



## CONTRAT WEBFACTURES

Le contrat WEBFACTURES permettant l'acceptation en paiement à distance sécurisé de cartes de paiement (ci-après dénommé le « Contrat ») est composé :

- des conditions particulières convenues ci-dessous entre la Banque et l'Accepteur (ci-après dénommées « Conditions Particulières de fonctionnement du service ») ;
- des Conditions Générales du contrat d'acceptation en paiement à distance sécurisé par cartes de paiement ;
- et des Conditions Générales de raccordement et d'accès aux fonctions de la plate-forme de paiement sécurisé et des services WEBFACTURES.

### CONDITIONS GENERALES DU CONTRAT D'ACCEPTATION EN PAIEMENT A DISTANCE SECURISE PAR CARTES DE PAIEMENT (VADS)

Les présentes Conditions Générales du contrat d'acceptation en paiement à distance sécurisé par cartes de paiement comportent deux parties :

- o Une Partie I : Conditions Générales communes à tous les Schémas de cartes de paiement,
- o Une Partie II : Dispositions spécifiques à chaque Schéma de cartes de paiement.

#### PARTIE 1 CONDITIONS GENERALES COMMUNES A TOUS LES SCHEMAS

#### ARTICLE 1 – DEFINITIONS

- 1) L'"Accepteur" peut être tout commerçant, tout prestataire de services, toute personne exerçant une profession libérale, et d'une manière générale, tout professionnel vendant ou louant des biens et/ou des prestations de services ou toute entité dûment habilitée à recevoir des dons ou à percevoir des cotisations, susceptible d'utiliser un Système d'Acceptation reconnu par le(s) Schéma(s) dûment convenu(s) avec l'Acquéreur.
- 2) Par "Marque", il faut entendre tout nom, terme, sigle, symbole (matériel ou numérique) ou la combinaison de ces éléments susceptible de désigner le Schéma.  
Les Marques pouvant être acceptées entrant dans le champ d'application du présent Contrat sont visées en Partie 2.
- 3) Par "Acquéreur" il faut entendre tout établissement habilité à organiser l'acceptation des Cartes portant la(les) Marque(s) du(des) Schéma(s) visé(s) en Partie 2 du présent Contrat.
- 4) Par "Système d'Acceptation", il faut entendre les logiciels et protocoles, conformes aux spécifications définies par chaque Schéma, et nécessaires à l'enregistrement, à la transmission et au traitement sécurisé des ordres de paiement par Cartes portant la (l'une des) Marque(s) dudit Schéma. L'Accepteur doit s'assurer que le Système d'Acceptation a fait l'objet d'un agrément ou d'une approbation par l'entité responsable du Schéma, le cas échéant en consultant la liste des Systèmes d'Acceptation reconnus par l'entité responsable du Schéma.
- 5) Par « Règlement », il faut entendre le Règlement UE n°2015/751 du 29 avril 2015.
- 6) Par "Schéma", il faut entendre un ensemble de règles régissant l'exécution d'opérations de paiement liées à une carte tel que défini à l'article 2 du Règlement.

Les Schémas CB/Visa/Mastercard reposent sur l'utilisation de Cartes auprès des Accepteurs acceptant la (l'une des) Marque(s) desdits Schémas et cela dans le cadre des seules dispositions et procédures définies ou homologuées par lesdits Schémas.

- 7) Par « Carte », on entend une catégorie d'instrument de paiement qui permet au payeur d'initier une opération de paiement. Elle porte une ou plusieurs Marque(s).

Lorsque la Carte est émise dans l'Espace Economique Européen (ci-après l'"EEE" qui comprend les Etats membres de l'Union Européenne, l'Islande, le Liechtenstein et la Norvège), elle porte au moins l'une des mentions suivantes :

- crédit ou carte de crédit,

Groupe Crédit du Nord  PLUS LOIN, AVEC VOUS

Banque  
Courtois

Banque  
Kolb

Banque  
Laydernier

Banque  
Nuger

Banque  
Rhône-Alpes

Banque  
Tarneaud

Société  
Marseillaise de Crédit

Crédit  
du Nord



- débit,
- prépayé,
- commercial,

ou l'équivalent dans une langue étrangère.

- 8) Par « Catégorie de carte », on entend les catégories de Carte suivantes :
- carte de crédit,
  - carte de débit,
  - carte prépayée,
  - carte commerciale.
- 9) Par "Paiements récurrents et/ou échelonnés" (ci-après les "Paiements Récurrents"), il faut entendre plusieurs opérations de paiement successives et distinctes (série d'opérations) ayant des montants et des dates déterminés ou déterminables et/ou à des échéances convenues entre l'Accepteur et le titulaire de la Carte.
- 10) Par « Parties », il faut entendre l'Acquéreur et l'Accepteur.

## ARTICLE 2 - OBLIGATIONS DE L'ACCEPTEUR

L'Accepteur s'engage à :

- 2.1 Afficher visiblement la (les) Marque(s) qu'il accepte et la (les) Catégorie(s) de carte qu'il accepte ou refuse pour chaque Marque notamment en apposant ces informations de façon apparente sur l'écran du dispositif technique ou /et sur tout autre support de communication.
- Pour la(les) Marque(s) qu'il accepte, l'Accepteur doit accepter toutes les Cartes émises hors de l'EEE sur lesquelles figure(nt) cette(ces) Marque(s), quelle que soit la Catégorie de carte.
- 2.2 Afficher visiblement le montant minimum éventuel à partir duquel la Carte est acceptée afin que le titulaire de la Carte en soit préalablement informé.
- 2.3 En cas de présence de plusieurs Marques sur la Carte, respecter la Marque choisie par le titulaire de la Carte pour donner l'ordre de paiement.
- 2.4 Respecter les lois et règlements (y compris en matière fiscale), les dispositions professionnelles ainsi que les bonnes pratiques applicables aux ventes et prestations réalisées à distance ainsi que celles applicables au commerce électronique, et notamment aux échanges utilisant les réseaux et les différents terminaux de communication (ex : mobile et ordinateur).
- A cet effet l'Accepteur organise la traçabilité adéquate des informations liées au paiement en ligne.
- 2.5 Utiliser le Système d'Acceptation en s'abstenant de toute activité qui pourrait être pénalement sanctionnée, telle que la mise en péril de mineurs, des actes de pédophilie, des actes de contrefaçon d'œuvres protégées par un droit de propriété intellectuelle et de moyens ou instruments de paiement, le non-respect de la protection des données à caractère personnel, des atteintes aux systèmes de traitement automatisé desdites données, des actes de blanchiment, le non-respect des dispositions relatives aux jeux d'argent et de hasard, aux courses de chevaux, aux loteries et des dispositions relatives aux conditions d'exercice de professions réglementées.
- 2.6 Garantir l'Acquéreur, et, le cas échéant, les Schémas, contre toute conséquence dommageable pouvant résulter pour eux du manquement aux obligations visées à l'article 2.5.
- 2.7 Afin que le titulaire de la Carte n'ait pas de difficulté à vérifier et identifier les opérations de paiement qu'il a initiées, vérifier avec l'Acquéreur la conformité des informations transmises pour identifier son point de vente en ligne.
- Les informations doivent indiquer une dénomination commerciale connue des titulaires de Carte et permettre de dissocier ce mode de paiement des autres modes de paiement (ex : automate et règlement en présence physique du titulaire de la Carte).
- 2.8 Accepter les paiements à distance sécurisés effectués avec la (les) Marque(s) et Catégorie(s) de carte qu'il a choisies d'accepter ou qu'il doit accepter en contrepartie d'actes de vente et/ou de prestations de services offerts à sa clientèle et qu'il fournit ou réalise lui-même ou à titre de dons ou pour le règlement du montant de cotisations,
- 2.9 Ne pas collecter au titre du présent Contrat une opération de paiement pour laquelle il n'a pas reçu lui-même le consentement exprès du titulaire de la Carte.



- 2.10 Afficher visiblement sur tout support, et notamment à l'écran du dispositif technique, le montant à payer ainsi que la devise dans laquelle ce montant est libellé.
- 2.11 Utiliser obligatoirement un Système d'Acceptation conforme aux spécifications du Schéma et les procédures de sécurisation des ordres de paiement donnés à distance par les titulaires de Cartes (en ce compris la procédure d'authentification de ces derniers) proposées par l'Acquéreur.
- 2.12 – Ne pas stocker sous quelque forme que ce soit le cryptogramme visuel (trois derniers chiffres du numéro figurant au verso de la Carte).
- 2.13 Régler, selon les Conditions Particulières convenues avec l'Acquéreur, les commissions, frais et, d'une manière générale, toute somme due au titre de l'acceptation des Cartes.
- 2.14 Prévoir, dans ses relations contractuelles avec les tiers, tels que les prestataires de services techniques ou sous-traitants intervenant dans le traitement et le stockage des données de paiement sensibles liées à l'utilisation des Cartes, que ces derniers s'engagent à respecter le Référentiel Sécuritaire Accepteur et le Référentiel Sécuritaire PCI DSS et acceptent que les audits visés à l'article 2.15 soient réalisés dans leurs locaux et que les rapports puissent être communiqués comme précisé à cet article.
- 2.15 Respecter les exigences du Référentiel Sécuritaire Accepteur annexé au présent Contrat ainsi que celles du Référentiel Sécuritaire PCI DSS dont il peut prendre connaissance à l'adresse suivante : <https://fr.pcisecuritystandards.org/minisite/env2/> ou qui lui sera communiqué par l'Acquéreur à première demande,
- 2.16 Permettre à l'Acquéreur et/ou au(x) Schéma(s) concerné(s) de faire procéder dans les locaux de l'Accepteur ou dans ceux des tiers visés à l'article 2.13 ci-dessus, à la vérification et au contrôle périodique par un tiers indépendant du fonctionnement des services de paiement sur Internet en fonction des risques de sécurité liés au Système d'Acceptation utilisé. Cette vérification, appelée "procédure d'audit", s'inscrit dans le respect des procédures de contrôle et d'audit définies par le Schéma concerné.
- Au cas où le rapport remis aux Parties par le tiers indépendant à l'issue de la procédure d'audit révélerait un ou plusieurs manquement(s) aux clauses du Contrat et/ou aux exigences du Référentiel Sécuritaire Accepteur et/ou du Référentiel Sécuritaire PCI DSS, l'Acquéreur peut procéder, le cas échéant à la demande du(des) Schéma(s) concerné(s), à une suspension de l'acceptation des Cartes portant la (les) Marques du(des) Schémas concerné(s) par l'Accepteur, voire à la résiliation du présent Contrat, dans les conditions prévues aux articles 8 et 9 de la présente Partie 1. L'Accepteur autorise la communication du rapport à l'Acquéreur et au(x) Schéma(s) concerné(s).
- 2.17 Dans le cas où il propose des Paiements Récurrents, l'Accepteur s'engage à :
- respecter les règles relatives au stockage des données à caractère personnel ou des données de paiement sensibles liées à l'utilisation de la Carte définies par la délibération de la CNIL n° 2018-303 du 6 septembre 2018
  - s'assurer que le titulaire de la Carte a consenti à ce que les données de paiement sensibles liées à sa Carte soient utilisées pour effectuer des Paiements Récurrents et, à ce titre, recueillir du titulaire de la Carte les autorisations et/ou mandats nécessaires à l'exécution des Paiements Récurrents et en conserver la preuve pendant quinze (15) mois à compter de la date du dernier paiement,
  - donner une information claire au titulaire de la Carte sur les droits dont il dispose et notamment sur la possibilité de retirer à tout moment son consentement,
  - ne plus initier de paiements dès lors que le titulaire de la Carte a retiré son consentement à l'exécution de la série d'opérations de paiement considérée.
- 2.18 Faire son affaire personnelle des litiges liés à la relation sous-jacente (ex : contrat de vente) qui existe entre lui et le titulaire de la Carte et de leurs conséquences financières.
- 2.19 Informer dans les meilleurs délais l'Acquéreur en cas de fonctionnement anormal du Système d'Acceptation et de toutes autres anomalies (absence d'application des procédures de sécurisation des ordres de paiement, dysfonctionnement du Système d'Acceptation).
- 2.20 En cas de survenance d'un incident de sécurité majeur, notamment en cas de collecte et/ou d'utilisation frauduleuse des données liées au paiement, coopérer avec l'Acquéreur et, le cas échéant, les autorités compétentes. Le refus ou l'absence de coopération de la part de l'Accepteur pourra conduire l'Acquéreur à résilier le présent Contrat conformément à l'article 8 de la présente Partie 1.

