai est réduit à quinze (15) jours calendaires à compter de la date de débit du Compte résultant d'une opération de paiement non garantie, notamment en cas d'impayé.

24.3. Les réponses formulées par MONEXT pourront être communiquées au Client sur support papier ou électronique :

- pour toute demande concernant le Compte ou les services de paiement : dans un délai maximal de quinze (15) jours (pour des raisons indépendantes de la volonté de MONEXT, ce délai pourra être porté à trente-cinq [35] jours) ;
- pour tout autre sujet : dans un délai maximal de 2 mois.

24.4. En cas de réclamation et si aucun accord n'a pu être trouvé ou en l'absence de réponse dans les délais précités, le Client peut saisir, par écrit, le médiateur de MONEXT, chargé de recommander des solutions aux litiges avec les Clients, à l'adresse suivante : **Médiateur de l'AFEPAME**, 36 rue Taitbout, 75009 Paris.
Le médiateur est tenu de statuer dans un délai de deux (2) mois à compter de sa saisine. La procédure de médiation est gratuite pour le Client qui conserve cependant la charge de ses propres frais, notamment de déplacement ou liés à la rémunération du conseil qu'il choisirait de s'adjoindre.
Ni MONEXT, ni le Client n'est tenu de proposer ou demander la saisine du médiateur avant toute action judiciaire.
Par ailleurs, MONEXT ou le Client, que la décision du médiateur ne satisferait pas, peut saisir la juridiction compétente à l'issue de la procédure de médiation.

ARTICLE 25 : CONVENTION DE PREUVE

De convention expresse les enregistrements électroniques émanant notamment des systèmes d'information de MONEXT, de ses prestataires ou des Schémas, constituent la preuve des opérations de paiement remises au Client. En cas de conflit, ces enregistrements électroniques prévaudront sur ceux produits par le Client, sauf si le Client apporte la preuve de leur absence de fiabilité ou d'authenticité.

ARTICLE 26 : NON RENONCIATION

Le fait pour l'une ou l'autre Partie de ne pas exiger à un moment quelconque l'exécution stricte d'une disposition du présent Contrat Cadre 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 27 : INCESSIBILITE

Le Contrat Cadre ne peut faire l'objet d'une cession totale ou partielle par le Client, à titre onéreux ou gratuit, sans l'accord exprès et écrit de MONEXT. En cas de manquement à cette interdiction du fait du Client, outre la résiliation immédiate des présentes, la responsabilité de ce dernier pourra être engagée par MONEXT.

ARTICLE 28 : FORCE MAJEURE

Dans l'hypothèse où l'exécution, par MONEXT, de ses obligations au titre du Contrat Cadre serait empêchée ou deviendrait exagérément onéreuse du fait de circonstances échappant raisonnablement à son contrôle, telles que notamment, outre les cas de force majeure tels que définis par le code civil, un incendie, une guerre (qu'elle soit déclarée ou non), une grève (interne ou externe) ou une inondation, MONEXT en informera le Client par tout moyen.
Durant la durée de l'événement affectant l'exécution de ses obligations par MONEXT, les obligations respectives des Parties seront suspendues. MONEXT informera le Client par tout moyen dès que la reprise du Contrat Cadre pourra être raisonnablement envisagée.

ARTICLE 29 : INDEPENDANCE DES STIPULATIONS CONTRACTUELLES

Les titres des différents articles du présent Contrat n'ont été adoptés qu'à titre de convenance et ne sauraient avoir une quelconque influence ou affecter d'une manière quelconque le sens ou le contenu de tout terme, stipulation, engagement ou condition de celui-ci.
Si l'une quelconque des stipulations des présentes est tenue pour nulle ou sans objet, elle sera réputée non écrite et n'entraînera pas la nullité des autres stipulations. Si une ou plusieurs stipulations des présentes deviennent caduques ou sont déclarées comme telles en application d'une loi, d'un règlement ou à la suite d'une décision définitive rendue par une juridiction compétente, les autres stipulations conserveront leur force obligatoire et leur portée. Les stipulations déclarées nulles et non valides seront alors remplacées par les stipulations qui se rapprocheront le plus quant à leur sens et à leur portée des stipulations initialement convenues.

ARTICLE 30 : LANGUE DU PRESENT CONTRAT CADRE

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

ARTICLE 31 : LOI APPLICABLE / TRIBUNAUX COMPETENTS

Le présent Contrat Cadre 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 Cadre est soumis à la compétence exclusive des tribunaux compétents du ressort de la Cour d'appel d'Aix-en-Provence, y compris les procédures tendant à obtenir des mesures d'urgence ou conservatoires, en référé ou sur requête.

ANNEXE 1 : SPECIFICITES DU SCHEMA DE CARTES CB

1. DEFINITION DU SYSTEME

Le système de paiement par Carte "CB" repose sur l'utilisation de Cartes "CB" ou agréées "CB" pour le paiement d'achats de biens ou de prestations de services auprès des Accepteurs adhérant au Système "CB" et cela dans le cadre des seules dispositions et procédures définies ou homologuées par le GIE "CB". Le GIE "CB" intervient notamment, pour des raisons sécuritaires, dans les modifications du seuil de demande d'autorisation, la suppression de l'acceptabilité de certaines Cartes "CB" ou de Cartes agréées "CB" et la suspension de l'adhésion au Système "CB". Il établit des conditions générales d'adhésion, l'Acquéreur "CB" définissant certaines conditions particulières de fonctionnement. Lorsque MONEXT représente le GIE "CB", le terme de "représentation" ne concerne que l'ensemble des conditions techniques d'acceptation de la Carte "CB" et de Cartes agréées "CB" et de remise des opérations à l'Acquéreur "CB", et non la mise en jeu de la garantie du paiement visée à l'article « Garantie du Paiement » des Conditions Générales.

2. DISPOSITIONS RELATIVES AUX CARTES CB ET APPLICATION DE PAIEMENT CB

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

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

3. TRANSMISSION DES ENREGISTREMENTS

Le Client doit transmettre à MONEXT les enregistrements des opérations de paiement, dans les délais prévus dans les Conditions Particulières. Au-delà d'un délai maximum de six (6) mois après la date de l'opération, l'encaissement des opérations de paiement n'est plus réalisable dans le cadre du Schéma de cartes CB.

4. EQUIPEMENT ELECTRONIQUE AGREE

Le Client doit utiliser obligatoirement un Equipement Electronique 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 le Groupement des Cartes Bancaires CB). A cet effet, le Client peut prendre information de la date de fin de vie auprès de la documentation du Groupement des cartes Bancaires CB (notamment en consultant son site internet).

5. MESURE DE PREVENTION ET DE SANCTION MISE EN ŒUVRE PAR LE GIE CB

5.1. En cas de manquement aux dispositions du présent Contrat Cadre concernant les mesures de sécurité ou en cas de taux d'impayés constaté anormalement élevé (notamment dans les hypothèses où le Client ventile 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 l'acceptation des Cartes CB du Client. Cette suspension intervient s'il n'est pas remédié aux problèmes constatés dans un délai de trois (3) mois suivant la mise en demeure d'y remédier.
- Ce délai peut être ramené à quelques jours en cas d'urgence et à un (1) mois au cas où le Client aurait déjà fait l'objet d'une mesure de suspension dans les vingt-quatre (24) mois précédant l'avertissement.
- La suspension est motivée et notifiée par l'envoi d'une lettre recommandée avec avis de réception. Cette suspension prend effet deux (2) jours francs à compter de la première présentation du courrier de notification.
- la radiation de l'adhésion du Client 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 motivée et notifiée par l'envoi d'une lettre recommandée avec avis de réception.

5.2. Le Client s'engage alors à restituer les dispositifs techniques et sécuritaires et les documents en sa possession dont MONEXT est propriétaire et à retirer immédiatement de son établissement tout signe d'acceptation des Cartes du Schéma CB.

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

A l'expiration de ce délai, le Client peut demander la reprise d'effet du Contrat Cadre 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 MONEXT ou par le GIE CB et portant sur le respect des bonnes pratiques et des mesures de sécurité visées aux présentes.

ANNEXE 2 : PAIEMENT DE PROXIMITE

1. PERIMETRE D'APPLICATION

Cette annexe s'applique au paiement par carte en vente de proximité : tout paiement réalisé au moyen d'un Equipement Electronique dans le point de vente du Client.

2. MESURES DE SECURITE

2.1. Le Client s'engage à utiliser obligatoirement un Système d'Acceptation conforme aux spécifications définies par les Schémas, aux procédures de sécurisation des ordres de paiement donnés par les titulaires de Cartes et aux stipulations du Référentiel sécuritaire accepteur, annexé aux présentes.

2.2. Lors du paiement, le Client s'engage à :

2.2.1. Vérifier l'acceptabilité de la Carte, c'est-à-dire :

- la marque, la catégorie de carte ou l'application de paiement du Schéma de cartes concerné par l'acceptation ;
- le cas échéant l'hologramme sauf pour les Cartes ne le prévoyant pas ;
- la puce sur les Cartes et catégorie de cartes lorsqu'elle y est prévue par le Schéma de cartes ;
- les marque et catégorie de la Carte définies dans les Conditions particulières ;
- la période de validité (fin et éventuellement début).

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

- après la lecture de la puce des Cartes lorsqu'elle est présente :
  - permettre le contrôle du code confidentiel ou des données de sécurité personnalisées 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 ou qu'elle ne fonctionne pas, 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.

2.2.3. Contrôler le numéro de la Carte par rapport à la dernière liste des Cartes faisant l'objet d'un blocage ou d'une opposition transmise par MONEXT.

2.2.4. Lorsque la puce le demande à l'Equipement Electronique, faire composer par le titulaire de la Carte, dans les meilleures conditions de confidentialité, son code confidentiel ou ses données de sécurité personnalisées ou mettre en œuvre la méthode d'authentification prévue et adaptée à la technologie applicable. La preuve de la frappe du code confidentiel ou de la vérification des données de sécurité personnalisées est apportée par le certificat qui doit figurer sur le ticket émis par le TPE.

2.2.5. Lorsque le code confidentiel ou les données de sécurité personnalisées ne sont pas vérifiés, l'opération n'est réglée que sous réserve de bonne fin d'encaissement, même en cas de réponse positive à la demande d'autorisation.
2.2.6. "Mode sans contact" : en cas d'opération en mode sans contact permise par l'Equipement Electronique, l'opération de paiement est garantie même si le code confidentiel n'est pas vérifié ou si les données de sécurité personnalisées ne sont pas vérifiées, sous réserve du respect de l'ensemble des autres mesures de sécurité à votre charge.
2.2.7. Obtenir une autorisation d'un montant identique à l'opération :
• 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 de vente, dépasse celui du seuil de demande d'autorisation fixé dans les Conditions Particulières, et ceci quelle que soit la méthode d'acquisition des informations,
• lorsque l'Equipement Electronique ou la Carte à puce déclenche une demande d'autorisation, indépendamment du seuil de demande d'autorisation fixé dans les Conditions Particulières.
A défaut, l'opération ne sera pas garantie, même pour la fraction autorisée ou correspondant au montant du seuil de demande d'autorisation.
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 de vente.
2.2.8. Faire signer le Ticket TPE :
• Dans tous les cas où l'Equipement Electronique le demande.
• Lorsque le montant de l'opération est supérieur à 1 500 euros.
2.2.9. 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.
2.2.10. Remettre au titulaire de la Carte l'exemplaire du Ticket TPE qui lui est destiné.
2.3. Après une opération de paiement, le Client doit :
2.3.1. Transmettre à MONEXT 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. Le Client ne doit transmettre que les enregistrements électroniques des opérations pour lesquelles un ordre de paiement a été donné à son profit. Toute opération ayant fait l'objet d'une autorisation doit être obligatoirement remise à MONEXT.
2.3.2. Archiver et conserver, à titre de justificatif, pendant la durée requise par les règles du Schéma de cartes 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.
2.3.3. Communiquer, sur demande de MONEXT et dans les délais prévus dans les Conditions Particulières, tout justificatif des opérations de paiement.
2.4. Le Client s'engage à ne stocker, sous quelque forme que ce soit, aucune des données de paiement sensibles liées à la carte ci-après :
• le cryptogramme visuel ;
• la piste magnétique dans son intégralité ;
• le code confidentiel.