### ARTICLE 3 - OBLIGATIONS DE L'ACQUEREUR

L'Acquéreur s'engage à :

- 3.1 Mettre à la disposition de l'Accepteur les informations relatives à la sécurité des opérations de paiement, notamment l'accès au serveur d'autorisation.



- 3.2 Fournir à l'Accepteur les informations le concernant directement sur le fonctionnement du/des Schéma(s) visé(s) dans la Partie 2 du présent Contrat et son/leur évolution, la (les) Marque(s) et Catégorie(s) de carte dont il assure l'acceptation, ainsi que les frais applicables à chaque Marque et Catégorie de carte acceptées par lui, y compris les commissions d'interchange et les frais versés au(x) Schéma(s).
- 3.3 Respecter le choix de la Marque utilisée pour donner l'ordre de paiement conformément au choix de l'Accepteur ou du titulaire de la Carte.
- 3.4 Inscire l'Accepteur dans la liste des accepteurs habilités à recevoir des paiements à distance sécurisés par Cartes.
- 3.5 Indiquer à l'Accepteur la liste et les caractéristiques des Cartes pouvant être acceptées ainsi que les méthodes utilisées pour cette acceptation et lui fournir à sa demande le fichier des codes émetteurs (BIN).
- 3.6 Créditer le compte de l'Accepteur des sommes qui lui sont dues au plus tard le jour ouvrable (un jour ouvrable est un jour au cours duquel l'ensemble des personnes impliquées dans l'exécution d'une opération de paiement exerce une activité permettant d'exécuter l'opération de paiement concerné) suivant le moment de réception des enregistrements des opérations de paiement. Les parties conviennent que le moment de réception est le jour ouvrable au cours duquel l'Acquéreur reçoit les enregistrements. Toutefois, les enregistrements reçus après 10h00 sont réputés avoir été reçus le jour ouvrable suivant.
- 3.7 Ne pas débiter, au-delà du délai maximum de quinze (15) mois à partir de la date du crédit initial porté au compte de l'Accepteur, les opérations non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.
- 3.8 Selon les modalités convenues avec l'Accepteur, communiquer au moins une fois par mois les informations suivantes :
- la référence lui permettant d'identifier l'opération de paiement,
  - le montant de l'opération de paiement exprimé dans la devise dans laquelle son compte est crédité,
  - le montant de tous les frais appliqués à l'opération de paiement et le montant de la commission de service acquittée par l'Accepteur et de la commission d'interchange.
- L'Accepteur peut demander à ce que les informations soient regroupées par Marque, par Catégorie de carte et par taux de commission d'interchange applicable à l'opération.
- 3.9 Indiquer et facturer à l'Accepteur les commissions de services à acquitter séparément pour chaque Catégorie de carte et chaque Marque selon les différents niveaux de commission d'interchange.
- L'Accepteur peut demander à ce que les commissions de services soient regroupées. par Marque, Catégorie de carte et par taux de commission d'interchange applicable à l'opération.
- 3.10 En cas de présence de plusieurs Marques sur la Carte, respecter le choix de la Marque et de la catégorie de Carte conformément à l'article 8 du Règlement UE n°2015 / 751 du 29 avril 2015, retenu par l'Accepteur et le Titulaire de la Carte pour donner l'ordre de paiement au point de vente ou d'acceptation.

#### **ARTICLE 4 : GARANTIE DE PAIEMENT**

Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées tant à l'article 5 qu'en Partie 2 des présentes, ainsi que dans les Conditions Particulières.

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

En cas de non-respect d'une seule de ces mesures ou lorsque l'opération ne fait pas l'objet d'une authentification forte sur demande de l'Accepteur conformément à l'article 2.3 de l'Annexe 1, les opérations de paiement ne sont réglées que sous réserve de bonne fin d'encaissement et ce, en l'absence de contestations.

#### **ARTICLE 5 - MESURES DE SECURITE**

##### **5.1 Lors du paiement**

L'Accepteur s'engage à :

- 5.1.1 Appliquer la procédure de sécurisation des ordres de paiement (en ce compris la procédure d'authentification) décrite dans les Conditions Générales et en annexe.
- 5.1.2 Obtenir de l'Acquéreur un justificatif d'acceptation matérialisant les contrôles effectués et la validité de l'ordre de paiement. Les conditions d'obtention du justificatif d'acceptation sont décrites à l'article 2 de l'annexe 1.
- 5.1.3 Vérifier l'acceptabilité de la Carte c'est-à-dire :
- la période de validité (fin et éventuellement début),



- que la Marque est indiquée dans les Conditions Particulières ou figure dans la Partie 2 des présentes.

5.1.4 Obtenir une autorisation d'un montant identique à l'opération sous-jacente. La demande d'autorisation doit obligatoirement mentionner le CVX2 (cryptogramme visuel). Une réponse de type « interdit », faite par le Système d'Acceptation, annule la garantie pour toutes les transactions faites postérieurement, le même jour avec la même Carte, dans le même point de vente en ligne.

## 5.2 Après le paiement

L'Accepteur s'engage à :

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

L'Accepteur ne doit transmettre que les enregistrements électroniques des opérations pour lesquelles un ordre de paiement a été donné à son profit. Toute opération ayant fait l'objet d'une autorisation transmise par l'Acquéreur doit être obligatoirement remise à ce dernier.

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

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

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

## ARTICLE 6 : MODALITES ANNEXES DE FONCTIONNEMENT

### 6.1 Réclamation

Toute réclamation doit être formulée par écrit à l'Acquéreur, 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 en compte résultant d'une opération de paiement non garantie, notamment en cas d'impayé.

En cas de mauvaise exécution, il appartient à l'Accepteur d'établir l'erreur imputable à l'Acquéreur. Si la preuve de l'erreur de l'Acquéreur est démontrée par l'Accepteur, l'Acquéreur remboursera immédiatement ce dernier et rétablira le compte débité dans l'état où il se serait trouvé si l'opération de paiement mal exécutée n'avait pas eu lieu.

### 6.2 Convention de preuve

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

En cas de conflit, les enregistrements électroniques produits par l'Acquéreur ou le Schéma prévaudront sur ceux réalisés par l'Accepteur, à moins que ce dernier ne démontre l'absence de fiabilité ou d'authenticité des documents produits par l'Acquéreur ou le Schéma.



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

## ARTICLE 7 : MODIFICATIONS

- 7.1 L'Acquéreur peut modifier à tout moment les dispositions du présent Contrat.
- L'Acquéreur peut notamment apporter :
- des modifications techniques telles que l'acceptabilité de nouvelles Cartes, les modifications de logiciel, le changement de certains paramètres, la remise en l'état du Système d'Acceptation suite à un dysfonctionnement etc.
  - des modifications sécuritaires telles que :
    - la suppression de l'acceptabilité de certaines Cartes,
    - la suspension de l'acceptabilité de Cartes portant certaines Marques.
- 7.2 Les nouvelles conditions entrent généralement en vigueur au terme d'un délai minimum fixé à un (1) mois à compter de l'envoi de la notification sur support papier ou sur tout autre support durable.
- D'un commun accord, précisé dans les Conditions Particulières convenues entre l'Acquéreur et l'Accepteur, les Parties peuvent déroger à ce délai en cas de modifications importantes.
- 7.3 Ce délai est exceptionnellement réduit à cinq (5) jours calendaires lorsque l'Acquéreur ou le Schéma constate une utilisation anormale de Cartes perdues, volées ou contrefaites.
- 7.4 En cas de désaccord, l'Accepteur a la possibilité de résilier son Contrat, selon les modalités prévues à l'article 8 de la présente Partie 1.
- Passés les délais visés au présent article, les modifications sont opposables à l'Accepteur s'il n'a pas résilié le présent Contrat, sans que l'Acquéreur ait à lui rappeler cette faculté.
- 7.5 Le non-respect des nouvelles conditions techniques et sécuritaires, dans les délais impartis, peut entraîner la suspension par l'Acquéreur de l'acceptation des Cartes portant la (les) Marque(s) du(des) Schéma(s) concerné(s), dans les conditions prévues à l'article 9 de la présente Partie 1, voire la résiliation du Contrat, dans les conditions prévues à l'article 8 de la présente Partie 1.

## ARTICLE 8 : DUREE ET RESILIATION DU CONTRAT

- 8.1. Le présent Contrat est conclu pour une durée indéterminée, sauf dispositions contraires visées dans les Conditions Particulières.
- L'Accepteur d'une part, l'Acquéreur d'autre part, peuvent, à tout moment, sans justificatif ni préavis (sauf dérogation particulière convenue entre les Parties), sous réserve du dénouement des opérations en cours, mettre fin au présent Contrat, sans qu'il soit nécessaire d'accomplir aucune autre formalité que l'envoi d'une lettre recommandée avec demande d'avis de réception. L'Accepteur garde alors la faculté de continuer à accepter les Cartes de tout Schéma avec tout autre acquéreur de son choix.



- 8.2 En outre, à la demande de tout Schéma, l'Acquéreur peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à la résiliation du présent Contrat. Elle peut être décidée notamment pour l'une des raisons visées à l'article 9.2 ci-dessous. Elle est notifiée par lettre recommandée avec demande d'avis de réception et doit être motivée. Son effet est immédiat.
- 8.3 Toute cessation d'activité de l'Accepteur, cession ou mutation du fonds de commerce, entraîne la résiliation immédiate de plein droit du présent Contrat sous réserve du dénouement des opérations en cours.
- Dans le cas où, après résiliation du présent Contrat, il se révélerait des impayés, ceux-ci seront à la charge de l'Accepteur ou pourront faire l'objet d'une déclaration de créances.
- 8.4 L'Accepteur est tenu de restituer à l'Acquéreur les dispositifs techniques et sécuritaires et les documents en sa possession dont l'Acquéreur est propriétaire.
- Sauf dans le cas où il a conclu un ou plusieurs autre(s) contrat(s) d'acceptation, l'Accepteur s'engage à retirer immédiatement de son point de vente en ligne et de ses supports de communication tout signe d'acceptation des Cartes.
- 8.5 L'Acquéreur peut suspendre ou résilier le Contrat sans préavis, sans autre formalité que l'envoi d'une lettre recommandée avec demande d'avis de réception, dès lors qu'il est informé de l'illicéité du contenu du site Internet de l'Accepteur.