ANNEXE 3 : VENTE A DISTANCE SECURISEE

ANNEXE 3.1 STIPULATIONS SPECIFIQUES

1. PERIMETRE D'APPLICATION

Cette annexe s'applique à tout Client utilisant des moyens électroniques ou non pour vendre à distance des biens et des services et qui souhaite recevoir des paiements à distance en contrepartie d'actes de vente ou de fournitures de prestation de service qu'il réalise lui-même, et en particulier :
• au paiement en vente à distance : tout paiement réalisé au moyen d'un Terminal de Paiement Electronique (non virtuel) et faisant suite au recueil à distance (courrier, téléphone, fax…) de données Carte ;
• au paiement sur Internet : tout paiement réalisé via une interface informatique (ou TPE virtuel) et faisant suite au recueil à distance (courrier, téléphone, fax…) de données Carte.

2. MESURES DE SECURITE

2.1. Le Client s'engage à :
• utiliser obligatoirement un Système d'Acceptation conforme aux spécifications définies par les Schémas, aux procédures de sécurisation des ordres de paiement donnés à distance par les titulaires de Cartes, ainsi qu'aux stipulations du Référentiel sécuritaire accepteur et du Protocole 3D Secure, tous deux annexés au Contrat Cadre ;
• lutter contre la fraude dont son point d'acceptation pourrait être victime, notamment en mettant en œuvre sans délai les mesures sécuritaires appropriées.

2.2. Lors du paiement, le Client s'engage à :
2.2.1. Appliquer les procédures décrites dans les Conditions Particulières, notamment à l'article « Conditions liées à la Garantie de Paiement ».
2.2.2. Obtenir un justificatif d'acceptation matérialisant les contrôles effectués et la validité de l'ordre de paiement.
2.2.3. 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 à l'article « Définitions » des Conditions Générales.
2.2.4. Demander obligatoirement une autorisation en cas d'acceptation d'un ordre de paiement transmis par Internet.
2.2.5. Obtenir une autorisation d'un montant identique à l'opération.
2.2.6. Contrôler (ou faire contrôler) le cryptogramme visuel donné par le titulaire de la Carte.
2.3. Après une opération de paiement, le Client s'engage à :
2.3.1. Transmettre à MONEXT 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. Le Client ne doit transmettre que les enregistrements électroniques des opérations pour lesquelles un ordre de paiement a été donné à son profit. Toute opération ayant fait l'objet d'une autorisation doit être obligatoirement remise à MONEXT.
2.3.2. Envoyer au titulaire de la Carte, lorsqu'il le demande, un ticket précisant, entre autres, le mode de paiement par Carte utilisée.
2.3.3. Communiquer, à la demande de MONEXT et dans les délais prévus dans les Conditions Particulières, tout justificatif des opérations de paiement.

2.4. L'ensemble des mesures de sécurité énumérées dans la présente annexe pourront être modifiées et complétées pendant toute la durée du présent Contrat Cadre, selon la procédure prévue à l'article « Modifications » des Conditions Générales.

ANNEXE 3.2 PROTOCOLE 3D SECURE

Utilisation du protocole de sécurisation des paiements sur internet 3D Secure (déployé également sous les appellations commerciales « Verified by Visa » et « MasterCard SecureCode ») :
Pour bénéficier de la garantie de paiement le Client doit être enregistré au programme 3D-Secure et respecter l'ensemble de la procédure décrite au sein de la présente annexe ; la banque du titulaire de Carte devant authentifier le titulaire de Carte et autoriser la transaction.

1. PRINCIPE

Le protocole 3D Secure n'est applicable que pour les paiements à distance effectués par Cartes CB, Visa ou MasterCard sur Internet, et pour lesquels le titulaire de Carte saisit, lui-même, ses données Carte.
Le principe consiste à demander à l'acheteur, en complément de ses données de Carte de paiement, un code d'authentification à usage unique (reçu le plus souvent par SMS) afin de s'assurer qu'il est bien le titulaire de la Carte.
La transaction estampillée 3D Secure bénéficie, dans la plupart des cas, d'un transfert de la responsabilité du Client vers la banque du titulaire de Carte en cas de répudiation du paiement, cas où le titulaire de Carte nie être l'auteur du paiement.
Pour le Client, ce dispositif a plusieurs effets immédiats sur la gestion de ses transactions :

- Diminution significative du risque d'impayé ;
- Diminution du temps consacré à la vérification des commandes ;
- Transfert aux banques émettrices de la responsabilité des paiements frauduleux.

2. PARAMETRAGE

Si le Client ne souhaite pas mettre en œuvre le protocole 3D Secure ou s'il souhaite l'utiliser de manière modulable, il supporte seul les risques relatifs à l'augmentation des impayés et les éventuelles pénalités liées à la fraude facturées par CB, Visa et MasterCard et renonce ainsi à la garantie de paiement.
En cas d'utilisation du dispositif 3D Secure en mode modulable, MONEXT fournira une deuxième référence de contrat accepteur, il reviendra alors au Client d'utiliser la référence de contrat accepteur 3D Secure pour traiter les transactions 3D Secure et la seconde référence pour les transactions non 3D Secure.

3. LIMITATIONS

Le protocole 3D Secure, et le transfert de responsabilité qui en découle, comportent certaines exclusions dans leurs périmètres d'application qui peuvent évoluer dans le temps. Les exclusions actuelles listées ci-dessous sont données à titre indicatif :

- Les Cartes non éligibles par décision des Schémas CB, Visa et MasterCard : les Cartes prépayées ainsi que les Cartes privatives d'achat et de retrait ;
- Les transactions que vous réalisez à partir des données Carte transmises par téléphone, télécopie, courriel ou courrier ;
- Les transactions réalisées sans la saisie du cryptogramme visuel de la Carte comme c'est le cas dans le cadre de paiements récurrents ou fractionnés et plus généralement de transactions réalisées à partir d'un porte-monnaie électronique (e-wallet) ;
- Une indisponibilité technique entre le Prestataire de Solution de Paiement, MONEXT, la banque du titulaire de Carte ou les Schémas CB, Visa et MasterCard empêchant l'application du dispositif 3D Secure.

ANNEXE 4 : NOTICE D'INFORMATION RELATIVE AUX CONTRATS CONCLUS SUITE A UN ACTE DE DEMARCHAGE BANCAIRE OU FINANCIER OU A UNE ENTREE EN RELATION A DISTANCE

1. DEFINITIONS

1.1. Démarchage bancaire et financier

Le démarchage bancaire ou financier consiste en :

- une prise de contact non sollicitée, par quelque moyen que ce soit, avec une personne physique ou morale déterminée, en vue d'obtenir, de sa part, un accord sur la fourniture des services de paiement de MONEXT ;
- un déplacement du démarcheur de MONEXT, en vue des mêmes fins, au siège social du client ou dans tous lieux autres que ceux de MONEXT, quelle que soit la personne à l'initiative de la démarche.

1.2. Entrée en relation à distance

L'Entrée en Relation à Distance consiste pour MONEXT à conclure, avec son client, le présent contrat cadre de services de paiement totalement à distance, c'est-à-dire, hors la présence physique et simultanée des parties, en utilisant exclusivement une ou plusieurs techniques de communication à distance (courrier, téléphone, Internet, fax...) du stade de la relation précontractuelle jusqu'à la conclusion du contrat.
Seule la conclusion du présent contrat cadre de services de paiement est concernée et non les opérations qui en découlent. Dans le cadre de la relation contractuelle, le client peut changer les techniques de communication à distance utilisées.

2. L'INFORMATION

2.1. Information précontractuelle

Le client est informé des caractéristiques des services de paiement faisant l'objet de la proposition de contracter au moyen des documents d'information prévus par la réglementation et/ou d'une fiche d'information commerciale, ainsi que par les documents présentant les Conditions Générales et Tarifaires qui lui sont applicables. Ces documents, rédigés en français, sont, remis en mains propres, adressés au client ou bien encore disponibles sur le site Internet de MONEXT, selon la technique de communication utilisée.

2.2. Contrat

Le contrat relatif aux services de paiement proposé par MONEXT peut être conclu, dans ses locaux, au siège social du client ou en tout autre lieu convenu avec lui. Lorsqu'il est conclu à distance, le lieu de conclusion du contrat est celui du lieu de situation de MONEXT qui tient le compte de paiement du client.
Le contrat est rédigé en français et est soumis au droit français.
Le contrat est communiqué au client préalablement à tout engagement de sa part et se compose :

- des Conditions Particulières contenant les modalités spécifiques du compte de paiement ainsi que les modalités de conclusion du contrat ;
- des Conditions Générales applicables au compte de paiement et aux services de paiement souscrits. Elles complètent les Conditions Particulières. Elles précisent en particulier les droits contractuels de résiliation, les procédures de réclamation…
- de tout document supplémentaire prévu, le cas échéant, au contrat pour sa conclusion, ainsi qu'un bordereau de rétractation.

Lorsque la technique de communication ne permet pas de transmettre les documents susvisés avant la conclusion du contrat demandée par le client, les documents d'information et les conditions contractuelles lui sont adressés par écrit immédiatement après la conclusion du contrat. À tout moment au cours de la relation contractuelle, le client qui en fait la demande peut recevoir les conditions contractuelles sur un support papier.

2.3. Droit de rétractation

Le client dispose d'un droit de rétractation en cas de conclusion d'un contrat avec MONEXT à la suite d'un acte de démarchage ou dans le cadre d'une entrée en relation à distance. Le délai de rétractation est de 14 jours calendaires révolus. Le délai commence à courir :

- soit à compter du jour où le contrat est conclu ;
- soit à compter de celui où l'intéressé est informé de la conclusion du contrat.

2.4. Exception
Le droit de rétractation ne s'applique pas aux contrats exécutés intégralement par les deux parties à la demande expresse du client, avant que ce dernier n'exerce son droit de rétractation.

3. L'EXECUTION DU CONTRAT
Si le présent contrat cadre de services de paiement est conclu à distance, il ne peut recevoir de commencement d'exécution avant l'arrivée du terme du délai de rétractation sans que le client en ait fait la demande. Cette demande peut résulter de la toute première utilisation des services de paiement objet du contrat conclu, réalisée à l'initiative du client.

ANNEXE 5 : SECURITE

ANNEXE 5.1 REFERENTIEL SECURITAIRE 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 la Carte doit être hébergé dans un local sécurisé et répondre aux exigences édictées par les règles et recommandations de la CNIL.
Les petits matériels ou supports informatiques sensibles doivent être rendus inaccessibles à des tiers en période de non-utilisation. Notamment, les cartouches de sauvegarde doivent être stockées dans un coffre.
Dans le cas où ces petits matériels ou supports informatiques sensibles ne sont plus opérationnels, ils doivent être obligatoirement détruits et la preuve de leur destruction doit être établie.
La politique d'accès aux locaux sensibles doit être formalisée et les procédures doivent être établies et contrôlées.

Exigence 4 (E4) : Assurer la protection logique du 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 la Carte ne peuvent être utilisées que pour exécuter l'ordre de paiement et pour traiter les réclamations. Le cryptogramme visuel d'un titulaire de Carte ne doit en aucun cas être stocké par le Client.
Les données bancaires et à caractère personnel relatives à une opération de paiement, et notamment les données du titulaire de la Carte doivent être protégées lors de leur stockage et lors de leur routage sur les réseaux internes et externes au site d'hébergement conformément aux dispositions de la règlementation française et européenne et aux recommandations de la CNIL. Il en est de même pour l'authentifiant du Client 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 5.2 PCI DSS ET RISQUES ACQUEREURS

1. REGLES A RESPECTER

Le Client doit respecter les dispositions de l'Annexe « Référentiel Sécuritaire Accepteur » et les exigences de sécurité PCI DSS (se référer également au site officiel : https://fr.pcisecuritystandards.org/minisite/env2/).
Le Client doit se conformer aux obligations, règles et directives applicables émises respectivement par les Schémas de cartes CB, Visa et MasterCard, notamment les programmes « Cardholder Information Security Program » (CISP) et « Account Information Security Program » (AISP) de Visa ainsi que le programme « Site Data Protection Program » (SDP) de MasterCard dont certaines règles, de portée internationale, sont rédigées en anglais.
Des informations complémentaires sont disponibles sur les sites internet suivants :
- https://usa.visa.com/partner-with-us/pci-dss-compliance-information.html ;
- https://www.mastercard.us/en-us/about-mastercard/what-we-do/rules.html.