#### **ARTICLE 9 - SUSPENSION DE L'ACCEPTATION**

- 9.1 L'Acquéreur peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à une suspension de l'acceptation des Cartes portant certaines Marques par l'Accepteur. La suspension est précédée, le cas échéant, d'un avertissement à l'Accepteur, voire d'une réduction de son seuil de demande d'autorisation. Elle est notifiée par tout moyen et doit être motivée. Son effet est immédiat.
- Elle peut également intervenir à l'issue d'une procédure d'audit visée à l'article 2.15 ci-dessus au cas où le rapport révélerait un ou plusieurs manquement(s) tant aux clauses du présent Contrat qu'aux exigences du Référentiel Sécuritaire Accepteur et/ou du Référentiel Sécuritaire PCI DSS.
- 9.2 La suspension peut être décidée en raison notamment :
- 9.2.1 du non-respect répété des obligations du présent Contrat et du refus d'y remédier, ou d'un risque de dysfonctionnement important du Système d'Acceptation d'un Schéma,
  - 9.2.2 d'une participation à des activités frauduleuses, notamment d'une utilisation anormale de Cartes perdues, volées ou contrefaites,
  - 9.2.3 d'un refus d'acceptation répété et non motivé de la (des) Marque(s) et/ou Catégorie(s) de carte qu'il a choisie(s) d'accepter ou qu'il doit accepter,
  - 9.2.4 de plaintes répétées d'autres membres ou partenaires d'un Schéma et qui n'ont pu être résolues dans un délai raisonnable,
  - 9.2.5 de retard volontaire ou non motivé de transmission des justificatifs,
  - 9.2.6 d'un risque aggravé en raison des activités de l'Accepteur.
- 9.3 L'Accepteur s'engage alors à restituer à l'Acquéreur les dispositifs techniques et sécuritaires et les documents en sa possession dont l'Acquéreur est propriétaire, et à retirer immédiatement de son point de vente en ligne tout signe d'acceptation des Cartes du Schéma concerné.
- 9.4 En cas de suspension, la période de suspension est au minimum de six (6) mois, éventuellement renouvelable. A l'expiration de ce délai, l'Accepteur peut demander la reprise du présent Contrat auprès de l'Acquéreur, ou souscrire un nouveau contrat d'acceptation avec un autre acquéreur de son choix.

#### **ARTICLE 10 - MESURES DE PREVENTION ET DE SANCTION PRISES PAR L'ACQUEREUR**

- 10.1 En cas de manquement de l'Accepteur aux stipulations du présent Contrat ou aux lois en vigueur, ou en cas de constat d'un taux d'impayés anormalement élevé ou d'utilisation anormale de Cartes perdues, volées ou contrefaites, l'Acquéreur peut prendre des mesures de sauvegarde et de sécurité consistant, en premier lieu, en un avertissement à l'Accepteur valant mise en demeure précisant les mesures à prendre pour remédier au manquement ou résorber le taux d'impayés anormalement élevé constaté.
- 10.2 Si dans un délai de trente (30) jours, l'Accepteur n'a pas remédié au manquement ayant justifié l'avertissement ou n'a pas mis en œuvre les mesures destinées à résorber le taux d'impayés constaté, l'Acquéreur peut soit procéder à une suspension de l'acceptation des Cartes, dans les conditions précisées à l'article 9 ci-dessus, soit résilier de plein droit avec effet immédiat, sous réserve du dénouement des opérations en cours, le présent Contrat par lettre recommandée avec demande d'avis de réception.



- 10.3 De même, si dans un délai de trois (3) mois à compter de l'avertissement, l'Accepteur est toujours confronté à un taux d'impayés anormalement élevé, l'Acquéreur peut décider la résiliation de plein droit avec effet immédiat, sous réserve des opérations en cours, du présent Contrat, notifiée par lettre recommandée avec demande d'avis de réception.
- 10.4. En cas de suspension ou de résiliation, l'Accepteur s'engage à restituer à l'Acquéreur les dispositifs techniques et sécuritaires et les documents en sa possession dont l'Acquéreur est propriétaire et, à retirer immédiatement de son point de vente en ligne et de ses supports de communication tout signe d'acceptation des Cartes, sauf dans le cas où il a conclu un ou plusieurs autre(s) contrat(s) d'acceptation.

## ARTICLE 11 : SECRET BANCAIRE ET PROTECTION DES DONNEES A CARACTERE PERSONNEL

### 11.1 Secret bancaire

De convention expresse, l'Accepteur autorise l'Acquéreur à stocker le cas échéant des données secrètes ou confidentielles portant sur lui et les communiquer à des entités impliquées dans le fonctionnement du(des) Schéma(s) 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.

### 11.2 Protection des données à caractère personnel

Lors de la signature ou de l'exécution des présentes, chacune des Parties peut avoir accès à des données à caractère personnel.

Ainsi, en application de la réglementation française et européenne applicable en matière de protection des données à caractère personnel, et en particulier du Règlement (UE) 2016/679 du 27 avril 2016 sur la protection des données à caractère personnel, il est précisé que :

- 11.2.1 Les données à caractère personnel relatives à l'Accepteur, collectées par l'Acquéreur nécessaires pour l'exécution des ordres de paiement transmis et leur sécurisation, ne seront utilisées que pour les finalités suivantes :
- Le traitement des opérations de paiement par Carte. Ce traitement est nécessaire à la bonne exécution du présent contrat et à défaut le contrat ne pourra être exécuté ;
  - La poursuite des intérêts légitimes de l'Acquéreur que constituent la lutte contre la fraude à la carte de paiement et la gestion des éventuels recours en justice ;
  - La réponse aux obligations légales et réglementaires.

Ces données à caractère personnel traitées par l'Acquéreur sont conservées pour les durées suivantes :

- Les données nécessaires à l'exécution des opérations de paiement par Carte sont conservées pour une durée de 5 ans à compter de l'exécution de l'opération étant précisé que cette durée est portée à 10 ans dès lors qu'il s'agit d'un document comptable ;
- Les données nécessaires à la lutte contre la fraude sont conservées pour une durée maximale de 10 ans à compter de la clôture du dossier de fraude ;
- Les données nécessaires à la gestion d'un éventuel recours en justice sont conservées jusqu'au terme de la procédure. Elles sont ensuite archivées selon les durées légales de prescription applicables.

Pour satisfaire les finalités précisées ci-dessus, les données à caractère personnel relatives à l'Accepteur pourront être communiquées aux Emetteurs, partenaires, sous- traitants, prestataires de l'Acquéreur, ainsi qu'aux Schémas de cartes de paiement dont les marques sont acceptées par l'Accepteur.

Conformément à la réglementation applicable et notamment le chapitre III du Règlement (UE) 2016/679 du 27 avril 2016, l'Accepteur (personne physique ou personne physique le représentant sur laquelle portent les données à caractère personnel) peut :

- demander à accéder aux données à caractère personnel la concernant et / ou en demander la rectification ou l'effacement ;
- définir des directives relatives au sort des données à caractère personnel la concernant après son décès ;
- s'opposer au traitement de données à caractère personnel la concernant réalisé aux fins de lutte contre la fraude et / ou de gestion des éventuels recours en justice, sous réserve que l'Acquéreur n'invoque pas de motifs légitimes et impérieux ;
- demander des limitations au traitement des données à caractère personnel la concernant dans les conditions prévues à l'article 18 du Règlement (UE) 2016/679 du 27 avril 2016 ;





- demander à recevoir et / ou transmettre à un autre responsable du traitement les données à caractère personnel la concernant sous une forme couramment utilisée et lisible par un appareil électronique ;
- introduire une réclamation auprès de la Commission nationale de l'informatique et des libertés.

L'Accepteur peut exercer ses droits et contacter le délégué à la protection des données personnelles en s'adressant : auprès de l'agence dans laquelle est ouvert son compte, par courrier électronique à l'adresse suivante [dpo.cdn@cdn.fr](mailto:dpo.cdn@cdn.fr), aux coordonnées du service client indiquées dans les conditions générales du compte bancaire.

11.2.2 A l'occasion de l'exécution des ordres de paiement donnés par Carte, l'Accepteur peut avoir accès à différentes données à caractère personnel concernant notamment les titulaires de Cartes.

L'Accepteur s'engage à respecter la réglementation française et européenne applicable en matière de protection des données à caractère personnel et notamment le Règlement (UE) 2016/679 du 27 avril 2016.

L'Accepteur ne peut utiliser ces données à caractère personnel que pour l'exécution des ordres de paiement par Carte ainsi que pour les finalités prévues par la délibération n° 2018-303 du 6 septembre 2018 portant adoption d'une recommandation concernant le traitement des données relatives à la carte de paiement en matière de vente de biens ou de fourniture de services à distance. Sauf obligations légales et réglementaires, il ne peut ni les céder, ni en faire un quelconque usage qui ne soit pas directement visé par le présent Contrat.

L'Accepteur s'engage à mettre en œuvre toutes les mesures techniques et organisationnelles appropriées pour que soient assurés la confidentialité et l'intégrité des données à caractère personnel du titulaire de la Carte qu'il est amené à recueillir à l'occasion de son activité et notamment lors de la réalisation d'une opération par Carte ainsi que le contrôle de l'accès à celles-ci et ce, conformément aux dispositions de l'article 32 du Règlement (UE) 2016/679 du 27 avril 2016.

Les titulaires de Cartes sur lesquels des données à caractère personnel ont été recueillies doivent pouvoir disposer, auprès de l'Accepteur, de l'intégralité des droits prévus par la réglementation française et européenne applicable en matière de protection des données à caractère personnel, et notamment de leurs droits d'accès, de rectification, d'effacement, d'opposition, de limitation ainsi que de leur droit à la portabilité. A cet égard, l'Accepteur s'engage d'ores et déjà à leur permettre d'exercer ces droits.

## **ARTICLE 12 : NON RENONCIATION**

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

## **ARTICLE 13 : LOI APPLICABLE/TRIBUNAUX COMPETENTS**

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

## **ARTICLE 14 : LANGUE DU PRESENT CONTRAT**

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



## PARTIE 2 DISPOSITIONS SPECIFIQUES A CHAQUE SCHEMA

### I. DISPOSITIONS SPECIFIQUES AUX SCHEMAS VISA ET MASTERCARD

#### ARTICLE 1 – FONCTIONNEMENT DES SCHEMAS

Les entités responsables des Schémas sont :

- Visa Europe et VISA Inc,
- Mastercard Europe SA.

Ces Schémas reposent sur l'utilisation des Cartes portant les Marques suivantes :

- Pour VISA Inc. et Visa Europe :
  - Visa,
  - V PAY,
  - ELECTRON.
- Pour Mastercard Europe SA. :
  - Mastercard,
  - Maestro.

#### ARTICLE 2 – OBLIGATION DE L'ACCEPTEUR

En complément de l'article 2.7 de la Partie 1, l'Accepteur s'engage à localiser son point de vente en ligne (en principe, pays de son établissement principal) et à faire en sorte que ce dernier porte mention de sa localisation.

#### ARTICLE 3 – OBLIGATION DE L'ACQUEREUR

Par dérogation à l'article 3.7 de la Partie 1 du Contrat, l'Acquéreur s'engage à ne pas débiter, au-delà du délai maximum de vingt-quatre (24) mois à partir de la date du crédit initial porté au compte de l'Accepteur, les opérations non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.

#### ARTICLE 4 - GARANTIE DE PAIEMENT

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

### II. DISPOSITIONS SPECIFIQUES AU SCHEMA CB

#### ARTICLE 1 - DEFINITION DU SCHEMA CB

Le Schéma CB repose sur l'utilisation de Cartes portant la Marque CB (ci-après les "Cartes CB") pour le paiement d'achats de biens et/ou de prestations de services, le règlement de dons ou de cotisations auprès des Accepteurs adhérant au Schéma 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 solutions de paiement CB et la suspension de l'adhésion au Schéma CB. Il établit les conditions du contrat d'acceptation, l'Acquéreur définissant certaines conditions spécifiques de fonctionnement.

Lorsque l'Acquéreur représente le GIE CB, le terme de "représentation" ne concerne que l'ensemble des conditions techniques d'acceptation de la Carte CB et de remise des opérations à l'Acquéreur, et non la mise en jeu de la garantie du paiement visée à l'article 4 de la Partie 1 du présent Contrat.

#### ARTICLE 2 - DISPOSITIONS RELATIVES AUX CARTES CB ET AUX SOLUTIONS DE PAIEMENT CB

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

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

#### ARTICLE 3 : DISPOSITIONS SUR L'ACCEPTATION DE CARTES CB

En complément des dispositions de l'article 2 de la Partie 1 du présent Contrat, l'Accepteur s'engage à :



- 3.1 Accepter les Cartes CB pour le paiement d'achats de biens et/ou de prestations de services offerts à sa clientèle et réellement effectués, même lorsqu'il s'agit d'articles vendus à titre de promotion ou de soldes, à titre de dons ou en contrepartie du règlement du montant de cotisations.
- 3.2 Régler, selon les Conditions Particulières convenues avec l'Acquéreur les commissions, frais et d'une manière générale, toute somme due au titre de l'adhésion et du fonctionnement du Schéma CB.
- 3.3 Transmettre les enregistrements des opérations de paiement à l'Acquéreur, dans les délais prévus dans les Conditions Particulières convenues avec lui. 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 CB.
- 3.4 En cas d'audit par le GIE CB, permettre à l'Acquéreur de faire procéder dans les locaux de l'Accepteur ou dans ceux des tiers visés à l'article 2.13 de la Partie 1, à la vérification par un tiers indépendant du respect tant des clauses du présent Contrat que des exigences du Référentiel Sécuritaire Accepteur joint et/ou du Référentiel Sécuritaire PCI DSS. Cette vérification, appelée "procédure d'audit", peut intervenir à tout moment dès la conclusion du présent Contrat et/ou pendant sa durée.
- Au cas où le rapport remis aux Parties par le tiers indépendant à l'issue de la procédure d'audit révélerait un ou plusieurs manquements à ces clauses ou exigences, le GIE CB peut procéder à une suspension de l'acceptation des Cartes CB, voire à une radiation du Schéma CB tel que prévu à l'article 5 de la présente Partie.
- L'Accepteur autorise la communication du rapport à l'Acquéreur et au GIE CB.

#### ARTICLE 4 : PROTECTION DES DONNEES A CARACTERE PERSONNEL

L'Acquéreur, au titre de l'acceptation en paiement par Carte dans le Système CB, informe que le GIE CB traite des données à caractère personnel de l'Accepteur (personne physique ou personne physique le représentant) qui concernent notamment son identité et ses fonctions.

Ces données à caractère personnel font l'objet de traitements afin de permettre :

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

Les données à caractère personnel traitées par le GIE CB sont conservées pour les durées suivantes :

- En matière de lutte contre la fraude, les données utilisées pour l'émission d'alertes sont conservées pour une durée maximale de douze (12) mois à compter de l'émission des alertes. En cas de qualification de fraude avérée, les données relatives à la fraude sont conservées au maximum cinq (5) années, conformément à la réglementation de la CNIL.
- Les données nécessaires à la gestion d'un éventuel recours en justice sont conservées jusqu'au terme de la procédure. Elles sont ensuite archivées selon les durées légales de prescription applicables.

L'Accepteur (personne physique ou personne physique le représentant sur laquelle portent les données à caractère personnel) peut exercer les droits prévus au chapitre III du Règlement (UE) 2016/679 du 27 avril 2016 et détaillés dans la Partie I à l'article 11 des présentes conditions générales par courriel à [protegezvosdonnees@cartes-bancaires.com](mailto:protegezvosdonnees@cartes-bancaires.com).

Pour toute question en lien avec la protection des données à caractère personnel traitées par le GIE CB, l'Accepteur (personne physique ou personne physique le représentant sur laquelle portent les données à caractère personnel) peut :

- Consulter la Charte de protection des données à caractère personnel du GIE CB accessible à [www.cartes-bancaires.com/protegezvosdonnees](http://www.cartes-bancaires.com/protegezvosdonnees) ;
- Contacter le Délégué à la protection des données désigné par le GIE CB par courriel à [protegezvosdonnees@cartes-bancaires.com](mailto:protegezvosdonnees@cartes-bancaires.com).

#### ARTICLE 5 : RECLAMATION

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

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



## ARTICLE 6 : MESURES de PREVENTION ET DE SANCTION

### 6.1 Mesures de prévention et de sanction mises en œuvre par l'Acquéreur.

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

Si dans un délai de trente (30) jours, l'Accepteur n'a pas remédié au manquement ayant justifié l'avertissement ou n'a pas mis en œuvre les mesures destinées à résorber le taux d'impayés constaté, l'Acquéreur peut résilier de plein droit avec effet immédiat le présent Contrat, par lettre recommandée avec demande d'avis de réception.

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

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

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

- la suspension de l'acceptation des Cartes CB par l'Accepteur. Cette suspension intervient s'il n'est pas remédié aux problèmes constatés dans un délai de trois (3) mois suivant la mise en demeure d'y remédier.

Ce délai peut être ramené à quelques jours en cas d'urgence et à un (1) mois au cas où l'Accepteur aurait déjà fait l'objet d'une mesure de suspension dans les vingt quatre (24) mois précédant l'avertissement.

La suspension de l'adhésion au Système CB peut être immédiate lorsqu'elle est décidée en raison d'un des motifs suivants :

- une utilisation anormale de Cartes perdues, volées ou contrefaites,
- une utilisation d'un Système d'Acceptation non agréé,
- un risque de dysfonctionnement important du Système CB,
- une utilisation anormale ou détournée du Système d'Acceptation.

La suspension est notifiée par l'envoi d'une lettre recommandée et motivée, avec demande d'avis de réception. Cette suspension prend effet deux (2) jours francs à compter de la réception de la notification.

- La radiation de l'adhésion de l'Accepteur au Schéma CB en cas de survenance de manquements d'une exceptionnelle gravité, de comportement dolosif ou frauduleux ou en cas de persistance d'un taux anormalement élevé d'incidents ayant déjà justifié antérieurement une mesure de suspension vis-à-vis de l'Accepteur concerné. Cette radiation est notifiée par l'envoi d'une lettre recommandée et motivée avec demande d'avis de réception.

### 6.3 En cas de suspension ou de radiation, l'Accepteur s'engage alors à restituer à l'Acquéreur les dispositifs techniques et sécuritaires et les documents en sa possession dont l'Acquéreur est propriétaire et à retirer immédiatement de ses supports de communication tout signe d'acceptation des Cartes CB.

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

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

Cette reprise d'effet ou cette nouvelle d'adhésion pourra être subordonnée à la mise en œuvre de recommandations d'un auditeur désigné par le GIE CB ou l'acquéreur concerné, et portant sur le respect des bonnes pratiques en matière de ventes et prestations réalisées à distance visées à l'article 2.4 de la Partie 1 et des mesures de sécurité visées à l'article 5 de la Partie 1.



## CONDITIONS GENERALES DU SERVICE WEBFACTURES

Webfactures est un service consistant en la mise à disposition de l'Accepteur d'un ensemble de moyens logistiques et humains permettant le traitement des ordres de paiement par carte de paiement, donnés dans le cadre de règlements de factures en ligne. Les informations nécessaires au paiement sont transmises de façon sécurisée depuis le serveur mis à la disposition de l'Accepteur, via le terminal de l'internaute porteur de la carte de paiement, vers le service de paiement électronique de la Banque.

Les fonctions et les modalités d'utilisation de ce service et les différentes fonctions que peut souscrire l'Accepteur, sont décrites dans l'annexe 1.

Les présentes Conditions générales ne s'appliquent que pour les ordres de paiement donnés par l'intermédiaire du service Webfactures. Toute autre utilisation de services de paiement à distance devra faire l'objet d'une convention distincte.

### ARTICLE 1 – MOYENS NECESSAIRES A L'UTILISATION DE WEBFACTURES

L'utilisation de Webfactures nécessite l'utilisation d'un micro-ordinateur équipé d'un système d'exploitation, d'une connexion à un réseau de communication électronique pour le transport des informations, et des logiciels de communication et de navigation que l'Accepteur installe sur son micro-ordinateur selon la procédure requise. L'accès à Webfactures se fait via l'utilisation d'un navigateur internet présentant des normes de sécurité (cryptage notamment) nécessaires au dit accès. L'Accepteur fait son affaire personnelle de son accès à Internet (notamment choix d'un fournisseur d'accès), du choix et de l'installation de son navigateur et du bon fonctionnement de son équipement informatique. L'Accepteur doit s'être assuré, sous sa responsabilité, de la compatibilité du matériel et des logiciels destinés à utiliser Webfactures. La plate-forme Webaffaires Gestion - Webfactures est accessible via l'adresse Internet : <https://office.webaffaires.org>.

L'accès à Webaffaires Gestion - Webfactures n'est possible qu'au moyen de données de sécurité personnalisées composées d'un identifiant et d'un mot de passe. L'identifiant est envoyé à l'adresse électronique indiquée dans les Conditions Particulières. Le mot de passe est adressé par courrier à l'Accepteur. L'Accepteur doit prendre toutes les mesures propres à assurer la confidentialité de ses données de sécurité personnalisées.

### ARTICLE 2 – DESCRIPTION DU SERVICE WEBFACTURES

Webfactures repose sur une plate-forme de paiement sécurisée, élaborée à partir de la solution de paiement sécurisé SIPS dont Worldline est propriétaire. Une documentation technique décrivant les fonctionnalités de Webfactures, est mise à disposition de l'Accepteur dans la rubrique « Aide » de Webfactures.

Le service Webfactures se compose :

- 2.1 : d'un service de création de « Pré-transactions », qui pourront, par la suite, être payées par Cartes portant la(les) Marque(s) CB, Visa ou MasterCard ou toute autre carte visée dans les Conditions Particulières. Pour créer une Pré-transaction, l'Accepteur doit saisir dans Webfactures : un montant, la date de validité de la Pré-transaction (au-delà de cette date, la Pré-transaction ne pourra plus être payée par carte de paiement), le mode d'envoi des données relatives à l'opération de paiement, le délai d'envoi à l'Acquéreur des données relatives à l'opération de paiement et l'identification du Client devant procéder au règlement de la Pré-transaction (ci-après Client final). Un numéro est associé à chaque Pré-transaction ainsi créée et communiqué à l'Accepteur.

- 2.2 : d'un service de paiement des Pré-transactions, par Cartes portant la(les) Marque(s) CB, Visa, MasterCard ou par toute autre carte visée dans les Conditions Particulières. Lors d'une demande de paiement par carte, les éléments suivants sont contrôlés : date de validité antérieure ou égale à la date du jour, présence du cryptogramme visuel, présence d'un numéro de carte de 10 à 19 caractères numériques. Si l'un de ces contrôles se révèle négatif, le Client final est invité à recommencer. Après 3 tentatives infructueuses, la transaction est abandonnée. Si les contrôles sont positifs, une demande d'authentification est effectuée, dans le cadre du programme 3D Secure. Si l'authentification est possible, le Client final est redirigé vers la page de saisie de la donnée d'authentification que lui a communiquée sa banque. La réponse à la demande d'authentification générée par le programme 3D Secure est systématiquement transmise, quelle qu'en soit l'issue, à l'Accepteur, dans le journal des transactions envoyé chaque matin (le champ prévu à cet effet indique Yes, No ou n'est pas renseigné). Elle est également disponible dans l'outil de gestion en ligne, dans le menu « consultation de transaction ». Si les contrôles visés ci-dessus sont positifs, et même si l'authentification de l'internaute, a échoué, une demande d'autorisation est systématiquement transmise de l'Acquéreur vers la banque du Client final sur la base des informations communiquées par le Client final (numéro de carte, date de validité et cryptogramme visuel). L'Accepteur, sur l'extranet Webaffaires Gestion - Webfactures, et le Client final sur son écran, sont informés en temps réel du résultat de la transaction. Si l'Accepteur a opté pour l'option « envoi de la confirmation du paiement par e-mail », un justificatif de transaction est envoyé à l'adresse électronique transmise par l'Accepteur. L'adresse électronique peut également être saisie en ligne par le Client final. L'Accepteur doit mettre en place les procédures appropriées pour que le Client final soit informé des modalités selon lesquelles il peut obtenir un justificatif de la transaction.