En conséquence, le Client s'interdit 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 »).
Le Client doit justifier auprès de MONEXT la bonne réalisation de ses obligations et en fournir les documents associés sur simple demande.

2. RECOURS A 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 de paiement sensibles liées à l'utilisation des cartes, le Client doit s'assurer que ces derniers s'engagent à respecter le référentiel de sécurité PCI DSS et les mesures du « Référentiel Sécuritaire Accepteur ». Le Client doit tenir MONEXT informé du nom et des coordonnées des sous-traitants auxquels il fait appel dans le cadre de la mise en œuvre de sa solution de paiement.

3. CLAUSE D'AUDIT

MONEXT et/ou les Schémas peuvent faire procéder, dans les locaux du Client ou ceux de ses prestataires, à la vérification par un tiers indépendant du respect des engagements définis au présent Contrat Cadre, figurant notamment 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 Cadre.
Le Client autorise la communication des rapports d'audit à MONEXT, ainsi qu'aux Schémas mentionnés sur les Cartes qu'il accepte, telles que définies aux présentes.
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 du Client à ses engagements, chacun des Schémas pourra procéder à une suspension de l'adhésion, voire à une radiation du Schéma telle que prévue dans les Conditions Générales.
Le Client est tenu d'informer immédiatement MONEXT et de suivre intégralement ses instructions s'il 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. Le Client fournit dans ce cas sans délai à MONEXT, de sa propre initiative ou à la demande de MONEXT, toutes les informations (telles que les données de transaction) en vue du traitement du dossier.
Le Client est tenu d'apporter son concours à l'enquête et de suivre intégralement toutes les instructions de MONEXT si cette dernière soupçonne ou constate que des données de transaction erronées, falsifiées ou volées ont été utilisées dans le point de vente du Client, ou l'utilisation de données compromises ou d'autres actes et/ou transactions frauduleux. Le Client autorise MONEXT à partager les résultats de l'enquête avec des tiers tels que les Schémas.
Le Client 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.
MONEXT peut aussi être amené à bloquer les fonds « suspects ».
Le Client accepte d'être facturé des éventuelles pénalités qui pourraient lui être appliquées par les Schémas en cas de compromission de données du fait de manquements, d'actes ou de faits relevant de sa responsabilité notamment après un audit.

4. INVENTAIRE DES TERMINAUX DE PAIEMENT

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

5. ENTREE EN RELATION ET SUIVI DE LA RELATION

Le Client doit informer MONEXT, sur demande de cette dernière :
- 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 Cadre et pouvant impacter ses déclarations initiales.

6. ACTIVITES ILLEGALES

Le Client déclare ne pas exercer une activité de type : pornographie infantile, vente illégale de drogues ou tabacs, vente de marchandises contrefaites ou commercialisées en violation des droits de propriétés, pornographie « agressive » (bestialité, viol, mutilation…) ou plus généralement toute autre activité punie par la loi.

7. IMPAYES ET RISQUES DE FRAUDE

7.1. Impayés

Le Client s'engage à respecter les dispositions des programmes « Visa Chargeback Monitoring Program » (VCMP) et MasterCard « Excessive Chargeback Programme » (ECP), visant à limiter le ratio d'impayés des commerçants. Certaines règles de ces programmes sont de portée internationale et sont rédigées en anglais.
Des informations complémentaires sont disponibles dans les documents suivants :
- Visa Core Rules and Visa Product and Service Rules (https://www.visa.co.uk/about-visa/visa-in-europe.html#2)
- MasterCard Security Rules and Procedures (https://www.mastercard.us/en-us/about-mastercard/what-we-do/rules.html).
En cas d'alerte en provenance des Schémas, dans le cadre de ces programmes, vous vous engagez à mettre en œuvre les solutions que nous vous proposerons, telle que l'activation du protocole 3D Secure, afin de réduire les impayés et le taux d'impayés au sein de votre point de vente.

7.2. Risques de fraude Visa et MasterCard

Le Client s'engage à respecter les dispositions des programmes Visa « Visa Fraud Monitoring Program » (VFMP) et MasterCard « Fraud Loss Control Standard » (FLC) visant à limiter la fraude des commerçants. Certaines règles de ces programmes sont de portée internationale et sont rédigées en anglais.
Des informations complémentaires sont disponibles dans les documents suivants :
- Visa Core Rules and Visa Product and Service Rules (https://www.visa.co.uk/about-visa/visa-in-europe.html#2) ;
- MasterCard Security Rules and Procedures (https://www.mastercard.us/en-us/about-mastercard/what-we-do/rules.html).
En cas d'alerte en provenance des Schémas, dans le cadre de ces programmes, le Client s'engage à mettre en œuvre sans délai les solutions proposées par MONEXT, telle que l'activation du protocole 3D Secure, afin de réduire la fraude et le taux de fraude au sein de son point de vente.

7.3. Risques de fraude CB

Le Client s'engage à respecter les dispositions du programme CB visant à limiter la fraude en vente à distance des commerçants. En cas d'alerte en provenance du Schéma CB, dans le cadre de ce programme, le Client s'engage à mettre en œuvre les solutions proposées par MONEXT, telle que l'activation du protocole 3D Secure, afin de réduire la fraude et le taux de fraude au sein de son point de vente.

7.3.1. Définitions du programme CB

- Transaction frauduleuse : toute transaction qui n'est pas faite par le titulaire légitime de la carte et qui est formellement contestée par lui, avec une Carte opposée ou non, toute transaction réalisée au moyen d'un numéro d'identifiant carte qui n'est attribué à aucun titulaire de Carte ou toute transaction effectuée sur une carte en opposition auprès du GIE CB.
- Taux de fraude : calculé sur la base des déclarations de fraude VAD CB/CB faites par les émetteurs, auxquels sont ajoutés les impayés motif 45 (Transaction contestée) qui n'ont pas fait l'objet d'une déclaration de fraude.
- Taux de fraude anormalement élevé (en montant) : taux de fraude qui excède de manière significative les valeurs moyennes observées pour l'ensemble des banques membres du GIE CB.
- Taux d'impayés : rapport entre le nombre d'impayés émis par le Client pour des opérations VAD CB/CB et le nombre d'opérations VAD CB/CB qu'il a acceptées. La date de référence de chaque impayé est la date locale de l'opération de la transaction initiale.
- Taux d'impayés anormalement élevé (en nombre) : taux d'impayés qui excède de manière significative les valeurs moyennes observées pour l'ensemble des banques membres du GIE CB.