La transaction autorisée sera envoyée sous forme de remises à l'Acquéreur. A moins que l'Accepteur effectue un paramétrage différent, les remises sont adressées chaque jour ouvré à l'Acquéreur. Elles sont adressées au plus tard, à 22h30.

- 2.3 : d'un outil de gestion en ligne qui permet techniquement à l'Accepteur, notamment, de consulter, d'annuler partiellement ou totalement ou rembourser partiellement ou totalement des opérations de paiement, ainsi que de paramétrer la remise en banque. L'Accepteur peut prévoir, par l'intermédiaire de Webaffaires Gestion - Webfactures, de transmettre à l'Acquéreur une opération plus de 6 jours après qu'elle ait été effectuée. Dans ce cas, la demande d'autorisation pour le montant total de l'opération n'est effectuée qu'avant la transmission de l'opération à l'Acquéreur. L'Acquéreur attire l'attention de l'Accepteur sur le fait, qu'en application des Conditions Générales du contrat d'acceptation en paiement à distance sécurisé, ces opérations ne pourront pas être garanties si le titulaire de la carte conteste l'opération ou son montant.

2.4 d'outils de reporting : Des journaux notamment un journal des transactions et un journal des opérations sont transmis quotidiennement par courrier électronique à l'Accepteur ;

2.5 des outils sécuritaires mentionnés ci-après.

2.5.1 Le paramétrage des outils sécuritaires est placé sous la responsabilité de l'Accepteur. Il appartient à l'Accepteur de s'assurer de la régularité des contrôles qu'il met en place.



Une documentation technique détaillant les paramétrages est mise à disposition de l'Accepteur dans l'outil de gestion. L'Accepteur peut choisir le mode pré-autorisation (dans ce cas, l'opération est bloquée si le contrôle se révèle positif) ou le mode post- autorisation (dans ce cas, l'Accepteur est seulement informé dans le Journal des transactions que le contrôle est positif). Les contrôles sélectionnés sont effectués les uns après les autres dans l'ordre utilisé ci-dessous. Si l'un des contrôles est positif, les contrôles suivants ne sont pas effectués.

#### 2.5.2 Contrôle d'encours IP

Un contrôle est effectué sur le nombre de présentations d'une même adresse IP sur une période de référence.

#### 2.5.3 Contrôle du pays de la carte (Bin étranger)

Le contrôle est positif si le code du pays d'origine de la carte ne coïncide pas avec celui de l'Accepteur.

#### 2.5.4 Sur demande de l'Accepteur et après acceptation de l'Acquéreur, le contrôle suivant peut également être mis en place : Contrôle de similitude entre le pays d'émission de la carte et le code pays de l'adresse IP.

Le contrôle est positif si le code du pays associé à l'adresse IP du fournisseur d'accès de l'internaute ne coïncide pas avec le code pays de la carte.

L'Accepteur peut préciser un montant maximum par commande ou un montant cumulé pour plusieurs commandes.

2.6 L'Accepteur peut insérer sur son site Internet un lien permettant au Client final d'être redirigé vers l'adresse URL de la plate-forme de règlement. L'Accepteur doit, préalablement à la connexion du Client final à la plate-forme de règlement, saisir les informations permettant de créer une « Pré-transaction » et communiquer le numéro de la « Pré-transaction » et son identifiant « Accepteur » au titulaire de la carte ainsi que l'adresse Internet permettant d'effectuer le règlement. Pour des raisons de sécurité, l'Accepteur ne doit jamais communiquer l'URL d'accès direct à la page de règlement au Client final, c'est-à-dire la page contenant les données du Client final et de la facture. Un document appelé « avis de paiement », contenant l'ensemble des informations nécessaires au règlement, est mis à disposition de l'Accepteur suite à la création d'une Pré-transaction. Cet avis de paiement peut être imprimé ou enregistré par l'Accepteur. Il n'est pas stocké par Webaffaires Gestion - Webfactures. S'il n'est pas enregistré par le commerçant après la saisie de la « Pré-transaction », il ne pourra être récupéré ultérieurement. Lors de sa connexion à la plate-forme de règlement, le service Webfactures invite le Client final à saisir l'identifiant de l'Accepteur et celui de la pré-transaction. La plate-forme de règlement vérifie l'existence des identifiants et que l'identifiant de pré-transaction est associé à l'identifiant du commerçant. La plate-forme de règlement indique au Client final les informations qui concernent sa transaction (montant, identification du Client final,...) et l'invite à saisir les données liées à sa carte de paiement :

- numéro de carte,
- date d'expiration,
- numéro du cryptogramme visuel.

Le Client final est ensuite invité à valider ces informations. Si les contrôles effectués par la plate-forme Webaffaires Gestion - Webfactures sont positifs, le Client final est informé que son ordre de paiement a bien été enregistré. La sécurité du paiement entre le poste du Client final et la plate-forme de paiement repose sur la mise en oeuvre de la technologie Secure Socket Layer (SSL). Cette technologie de cryptographie permet d'empêcher la circulation en clair sur Internet des numéros de cartes bancaires.

## ARTICLE 3 – OBLIGATIONS DE L'ACQUEREUR

### L'Acquéreur s'engage

3.1 - à mettre à la disposition de l'Accepteur un service permettant de traiter de façon sécurisée les opérations de paiement effectuées via ce service, à le gérer et à l'exploiter ;

3.2 - à assurer la maintenance de la plate-forme de paiement utilisée dans le cadre de ce service ;

3.3 - en cas de dysfonctionnement des moyens de télécommunication mis en oeuvre par l'Acquéreur, à intervenir pour obtenir, dans les meilleurs délais, le rétablissement du service ;

3.4 - à mettre en oeuvre dans les délais prévus par le Schéma les évolutions demandées par la communauté des établissements de crédit relatives :

- au paiement par carte, conformément aux règles opérationnelles et aux normes applicatives en matière de paiement à distance,
- aux raccordements au réseau d'autorisation,
- aux procédures d'authentification des titulaires de cartes et des Accepteurs, conformément aux spécifications techniques approuvées par le Schéma ;

3.5 - à mettre en place les moyens nécessaires pour préserver la confidentialité des informations transmises par l'Accepteur ;

3.6 - à favoriser une disponibilité du service 24h/24 et 7j/7. Le service pourra toutefois être interrompu temporairement pour des besoins de maintenance et d'évolution, sous réserve d'une information préalable à l'Accepteur ; cette information pourra être réalisée par l'insertion d'un message sur le site Internet de la plate-forme de paiement ;

3.7 - à communiquer à l'Accepteur et à sa demande les mesures des indicateurs de qualité liés au service (durée de disponibilité) pour en apprécier l'impact sur le niveau de service global.

## ARTICLE 4 – OBLIGATIONS DE L'ACCEPTEUR

### L'Accepteur s'engage

4.1 - à collaborer activement et régulièrement avec la Banque dans l'intérêt du bon fonctionnement du service ;

4.2 - à se doter des moyens nécessaires à la bonne exécution du service et à utiliser les moyens mis à sa disposition conformément à ce qui est prévu au présent Contrat ;



4.3 - à s'assurer que les paramétrages de Webfactures qu'il réalise, ainsi que les utilisations qu'il en fait, répondent à ses besoins. En cas de doute, l'Accepteur prend contact avec l'Acquéreur.

4.4 - Afin de prévenir les tentatives de récupération de données confidentielles par des tiers, à inviter chacun de ses clients à ne communiquer les données de leur carte de paiement qu'après s'être assuré que la plate-forme de règlement contient des données cohérentes concernant sa facture (identification du Client final, montant de la facture).

4.5 - à effectuer obligatoirement une demande d'autorisation lorsqu'elle s'applique à l'acceptation d'un ordre de paiement transmis par Internet, ainsi qu'un contrôle du CV2X donné par le titulaire de la carte à sa demande.

## **ARTICLE 5 – RESPONSABILITE DE L'ACQUEREUR**

5.1 – L'Acquéreur est responsable de la bonne exécution des prestations objet du présent Contrat.

5.2 – L'Acquéreur assume une obligation de mise en œuvre de moyens en ce qui concerne la réception et le traitement des informations. L'Acquéreur n'effectue pas le transport des informations, il n'assume donc aucune responsabilité en ce qui concerne le transport des informations.

Sa responsabilité, limitée aux dommages directs, ne pourra être recherchée que s'il est établi qu'il a commis une faute lourde, étant précisé que les réclamations relatives aux opérations effectuées dans le cadre du présent contrat devront être formulées dans un délai de 6 mois à compter de l'événement dommageable, à peine de forclusion..

L'Acquéreur n'est pas responsable lorsque l'inexécution de ses obligations résulte d'un cas de force majeure notamment en cas d'interruption du service liée au transport des informations ou au système informatique de l'Accepteur, sauf dans ce dernier cas s'il est prouvé que ce dysfonctionnement provient d'un vice des logiciels mis à la disposition de l'Accepteur par la Banque. La Banque ne pourra être tenue responsable en cas de dommage provenant du non respect par l'Accepteur des préconisations d'installation des logiciels.

Pour les opérations non bancaires, le délai pour formuler une réclamation est celui du droit commun (5 ans).

5.3 La Banque n'est pas responsable des conséquences, frais, coûts ou dommages induits par les évolutions des normes du Schéma, entraînant, entre autre, une augmentation du nombre et/ou de la taille des autorisations, des télécollectes et des télé-paramétrages.

5.4 - Dans le cas où des malfaçons ou erreurs, qui remettraient en cause l'utilisation des travaux par l'Accepteur, se seraient produites à la suite d'une anomalie de fonctionnement des appareils de traitement de la Banque ou d'erreurs commises par son personnel, la Banque s'engage à corriger ou éventuellement à refaire les dits travaux à ses frais exclusifs dans les meilleurs délais.

5.5 - Les malfaçons ou erreurs ci-dessus énoncées devront être signalées par écrit à la Banque dans les quinze jours suivant la réception des états et documents ou logiciels et, en toute hypothèse, avant le traitement suivant. A défaut, la correction des travaux erronés sera facturée en sus à l'Accepteur. Copie des états erronés devra être remise à la Banque en même temps que la lettre signalant les malfaçons ou erreurs.

Au cas où la responsabilité de l'Acquéreur serait retenue, les Parties conviennent expressément que, toutes sommes confondues, la Banque ne sera pas tenue de payer un montant supérieur au tarif d'adhésion annuel au service stipulé dans les Conditions Particulières.

## **ARTICLE 6 – SECRET PROFESSIONNEL ET CONFIDENTIALITE**

6.1 – L'Acquéreur rappelle qu'il est tenu au secret professionnel.

6.2- L'Accepteur l'autorise toutefois à communiquer aux sous-traitants les informations strictement nécessaires à l'exécution par ces derniers des opérations sous-traitées.

6.3 - L'Accepteur s'engage à mettre en œuvre et à faire mettre en œuvre les dispositifs (matériels, procédures, ...) permettant d'assurer la confidentialité des informations communiquées, des documents de spécifications techniques, des éléments sécuritaires remis par la Banque dans le cadre du présent Contrat. L'Accepteur se porte fort du respect de cet engagement de confidentialité par ses préposés et sous-traitants. A cet effet, l'Accepteur s'engage notamment à faire signer à ses préposés et sous-traitants un engagement de confidentialité.

## **ARTICLE 7 - DROITS DE PROPRIETE INTELLECTUELLE**

Il n'y a pas de transfert des droits de propriété intellectuelle sur les logiciels (versions actuelles et futures) et documentations échangés dans le cadre du présent contrat. Leur utilisation par l'Accepteur est impérativement limitée aux fonctions décrites et nécessaires à l'exécution du présent contrat.

Le droit d'utilisation des logiciels susvisés n'emporte pas le droit de faire toute opération interdite telle qu'indiquée ci-après, y compris dans le cadre de sa destination contractuelle. Par "opération interdite" les parties entendent la reproduction permanente ou provisoire du logiciel autre qu'une copie de sauvegarde, en tout ou en partie par tout moyen et sous toute forme, ainsi que la traduction, l'adaptation, l'arrangement ou toute autre modification du logiciel et la reproduction du logiciel en résultant, la correction desdits éléments par soi-même ou par des tiers des éventuelles anomalies des éléments logiciels, la mise sur le marché à titre onéreux ou gratuit.

En cas de cessation ou de résiliation du contrat, l'Accepteur s'engage à restituer à la Banque les logiciels, dispositifs de sécurité et documents en sa possession sur lesquels il n'a aucun droit de propriété et que la Banque a mis à sa disposition et à retirer immédiatement de son site Internet et de ses supports de vente tout signe d'acceptation des cartes et toute indication du système





de paiement Webfactures.

## **ARTICLE 8 – PROTECTION DES DONNEES PERSONNELLES**

Par « traitement », il faut entendre toute opération ou ensemble d'opérations appliquées à des données à caractère personnel, effectuées ou non à l'aide de procédés automatisés, telles que la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

Chacune des Parties, pour les traitements effectués sous sa responsabilité, s'engage à respecter les obligations résultant de l'application de la législation applicable relative à la protection des données à caractère personnel et de la vie privée. Les Parties s'engagent à collaborer activement afin de permettre l'accomplissement des formalités déclaratives leur incombant et, le cas échéant, obtenir les autorisations des autorités de protection des données compétentes. Les Parties s'abstiennent de toute action susceptible de mettre l'autre Partie en situation de manquement à la loi précitée.

## **ARTICLE 9 - MODIFICATIONS**

L'Acquéreur attire l'attention de l'Accepteur, qui se déclare pleinement informé et en accepte les risques ainsi que leurs éventuelles conséquences financières, sur le fait que toute demande de modifications en cours de contrat est susceptible de générer des retards parfois significatifs par rapport aux plannings prévisionnels.

Les modifications, extensions ou diminutions des travaux demandées par l'Accepteur ne seront exécutées qu'après avoir fait l'objet d'un devis de l'Acquéreur et signature d'un avenant au présent Contrat.

Toutefois, lorsqu'une semblable modification, extension ou diminution apparaîtra nécessaire à l'Acquéreur, notamment en raison d'une insuffisance ou d'une inexactitude des renseignements fournis par l'Accepteur avant la signature du Contrat et en rendant l'exécution impossible ou plus onéreuse, l'Acquéreur fera connaître cette modification au moins huit jours à l'avance, par lettre recommandée avec accusé de réception, ou à l'occasion de comptes-rendus de réunion. Sauf refus de l'Accepteur signifié par lettre recommandée, la modification ainsi notifiée pourra être mise en œuvre de plein droit par l'Acquéreur.

En cas de refus de l'Accepteur des modifications apparues nécessaires, l'Acquéreur pourra résilier le Contrat et obtenir une indemnité pour les travaux effectués jusqu'à la date de résiliation.

## **ARTICLE 10 - PROTECTION DES FICHIERS ET DOCUMENTS**

L'Accepteur se prémunira impérativement contre tous risques concernant les fichiers, programmes et autres documents confiés à la Banque en constituant un double de ceux-ci. L'Accepteur se déclare à cet égard pleinement informé de ce que les supports informatisés présentent une fragilité et une fiabilité nécessitant d'une part, de vérifier la qualité et l'exhaustivité de ses sauvegardes, d'autre part, de réaliser des sauvegardes multiples.

Pour sa part, et sous réserve du respect de ses obligations de sauvegarde par l'Accepteur, la Banque s'engage à reconstituer dans les meilleurs délais les documents et fichiers qui lui auraient été confiés et qui viendraient à être perdus ou auraient été rendus inutilisables par sa faute, sous réserve que l'Accepteur lui fournisse les données nécessaires à leur reconstitution. Dans ce cas, l'Accepteur renonce à tout autre recours contre la Banque hormis cette reconstitution.

## **ARTICLE 11 – PRIX**

11.1 - Tous les prix mentionnés dans les Conditions Particulières au titre du raccordement et de l'accès aux fonctions de la plateforme de paiement et de services Webaffaires Gestion - Webfactures, hors les coûts stipulés "à la transaction" sont hors taxes, hors fournitures.

11.2 - Toute modification importante des données ou volumes, de l'objet et de l'étendue des interventions, devra donner lieu à l'établissement d'un devis et à la signature d'un avenant au présent Contrat.

## **ARTICLE 12 - FACTURATION ET REGLEMENT**

12.1 - Sauf dispositions contraires figurant aux Conditions Particulières, les factures de l'Acquéreur sont payables sans escompte dès réception, par débit du compte de l'Accepteur.

12.2 - Dans le cas où une facture ne serait pas réglée dans les trente jours de son envoi par l'Acquéreur à l'Accepteur, l'Acquéreur, après relance de l'Accepteur par lettre recommandée avec demande d'avis de réception restée sans effet pendant huit jours, aura la faculté de suspendre l'exécution du service Webfactures jusqu'au règlement de la facture en souffrance, sans que cette suspension puisse être considérée comme une résiliation de Contrat du fait de l'Acquéreur, ni ouvre un quelconque droit à indemnisation pour l'Accepteur.

12.3 - En outre, à compter du trente et unième jour, la somme due portera intérêt au taux de 1,5 fois le taux d'intérêt légal sans qu'une mise en demeure préalable soit nécessaire, même par simple lettre, l'intérêt étant dû et exigible par le seul fait de l'échéance du terme contractuel. Tout mois commencé sera entièrement dû.





## **ARTICLE 13 – SECURITE DES ECHANGES**

La sécurité entre le poste informatique ou terminal de l'Accepteur et Webaffaires Gestion - Webfactures et la sécurité du paiement entre le poste informatique ou terminal du Client final et Webaffaires Gestion - Webfactures repose sur la mise en œuvre de la technologie SecureSocket Layer (SSL). Les informations relatives au paiement sont systématiquement cryptées lorsqu'elles circulent sur Internet. L'Acquéreur gère la sécurité des échanges et s'assure de la protection des secrets (clés de chiffrement) et de leur gestion (tirage, affectation, constitution de certificat, changement périodique), selon les niveaux spécifiés par les différents Schémas (CB, VISA, MASTERCARD,...). La plate-forme de paiement sécurisée qui assure le traitement des données des cartes bancaires répond aux exigences du standard PCI DSS.

L'adhésion au Contrat garantit à l'Accepteur la mise en conformité du système de paiement Webfactures avec les standards interbancaires du Groupement des Cartes Bancaires, les standards internationaux et ceux mis en œuvre par chacun des émetteurs de cartes mentionnées ci-dessus.

## **ARTICLE 14 - CONVENTION SUR LA PREUVE**

Les Parties déclarent que les enregistrements électroniques effectués par les systèmes informatiques de l'Acquéreur ou exploités par ce dernier constituent la preuve des opérations de paiement remises à l'Acquéreur et font foi entre les Parties tant qu'aucun écrit contradictoirement authentifié et fiable, venant remettre en cause ces enregistrements, n'est pas produit.

En cas de transmission à distance de données, les éléments tels que notamment la teneur d'une information ou le moment de sa réception ou de son émission, ainsi que la qualité des données reçues feront foi par priorité tels que figurant sur les systèmes de l'Acquéreur, ou tels qu'authentifiés par les procédures informatisées de l'Acquéreur.

## **ARTICLE 15 - APPROBATION DES DOCUMENTS**

Tous documents, comptes-rendus, rapports d'analyse fonctionnelle ou organique, ou autres adressés par l'Acquéreur à l'Accepteur dans le cadre de l'exécution de l'intervention, seront considérés comme approuvés sans réserve s'ils n'ont fait l'objet d'une contestation par écrit dans les quinze jours de réception. L'Accepteur s'oblige, en conséquence, à les examiner avec tout le soin et la diligence requis.

## **ARTICLE 16 - SUSPENSION ET RESILIATION**

16.1 - Dans le cas où l'Accepteur ne remplirait pas les obligations mises à sa charge (fourniture de données, accès aux renseignements, etc) nécessaires à la bonne exécution du Contrat par l'Acquéreur, et notamment toutes les obligations découlant de son engagement à collaborer, l'Acquéreur pourra suspendre l'exécution du Contrat sans que cette exécution soit constitutive d'une résiliation.

16.2 En outre, l'Acquéreur se réserve la possibilité à tout moment, sans préavis et sans formalité particulière, de suspendre l'accès à certaines fonctions de la plate-forme de paiement ou de fermer l'accès à la plate-forme de paiement pour des raisons de sécurité, notamment en cas de risque de fraude ou de risque d'atteinte à la confidentialité des données. L'Acquéreur prendra contact avec l'Accepteur dans les plus brefs délais pour l'informer des raisons de ces modifications ou de la fermeture d'accès.

16.3 - La suspension sera notifiée à l'Accepteur par lettre recommandée avec accusé de réception indiquant les motifs de la suspension. L'exécution reprendra une fois les obligations de l'Accepteur remplies, compte tenu des modifications de prix et de délais encourus de ce fait.

16.4 - Le Contrat sera résilié de plein droit, sans formalité judiciaire et sans préjudice de tous dommages et intérêts, si bon semble à l'Acquéreur, en cas de manquement de l'Accepteur à l'une des obligations mise à sa charge et non réparée trente jours après mise en demeure par lettre recommandée avec demande d'avis de réception restée infructueuse. En pareil cas, la Banque aura droit au paiement des travaux exécutés et non facturés, ainsi qu'à une indemnité de résiliation égale à la plus importante des deux sommes suivantes : montant des travaux restant à effectuer par la Banque ou triple de la facturation du mois précédent.

16.5 - En cas de mise en redressement judiciaire ou de liquidation judiciaire prononcée à l'encontre de l'une des Parties, le Contrat sera résilié de plein droit, sauf décision contraire des tribunaux ou de l'administrateur judiciaire.

16.6 - En cas de clôture du compte courant, pour quelle que cause que ce soit, le Contrat sera immédiatement résilié.

16.7 - En cas de cession partielle ou totale du fonds de commerce, le Contrat sera immédiatement résilié.

16.8 - Au cas où les volumes de traitement viendraient à être nuls pendant 3 mois consécutifs, l'Acquéreur n'aura aucune obligation de conserver quelque élément que ce soit et notamment les programmes dédiés. Dans ce cas, l'Acquéreur pourra également procéder à la résiliation du Contrat.

16.9 - Le cas échéant, la réalisation de la prestation peut être soumise à des volumes minimaux de traitement confiés par l'Accepteur.

## **ARTICLE 17 - PRIORITE DES DOCUMENTS CONTRACTUELS**

Sauf dérogations, les documents contractuels, en cas de contradiction ou de difficulté d'interprétation prévalent dans l'ordre



décroissant suivant :

1. les Conditions Particulières,
2. les Conditions Générales,
3. les annexes,
4. les propositions commerciales éventuelles de la Banque, sous réserve d'une référence expresse dans les Conditions Particulières,
5. les comptes rendus de réunions et échanges de correspondance.