7.3.2. Critères d'entrée dans le programme CB

Seules les transactions CB/CB sont considérées.

1.1.1.1. Critères relatifs au taux de fraude (en montant)

- Le taux de fraude mensuel du Client excède un (1) % du montant de son chiffre d'affaires cartes.
- Le montant mensuel de sa fraude est supérieur à soixante-dix milles (70 000) euros.
- Le nombre mensuel des opérations frauduleuses est supérieur à cent (100).
- Seules les fraudes n'impactant pas nos porteurs de cartes sont prises en compte.

Ces critères sont cumulatifs et doivent être constatés durant 4 mois consécutifs.

1.1.1.2. Critères relatifs au taux d'impayés (en nombre)

- Le taux d'impayés mensuel du Client excède deux (2) % du nombre des opérations cartes acceptées par ce dernier.
- Le nombre d'impayés mensuel est supérieur à deux cents (200).
- Seuls les impayés n'impactant pas nos porteurs de cartes sont pris en compte.

Ces critères sont cumulatifs et doivent être constatés durant quatre (4) mois consécutifs.

Le taux, que ce soit de fraude ou d'impayés, du mois M est calculé à la fin du mois M+2.

7.3.3. Conséquences de l'entrée dans le programme CB

7.3.3.1. Mesures déclenchées par un taux de fraude anormalement élevé

En cas de déclenchement du programme, le Client a l'obligation de mettre en œuvre 3D Secure pour au moins trois (3) % des transactions VAD qu'il accepte, et ce dans un délai maximum de six (6) mois à compter de la notification adressée au Client lors de son entrée dans le programme.

A l'issue de ce délai de six (6) mois, à défaut de mise en œuvre de la mesure précitée, le Client se voit appliquer des pénalités calculées comme suit : cinq milles (5 000) euros par mois durant les trois (3) premiers mois, puis incrémentation de mille (1 000) euros par mois supplémentaire, étant précisé que le montant des pénalités est plafonné à dix (10 000) euros par mois. Le fait de repasser en-dessous des seuils ci-avant définis ne dispense pas de la mise en œuvre de 3D Secure.

Les pénalités cessent lorsque le Client met en œuvre 3D Secure pour au moins trois (3) % des transactions VAD CB/CB qu'il accepte.

7.3.3.2. Mesures déclenchées par un taux d'impayés anormalement élevé

En cas de déclenchement du programme, le Client entre dans une période dite d'observation d'une durée de trois (3) mois à compter de la fin de la période de quatre (4) mois durant laquelle les critères de déclenchement du programme ont été constatés. Ladite période d'observation doit permettre au Client de faire redescendre son taux d'impayés mensuel en-dessous de deux (2) % ou le nombre des impayés mensuels qu'il émet en-dessous de deux cents (200).

A l'issue de ce délai de trois (3) mois, à défaut d'avoir un taux d'impayés ou un nombre d'impayés mensuels revenus à un niveau inférieur aux seuils ci-avant définis, le Client se voit appliquer rétroactivement des pénalités à partir du cinquième mois, soit à compter du premier mois de la période d'observation.

Ces pénalités s'élèvent à cinquante (50) € par impayé émis. Sur ce montant, trente-cinq (35) € par impayé émis sont reversés à l'émetteur par le GIE CB.

Les pénalités cessent lorsque le taux d'impayés mensuel devient inférieur à un (1) % ou le nombre mensuel d'impayés inférieur à cent (100), et ce pendant trois (3) mois consécutifs.

7.3.3.3. Suspension de l'adhésion au Système CB

Si, à l'issue d'un délai de six (6) mois d'application des pénalités, le Client n'a toujours pas mis en œuvre 3D Secure pour au moins trois (3) % des transactions qu'il accepte ou n'a pas un taux d'impayés mensuel inférieur à un (1) % ou un nombre d'impayés mensuel inférieur à cent (100), le GIE CB peut procéder à la suspension de l'adhésion du Client au Schéma CB.

7.3.3.4. Changement d'acquéreur

Dans le cas où le Client visé par l'un de ces programmes change d'acquéreur, les exigences et pénalités ci-avant définies s'appliquent automatiquement et de manière identique au nouvel acquéreur.

7.3.3.5. Evolutions

Les critères relatifs au taux de fraude, au taux d'impayés ainsi que les conséquences du déclanchement du programme CB sont susceptibles d'évoluer. En cas d'évolution, MONEXT informera le Client des modifications par tous moyens.

7.3.4. Facturation des pénalités

Les pénalités appliquées par le GIE CB vous seront facturées.

8. ACTIVITES A HAUTS RISQUES

Le Client doit demander l'autorisation et obtenir l'accord préalable et écrit de MONEXT, avant d'exercer des activités à « hauts risques » telles que définies par les Schémas, notamment dans les documents « MasterCard Security Rules and Procedures » et « Visa Global Brand Protection Programme ».

Les domaines d'activités précisés ci-dessous sont donnés à titre indicatif et peuvent évoluer dans le temps :

- Cyberlocker proposant des services d'hébergement ou de téléchargement de données ;
- Fournisseur de Crypto-monnaie ;
- Grossiste en produits pharmaceutiques en vente à distance ou par e-commerce ;
- Détaillant de produits pharmaceutiques en vente à distance ou par e-commerce ;
- Agence de voyages en marketing direct ;
- Sites de télémarketing en vente à distance ou par e-commerce ;
- Sites de télémarketing pour adultes (« sexshop ») en vente à distance ou par e-commerce ;
- Sites pour adultes (vente de films, « streaming ») en vente à distance ou par e-commerce ;
- Vente de tabac et de produits de vapotage en vente à distance ou par e-commerce ;
- Vente de jeton, paris et jeux en ligne en vente à distance ou par e-commerce.

En cas de réponse favorable, le Client doit fournir à MONEXT les documents et informations demandés et autoriser MONEXT à débiter annuellement son compte des frais correspondants à l'enregistrement de son activité à « hauts risques » auprès des Schémas. Le montant de ces frais sera communiqué au Client, sur 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 », le Client sera alors considéré comme exerçant une activité à « hauts risques » et sera soumis à l'ensemble de ces obligations, notamment à un enregistrement de son activité à « hauts risques » auprès des Schémas ainsi qu'au paiement des frais correspondants.