## **ARTICLE 18 - CLAUSES GENERALES**

18.1 - En cas de difficulté d'interprétation entre les titres des articles et le texte de leur contenu, le texte des articles primera.

18.2 - Les dispositions du Contrat représentent l'intégralité de l'accord conclu entre les Parties. Elles prévalent sur toute proposition ou accord antérieur, ainsi que sur toute autre communication antérieure entre les Parties ayant trait à l'objet des présentes.

18.3 - Aucun document ne pourra engendrer des obligations au titre du présent Contrat s'il n'a fait l'objet d'un accord signé ou accepté par les deux Parties.

18.4 - Le fait que l'une des deux Parties n'ait pas exigé l'application d'une clause quelconque du présent Contrat, que ce soit de façon permanente ou temporaire, ne pourra en aucun cas être considéré comme une renonciation aux droits de cette Partie découlant de ladite clause ; il ne s'agirait dans ce cas que d'une situation tolérée pour le passé.

18.5 - Si l'une quelconque des stipulations du Contrat est nulle au regard d'une règle de droit ou d'une loi en vigueur, elle sera réputée non écrite, mais n'entraînera pas la nullité du Contrat.

## **ARTICLE 19 – FORCE MAJEURE**

Aucune des deux Parties ne sera tenue pour responsable vis-à-vis de l'autre de l'inexécution ou des retards dans l'exécution du présent Contrat qui serait du fait de l'autre Partie, ou de la survenance d'un cas de force majeure. Outre les cas habituels retenus par la jurisprudence, les Parties conviennent de considérer comme cas de force majeure : l'intervention des autorités civiles ou militaires, l'interruption du service liée au transport des informations ou au système informatique de l'Accepteur, l'interruption totale ou partielle des réseaux de communications, le refus de licence d'importation, les grèves totales ou partielles des prestataires de l'Acquéreur, les conflits sociaux, les intempéries, épidémies, incendies, tempêtes, inondations, dégâts des eaux, les blocages des réseaux de télécommunications, les dysfonctionnements de matériels ou toute autre cause qui serait raisonnablement hors du contrôle de la Partie concernée et tous autres cas indépendants de la volonté expresse des Parties empêchant l'exécution normale du Contrat.

## **ARTICLE 20 – REFERENCEMENT ET MARQUES**

20.1 – Sauf convention contraire, l'Acquéreur est autorisé au seul droit, non exclusif, pour la durée du présent Contrat, à citer à titre de référence le nom de l'Accepteur et les prestations réalisées.

En outre, l'Accepteur autorise expressément, dans les mêmes termes, l'Acquéreur à créer, le cas échéant, un lien hypertexte vers son site à partir du site [www.webaffaires.org](http://www.webaffaires.org) (site assurant la promotion des offres Webaffaires et Webfactures auprès des commerçants).

20.2 - Les marques Webfactures et Webaffaires ainsi que celle du nom de l'Acquéreur et des sociétés de son Groupe étant déposées, elles ne peuvent être utilisées sans l'autorisation préalable et écrite de l'entité concernée. Toutefois, l'Acquéreur accorde à l'Accepteur, le seul droit non exclusif, pour la durée du présent Contrat, de faire figurer les éléments du logo Webfactures ou du logo Webaffaires sur ces documents commerciaux et, le cas échéant son site internet.

## **ARTICLE 21 – DOMICILE ET LOI APPLICABLE**

21.1 - Pour l'exécution des présentes, ou ce qui en sera la suite ou la conséquence, l'Accepteur élit domicile en son siège social et l'Acquéreur en son siège central ou à défaut, en son siège social. Chacune des Parties déclare agir à titre professionnel et dans le cadre d'une activité commerciale.

21.2 - Le présent Contrat est régi par la loi française

## **ARTICLE 22 – LITIGES**

Tout litige né de la validité, de l'interprétation ou de l'exécution du Contrat sera tranché par le Tribunal de Commerce de Paris auquel les Parties attribuent expressément compétence, même en cas de pluralité de défendeur, appel en garantie, urgence ou référé ou encore opposition sur injonction de payer.



## Annexe 1 – Détail des services et options WEBFACTURES

### 1 - LA MISE EN OEUVRE DE WEBFACTURES

L'Accepteur, en accord avec l'Acquéreur, détermine les éléments particuliers de fonctionnement du service, selon notamment les systèmes de paiement qu'il a lui-même choisis et de leurs caractéristiques.

L'Accepteur note que le crédit en compte des transactions enregistrées à partir du site Webfactures s'effectue en euros.

### 2 - L'ACQUISITION DU PAIEMENT PAR CARTE

#### 2.1. Acceptation des cartes de paiement

Les cartes acceptées sont les cartes de paiement portant les Marques des Schémas CB, VISA, Mastercard et, selon les options souscrites, les cartes JCB, American Express Carte France et Pluriel (Franfinance). Les règlements des transactions par American Express Carte France, JCB et Pluriel de Franfinance sont régis par les conditions générales propres à chacun des établissements émetteurs. L'adhésion aux systèmes de paiement par carte, JCB, American Express Carte France et Pluriel de Franfinance nécessite l'adhésion préalable ou conjointe au système de paiement Webfactures. De même, la résiliation du contrat d'adhésion au système de paiement Webfactures entraîne la résiliation du contrat d'adhésion aux systèmes de paiement par carte JCB, American Express Carte France et Pluriel de Franfinance.

#### 2.2. Demande d'autorisation

Pour chaque transaction, une demande d'autorisation est effectuée en ligne.

Pour l'ensemble des systèmes de paiement dans chaque cas d'achat sur Internet, une réponse systématique est retournée vers le Client final et vers l'Accepteur, quelle que soit l'issue de la transaction (acceptée, refusée ou abandonnée). La réponse adressée à l'Accepteur ne comprend en aucun cas l'intégralité du numéro ou la date de fin de validité de la carte du Client final.

En fin de journée, un journal des transactions traitées est transmis à l'Accepteur, sous format texte ou tableur et les transactions acceptées sont traitées sous forme de remises par l'Acquéreur pour mise en compensation.

Après la compensation interbancaire, s'effectue le recouvrement :

- la Banque créditée le compte bancaire de l'Accepteur selon les conditions fixées dans les Conditions Particulières,
- la Banque du Client final débite le compte bancaire de ce dernier.

#### 2.3 Justificatif d'acceptation

En adhérant au service Webfactures, l'Accepteur demande à être inscrit dans le programme 3D Secure auprès des Schémas CB (Paiement sécurisé CB), Visa (VisaSecure©) et Mastercard (Mastercard Identity Check©).

Ce dernier génère, pour les paiements effectués au moyen de Cartes portant les marques CB, Visa, V PAY, Electron, Mastercard ou Maestro par un internaute à partir de la page de paiement Webfactures de l'Accepteur, en complément de la demande d'autorisation, une demande d'authentification du titulaire de la Carte.

L'Accepteur peut toutefois demander à l'émetteur (uniquement au titre de 3D Secure V2 et dans le cas d'une opération de paiement d'un montant inférieur ou égal à 30 € ou d'un Paiement Récurrent de rang supérieur à 1) de ne pas appliquer de procédure d'authentification forte du titulaire de la carte. L'émetteur est libre d'accepter ou non la demande.

Les opérations réalisées sans authentification forte à la demande de l'émetteur sont effectuées sans justificatif d'acceptation. La réponse à la demande d'authentification forte ou à la demande d'exemption à l'authentification forte est systématiquement transmise à l'Accepteur dans le journal des transactions envoyé chaque matin. Elle est également disponible via le portail de gestion, onglet « Gestion des transactions », menu « Transactions ».

L'Accepteur s'interdit de demander au titulaire de la Carte de lui communiquer le code d'authentification ou de sécurité que lui a transmis l'émetteur de la Carte, à l'exception du cryptogramme visuel.

L'obtention du justificatif d'acceptation, visé à l'article 5.1.2 des Conditions Générales du contrat d'acceptation en paiement à distance sécurisé par cartes de paiement (VADS), se matérialise uniquement par la réponse « YES » à la demande d'authentification avec la présence d'un cryptogramme qui doit être obligatoirement transmis dans la demande d'autorisation qui suit.

À défaut d'obtention de ce justificatif d'acceptation, l'opération de paiement ne sera pas garantie si le titulaire de la Carte conteste l'ordre de paiement. Lorsque la Carte n'est pas émise par l'Acquéreur, les contestations relatives aux opérations sont matérialisées par un « impayé » adressé par l'émetteur à l'Acquéreur.

L'Acquéreur pourra contrepasser le montant des opérations contestées par les titulaires de Carte pour lesquelles un justificatif d'acceptation n'a pas été obtenu.

### 3 - MISE A DISPOSITION DE MODULES D'AIDE A LA DECISION

#### 3.1. Détection de cartes étrangères

En choisissant de souscrire au contrôle « Pays d'émission de la carte », l'Accepteur est informé au moment de la transaction et après autorisation, que la carte présentée aux fins de règlement est émise par un établissement de paiement situé hors de France.

#### 3.2. Gestion d'une liste grise des cartes



En choisissant de souscrire au contrôle « Liste grise », l'Accepteur est informé au moment de la transaction que la carte est référencée dans la liste des cartes indésirables. Cette liste est gérée et mise à jour par le commerçant à partir de l'outil gestion de Webaffaires Gestion - Webfactures.

### **3.3. Information E-Carte Bleue**

Ce contrôle complémentaire à la demande d'autorisation permet à l'Accepteur de détecter les e-CB.

Fonctionnement de la e-CB : l'internaute ne saisit pas son numéro de carte réelle lors de l'acte d'achat sur Internet. Il accède à un serveur sécurisé grâce à des données de sécurité personnalisées que lui a procuré sa banque. Le serveur attribue un numéro de carte unique à l'internaute « e-numéro » pour un achat unique, chez un commerçant donné.

### **3.4. Contrôle de similitude des pays carte et adresse IP**

Ce contrôle permet à l'Accepteur de vérifier la concordance entre le pays de la carte et l'adresse IP.

### **3.5. Détection Cartes à autorisation systématique**

Ce contrôle permet à l'Accepteur de détecter les cartes à autorisation systématique

### **3.6. L'attention de l'Accepteur est attirée sur le fait que les modules d'aide à la décision :**

Ne sont que de simples indicateurs ou paramètres dont la mise en œuvre est sous la seule responsabilité de l'Accepteur. Ils ne constituent pour l'Accepteur qu'une aide à la prise de décision d'accepter ou non le paiement au moyen de la carte concernée, et qu'ils ne sauraient en aucun cas, constituer l'argument unique et décisif motivant de la part de l'Accepteur un refus de procéder à la transaction avec le porteur de la dite carte, l'Accepteur pouvant toujours demander à ce dernier de fournir, relativement au paiement suspendu, tout complément d'information jugé nécessaire, comme de régler la transaction avec un autre moyen ou instrument de paiement (chèque, virement, etc.).

## **4 - LE RAPPROCHEMENT BANCAIRE**

En choisissant de souscrire au module « journal de rapprochement bancaire », l'Accepteur peut obtenir le dénotage de façon automatique, entre les transactions adressées en banque au travers de la solution Webfactures et celles effectivement comptabilisées en banque.

Ces informations sont transmises chaque jour par e-mail dans un fichier reprenant l'ensemble des transactions de la veille.