9. PENALITES ET RESILIATION

En cas de manquement à l'une des obligations définies aux présentes, le Client s'expose à des pénalités en provenance des Schémas de cartes ainsi qu'à la résiliation du présent Contrat Cadre.

En cas de survenance d'un incident de sécurité majeur, notamment en cas de violation des données, le Client doit coopérer avec MONEXT et les autorités compétentes le cas échéant. Le refus ou l'absence de coopération de la part du Client pourra entrainer la résiliation du présent Contrat Cadre.

La résiliation du Contrat Cadre sera alors notifiée au Client par l'envoi d'une lettre recommandée, avec demande d'avis de réception. Son effet est immédiat.

ANNEXE 5.3 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 ont développé un ensemble de programmes de gestion de risques

auxquels les banques acquéreurs[1], les commerçants accepteurs[2] sont parties prenantes. Ce guide a pour objectif d'expliquer aux accepteurs la manière dont ils doivent appliquer les bonnes pratiques règlementaires.

1. 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 votre activité, votre réputation et augmente la confiance que vos clients placent en vous.

1.2. Qui devez-vous informer en cas de changement de mode de vente, ou de nature des biens, produits et services vendus ?

Le Contrat Cadre conclu avec MONEXT identifie votre activité principale selon la classification « Code NAF » normalisée de l'INSEE, et selon votre type de Commerce : proximité ou commerce en ligne.

Toute évolution de votre mode de vente devra faire l'objet d'une déclaration préalable à votre acquéreur. Par évolution du mode de vente, on entend :

- Modification du canal de vente (évolution de vente via TPE ou Automate vers vente sur internet).
- Modification des catégories de 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 et ne pourront pas faire l'objet d'un contrat d'acceptation de la part de MONEXT :

- Pornographie infantile ;
- Vente illégale de drogues, tabacs ;
- 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… ;
- Agrégateurs[3].

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

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

- Cyberlocker proposant des services d'hébergement ou de téléchargement de données ;
- Fournisseur de Crypto-monnaie ;
- Grossiste en produits pharmaceutiques en vente à distance ou par e-commerce ;
- Détaillant de produits pharmaceutiques en vente à distance ou par e-commerce
- Agence de voyages en marketing direct ;
- Sites de télémarketing en vente à distance ou par e-commerce ;
- Sites de télémarketing pour adultes (« sexshop ») en vente à distance ou par e-commerce ;
- Vente de tabac en vente à distance ou par e-commerce ;
- Sites pour adultes (vente de films, « streaming ») en vente à distance ou par e-commerce ;
- Paris et jeux en ligne en vente à distance ou par e-commerce.

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

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

1.4. Quels sont les différents niveaux d'exigence 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 vous détectez ou soupçonnez 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 votre acquéreur dans les plus brefs délais.

En cas de non-respect de la règlementation en vigueur ou de compromission de données importantes, des mesures pouvant donner lieu à des pénalités financières ou à la résiliation du Contrat Cadre pourraient être appliquées.

2. E-COMMERÇANTS

L'ensemble des informations précisées ci-après ne concernent que les commerçants Accepteurs sur internet.

2.1. Quelles sont vos obligations en tant que E-Commerçant ?

Dès lors que vous manipulez, transmettez ou stockez des données de cartes bancaires (et ce, quel que soit votre canal de paiement : point de vente physique, e-commerce, téléphone …) ou qu'un Fournisseur de Services s'en charge pour vous, vous êtes soumis à une mise en conformité à PCI DSS.

Les données de cartes bancaires concernées par PCI DSS sont :

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

2.2. 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 commerçants 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 terminal de paiement autonome, 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 :

[1] Les acquéreurs désignent les établissements bancaires

[2] Les accepteurs désignent les commerçants

[3] Un agrégateur est un commerçant qui traite les transactions d'un autre commerçant et les communique à sa banque acquéreur sans l'indiquer dans l'opération de paiement

Version du SAQ	Description	Proximité	E-Commerce	VàD (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 carte auprès d'un fournisseur de services conforme à PCI DSS. Aucune manipulation/transmission/ stockage de données de cartes sur l'environnement du commerçant 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	Paiement E-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 du commerçant 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 commerçants Accepteurs non pris en compte dans les descriptions des SAQ précédentes.	X	X	X

2.3. Qu'est-ce qu'un scan de vulnérabilités ?

Un scan de vulnérabilités est une revue de tous vos 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 vous assurera que votre 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

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

Si vous êtes éligible à un audit sur-site, vous devrez recourir aux services d'une société accréditée en tant que Qualified Security Assessor (QSA) qui validera chaque année la conformité PCI DSS de votre environnement.

La liste des sociétés accréditées QSA est accessible en ligne à l'adresse suivante :

https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors

2.5. Par où commencer ?

Le standard PCI DSS est accessible en ligne gratuitement sur le site suivant :

https://fr.pcisecuritystandards.org/minisite/env2/

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

S'il s'avère que certaines exigences PCI DSS ne sont pas opérationnelles, vous devrez 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://fr.pcisecuritystandards.org/_onelink_/pcisecurity/en2frfr/minisite/en/docs/Prioritized-Approach-v3_2.xlsx

Lorsque vous aurez finalisé la mise en conformité, vous devrez valider votre conformité au standard PCI DSS par le biais de la méthode qui correspond à votre niveau de commerçant Accepteur (chaque année : audit annuel sur-site ou auto-évaluation et scan ASV trimestriel), transmettre ces éléments à votre acquéreur et maintenir votre niveau de conformité dans le temps.

2.6. Quelles sont les actions que vous pouvez mener en urgence pour réduire les risques sur votre environnement et simplifier votre mise en conformité PCI ?

Le moyen le plus simple pour augmenter la sécurité des données de paiement de vos 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 conservez pas sous format électronique ou papier les données de paiement « très sensibles » comme le Cryptogramme Visuel.
- Recourez aux services de fournisseurs de services de paiement conformes au standard PCI DSS et utilisez des applications de paiement certifiées PA-DSS.

3. COMMERÇANT ACCEPTEUR DE PROXIMITE

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

3.1. Vous êtes un commerçant Accepteur de proximité. Etes-vous soumis à la conformité PCI DSS ?

Dès lors que vous manipulez, transmettez, ou êtes au contact de données de cartes bancaires, la conformité de votre environnement au Standard PCI DSS est requise.

Cependant, les menaces auxquelles vous êtes confrontés en tant que point de vente physique étant différentes de celles d'un marchand E - Commerce, le mécanisme de vérification de votre conformité PCI DSS est allégé. Vous n'aurez pas l'obligation de faire valider votre conformité PCI DSS chaque année par un auditeur externe ni à remonter l'état de conformité PCI DSS à votre acquéreur.

3.2. Quelles précautions devez-vous prendre pour assurer la sécurité de vos paiements de proximité ?

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

- Utilisez des TPE conformes à « PCI PED » (demandez à votre loueur, à votre mainteneur ou à votre acquéreur si vos terminaux sont conformes).
- Faites appel à des prestataires certifiés par votre acquéreur. Rapprochez-vous de votre centre d'affaires pour en connaître la liste.
- Rangez en lieu sûr (dans un tiroir sous le comptoir, dans une salle fermée à clé) les reçus commerçants sur lesquels le numéro de carte, le nom du porteur, 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 votre Société) sur vos TPE pour détecter toute substitution de terminal.
- Ne laissez pas votre TPE facilement accessible et sans surveillance, pour éviter qu'ils ne soient manipulés, modifiés et piratés.
- Maintenez à jour un inventaire des numéros de série, marque, modèle, localisation physique de chacun de vos TPE.
- Inspectez périodiquement vos TPE, leurs connexions, et vérifiez que leurs caractéristiques correspondent à votre inventaire.
- N'autorisez 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 vous utilisiez le questionnaire SAQ correspondant à votre environnement de paiement, pour autoévaluer et améliorer vos pratiques opérationnelles le cas échéant.

3.3. 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	Commerçant Accepteur utilisant des périphériques d'impression uniquement, ou des terminaux autonomes à ligne directe, sans stockage électronique de données de titulaires de carte. *Exemple : Commerçant Accepteur disposant de TPE RTC.*
B-IP	Commerçant Accepteur utilisant uniquement des terminaux de paiement 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	Commerçant 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	Commerçant 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 commerçants Accepteurs non décrits dans les descriptions des SAQ ci -dessus.

Les Questionnaires SAQ sont disponibles en ligne à l'adresse suivante :
https://fr.pcisecuritystandards.org/minisite/env2/ (section « SAQ »).

4. REGIMES SPECIFIQUES : HOTELS, COMPAGNIES AERIENNES

4.1. Vous êtes un hôtelier. Comment devez-vous valider votre 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[4] » sont conduites conformément à la règlementation - Visa Europe Operating Regulations, à savoir produire un reçu comportant les informations suivantes :
  - Montant de la nuitée facturée et des taxes applicables.
  - Nom du porteur 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 la 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[5]).

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.

4.2. Vous êtes une compagnie aérienne. Comment devez-vous valider votre 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 banque acquéreur un plan de mise en conformité à PCI DSS. La compagnie aérienne doit communiquer chaque année l'évolution de son plan d'action à son acquéreur.

5. NOUS CONTACTER

Pour tout renseignement concernant cette notice, vous pouvez nous contacter aux coordonnées figurant à l'article « Contact » des Conditions Générales.
Références
- Informations générales sur PCI :
http://pcisecuritystandards.org/
https://fr.pcisecuritystandards.org/minisite/env2/

6. LEXIQUE

ASV : Approved Scanning Vendor. Société habilitée par le Conseil PCI à réaliser des scans de vulnérabilité externes.
La liste des solutions ASV référencées est maintenue à jour :
https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php

Données d'authentification sensible : Au sens PCI DSS ce terme couvre individuellement ou non :
- La piste magnétique complète.
- Le code PIN.
- Le Cryptogramme Visuel (CVV).

Données porteurs : Les Données Porteurs sont constituées de l'un ou l'ensemble des éléments suivants :
- Le numéro de la carte.
- Le nom du porteur.
- La date de validité.
- Le code de service.

Environnement de données de carte(s) bancaire(s) Environnement porteur(s) : Ceci correspond aux individus, aux processus et aux technologies qui stockent, traitent ou transmettent les données de titulaires de cartes ou des données sensibles d'authentification, et comprend également tous les composants connectés du système.
ISA : Internal Security Assessor. Le registre du personnel certifié ISA est maintenu à jour par le Conseil PCI :
https://www.pcisecuritystandards.org/assessors_and_solutions/internal_security_assessors

PCI DSS : Payment Card Industry - Data Security Standard : Standard de sécurité qui s'applique aux systèmes d'informations qui manipulent des données sensibles au sens PCI (essentiellement les données des porteurs de carte comme le numéro de carte).

PA-DSS : Payment Application - Data Security Standard : Variante du standard PCI DSS qui s'applique aux applications de paiement

Prestataire de Services : Entité commerciale qui n'est pas une marque de carte de paiement, directement impliquée dans le traitement, le stockage et la transmission des données de titulaires de cartes. Ceci comprend notamment les sociétés qui assurent des services de contrôle ou susceptibles d'affecter la sécurité des données de titulaires de cartes.
Les prestataires de services gérés qui mettent à disposition des pares-feux, des IDS et autres services, ainsi que les fournisseurs et autres entités d'hébergement en sont des exemples.
Les entités telles que les sociétés de télécommunication fournissant uniquement des liens de communication sans accès à la couche application du lien de communication sont exclues.

SAQ : Questionnaire d'auto-évaluation de la conformité à PCI DSS. Il permet à toute entité d'auto évaluer le niveau de conformité de son système d'information à PCI DSS. Il est destiné aux entités qui n'ont pas l'obligation d'être évaluées par un auditeur
QSA.

QSA : Qualified Security Assessor : entreprise indépendante et disposant de compétences en sécurité de l'information qui a été qualifiée par le PCI Security Standards Council pour évaluer la conformité d'une entité à la norme PCI DSS. Le registre du personnel certifié QSA est maintenu à jour :
https://www.pcisecuritystandards.org/assessors_and_solutions/qualified_security_assessors

[4] 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 ».

[5] Le Property Management System (PMS) 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… 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.