## **5 - WEBFAIRES GESTION - WEBFACTURES**

Dans le cadre du Schéma de carte de paiement (CB, , Visa, Mastercard, American Express Carte France et Pluriel de Franfinance), l'Accepteur bénéficie d'un accès à un ensemble d'outils nécessaire à la gestion des transactions enregistrées. A partir d'une adresse Internet sécurisée, d'un code utilisateur et d'un mot de passe, le(s) représentant(s) habilité(s) par l'Accepteur peut (peuvent) accéder à la consultation et la recherche d'une transaction ou d'un ensemble de transactions, à la création d'une transaction, à l'annulation ou la validation différée de la transaction avant remise en banque, et à la possibilité de procéder à des remboursements de transactions.

L'adresse IP, mentionnée pour toute transaction consultée, est un moyen de preuve imparfait. L'Acquéreur attire l'attention de l'Accepteur sur le fait que l'adresse IP est susceptible d'être contrefaite, altérée ou modifiée. Par ailleurs, l'adresse IP étant une donnée permettant l'identification, l'Accepteur doit respecter la réglementation française et européenne applicable en matière de protection des données à caractère personnel. A ce titre, l'Accepteur devra, d'une part mentionner la collecte des adresses IP dans son registre des traitements, d'autre part faire figurer un avertissement sur son site informant les internautes de la récupération et de l'éventuelle utilisation de ces données ou à défaut de site internet, par tout moyen préalablement à la proposition faite de payer la facture en ligne. En cas de non respect de ces obligations, la Banque Acquéreur se réserve le droit de résilier le contrat Webfactures selon les termes de l'article 8 des « Conditions générales d'adhésion au système de paiement à distance sécurisé par cartes ».

## **7 – CONDITIONS FINANCIERES DES TRANSACTIONS CARTES BANCAIRES**

Les commissions précisées dans les Conditions Particulières du présent Contrat, sont établies en fonction des estimations de chiffres d'affaires, panier moyen et répartition zone domestique / zone étranger fournies par l'Accepteur. Elles sont donc susceptibles d'un ajustement tarifaire après une période d'observation.



## Annexe 2 - REFERENTIEL SECURITAIRE ACCEPTEUR

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

### Exigence 1 (E1)

#### Gérer la sécurité du système commercial et d'acceptation au sein de l'entreprise

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

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

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

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

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

### Exigence 2 (E2)

#### 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 applicatif commercial et 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 de paiement sensibles liées à la Carte du titulaire 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 commercial et d'acceptation

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

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

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

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

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



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

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

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

#### **Exigence 5 (E5)**

##### **Contrôler l'accès au système commercial et d'acceptation**

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

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

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

#### **Exigence 6 (E6)**

##### **Gérer les accès autorisés au système commercial et d'acceptation**

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

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

L'identification doit être nominative y compris pour les administrateurs et les personnels de maintenance. Les droits accordés à ceux-ci doivent être restreints aux opérations qui leur sont autorisées.

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

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

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

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

Les tentatives d'accès doivent être limitées en nombre.

Les mots de passe doivent être changés régulièrement.

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

#### **Exigence 7 (E7)**

##### **Surveiller les accès au système commercial et d'acceptation**

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

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

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

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

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

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

#### **Exigence 8 (E8)**

##### **Contrôler l'introduction de logiciels pernecieux**

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

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



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

**Exigence 9 (E9)**  
**Appliquer les correctifs de 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 commercial et d'acceptation**

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

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

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

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

**Exigence 12 (E12)**  
**Assurer la traçabilité des opérations techniques (administration et maintenance)**

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

**Exigence 13 (E13)**  
**Maintenir l'intégrité des informations relatives au système commercial et 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 commercial et 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 de paiement sensibles liées à la Carte du titulaire ne peuvent être utilisées que pour exécuter l'ordre de paiement et pour traiter les réclamations. Le cryptogramme visuel d'un titulaire de Carte ne doit en aucun cas être stocké par l'Accepteur .

Les données bancaires et à caractère personnel relatives à une opération de paiement, et notamment les données de paiement sensibles liées à la Carte du titulaire doivent être protégées lors de leur stockage et lors de leur routage sur les réseaux internes et externes au site d'hébergement conformément aux dispositions de la loi Informatique et Libertés et aux recommandations de la CNIL.

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

Le dossier de sécurité propre au système commercial et 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.

<p style="text-align: center;"><b>Exigence 16 (E16)</b> <b>Respecter le standard</b> <b>« Payment Card Industry – Data Security System » PCI-DSS</b></p>
--

En souscrivant le contrat Webfactures, vous adhérez également à ce standard intitulé PCI DSS dont le détail peut être obtenu sur le site internet [www.pcisecuritystandards.org](http://www.pcisecuritystandards.org).

Les obligations ou recommandations qui incombent aux commerçants sont fonction du nombre de transactions annuelles effectuées sur le site marchand. Quatre niveaux ont été définis. Nous vous invitons à vous reporter au document « Programme PCI-DSS » ci-après afin de prendre connaissance du niveau de votre entreprise.





## PROGRAMME PCI/DSS - WEBFACTURES

### Niveaux et actions à mener selon le nombre de transactions :

Sources : programmes PCI-DSS des Réseaux Visa Europe (AIS<sup>(1)</sup>) et Mastercard (SDP<sup>(2)</sup>). <http://www.visaeurope.com/receiving-payments/security/merchants>

[http://www.mastercard.com/us/company/en/whatwedo/determine\\_merchant.html](http://www.mastercard.com/us/company/en/whatwedo/determine_merchant.html)

	Critères	Actions à mener par le commerçant	Périodicité
Niveau 1	Accepteur ayant un volume annuel de transactions Visa et/ou Mastercard supérieur à 6 000 000 ou ayant fait l'objet d'une compromission l'année précédente	<ul style="list-style-type: none"> <li>✓ Rapport de conformité suite à un audit réalisé par un QSA 2 (Qualified Security Assessor) ou une ressource interne agréée auditeur PCI-DSS</li> <li>✓ Scan de vulnérabilité par un ASV<sup>3</sup> (Approved Scan Vendor)</li> <li>✓ Formulaire d'attestation de conformité</li> </ul> Obligation	⇨ Annuelle  ⇨ Trimestrielle
Niveau 2	Accepteur ayant un volume annuel de transactions Visa ou Mastercard compris entre 1 000 000 et 6 000 000	<ul style="list-style-type: none"> <li>✓ Questionnaire de self audit</li> <li>✓ Scan de vulnérabilité par un ASV<sup>3</sup> (Approved Scan Vendor)</li> <li>✓ Formulaire d'attestation de conformité</li> </ul> Obligation	⇨ Annuelle  ⇨ Trimestrielle
Niveau 3	Accepteur ayant un volume annuel de transactions commerce électronique Visa ou Mastercard compris entre 20 000 et 1 000 000	<ul style="list-style-type: none"> <li>✓ Questionnaire de self audit</li> <li>✓ Scan de vulnérabilité par un ASV<sup>3</sup> (Approved Scan Vendor)</li> </ul> Obligation	⇨ Annuelle  ⇨ Trimestrielle
Niveau 4	Accepteur ayant un volume annuel de transactions commerce électronique Visa ou Mastercard inférieur à 20 000	<ul style="list-style-type: none"> <li>✓ Questionnaire de self audit</li> <li>✓ Scan de vulnérabilité par un ASV<sup>3</sup> (Approved Scan Vendor)</li> </ul> Recommandation	⇨ Annuelle  ⇨ Trimestrielle

- ASV (Approved Scan Vendor) : prestataire spécialisé dans la sécurité informatique agréé pour la réalisation de scan de vulnérabilité.

Liste des ASV agréés par PCI-DSS :

[http://www.pcisecuritystandards.org/approved\\_companies\\_providers/approved\\_scanning\\_vendors.php](http://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php)

- QSA (Qualified Security Assessor) : prestataire spécialisé dans la sécurité informatique certifié pour la réalisation d'audits PCI-DSS.

Liste des QSA certifiés par PCI-DSS : [http://www.pcisecuritystandards.org/approved\\_companies\\_providers/qa\\_companies.php](http://www.pcisecuritystandards.org/approved_companies_providers/qa_companies.php)

– Questionnaire de self audit et formulaire d'attestation de conformité disponibles sur le site PCI-DSS :

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

(1) AIS : Account Information Security

(2) SDP : Site Data Protection

(3) Prestataires agréés ou certifiés par PCI-DSS (Conseil des normes de sécurité PSI — <https://fr.pcisecuritystandards.org/minisite/en/>)



## Annexe 3 - PROGRAMME 3D-SECURE

Le protocole 3D Secure (ci-après dénommée « 3DS » et, dans sa première version, « 3DS V1 ») a pour objet la mise en oeuvre, par l'émetteur de la Carte (ci-après dénommé « l'Émetteur »), de moyens techniques aux fins d'authentification forte du titulaire de la Carte.

Ce protocole a évolué (ci-après dénommé « 3DS V2 ») dans le but notamment de se conformer aux exigences de la Directive (UE) 2015/2366 dite « DSP2 » et des normes techniques en découlant (Règlement Délégué (UE) 2018/389) dites « RTS SCA ».

Dans le cadre de 3DS V2, la décision d'authentification du titulaire de la Carte appartient à l'Émetteur. Cette authentification est réalisée soit en interaction avec le titulaire de la Carte (il y a alors authentification forte), soit sans interaction avec ce dernier (dans les cas où une exemption à l'authentification forte est possible), au moyen d'un certain nombre d'informations relatives au contexte de l'opération de paiement (a minima nom et adresse électronique du titulaire de la Carte ainsi que l'adresse de facturation).

Votre attention est attirée sur le fait que certaines opérations de paiement ne peuvent être réalisées dans le cadre de 3DS en raison notamment de la catégorie de la Carte avec laquelle l'opération de paiement est effectuée (ex : cartes prépayées anonymes) ou du mode de paiement utilisé (ex : paiement en l'absence du titulaire de la Carte comme le paiement récurrent).

Par ailleurs, vous vous interdisez de demander au titulaire de la Carte la communication du code d'authentification ou de sécurité que lui a transmis l'Émetteur, à l'exception du cryptogramme visuel.

### Mise en œuvre

La mise en œuvre de 3DS V2, comme de 3DS V1 (possible en présence d'une opération de paiement VISA ou MASTERCARD), requiert :

- (i) Votre enrôlement préalable par l'Acquéreur auprès des Schémas CB (Paiement sécurisé CB – seulement pour 3DS V2), VISA (VisaSecure©) et MASTERCARD (Mastercard Identity Check©).
- (ii) L'utilisation de logiciels spécifiques compris dans les Services Webfactures.

### Authentification du titulaire de la carte

#### Authentification forte

Lors de l'opération de paiement, le titulaire de la Carte est redirigé vers la page d'authentification de l'Émetteur. L'authentification est effectuée conformément à une des/la méthode(s) d'authentification que ce dernier a choisie(s).

#### Exemption à l'authentification forte dans le cadre de 3DS V2 (également dénommée « frictionless »)

L'exemption à l'authentification forte est mise en œuvre à partir des informations que vous avez collectées envoyées par Webfactures (cf documentation technique dédiée mise à la disposition de ce dernier pour connaître le détail de ces informations) et des informations connues par la base de gestion de risque (ex : historique des transactions du titulaire de la Carte) sans interaction avec le titulaire de la Carte.

L'exemption à l'authentification forte est appliquée :

- (i) soit sur votre demande expresse (uniquement dans le cas d'une opération de paiement d'un montant inférieur ou égal à 30€ ou d'un paiement récurrent de rang supérieur à 1) validée par l'Émetteur (en présence d'une telle demande, l'Émetteur peut l'accueillir favorablement – outre la communication des informations obligatoires à Webfactures, la communication d'informations facultatives y concourt fortement - ou la refuser et décider d'appliquer une authentification forte).
- (ii) soit à l'initiative de l'Émetteur.

#### Conséquences de l'authentification forte et de l'exemption à l'authentification forte du titulaire de la Carte

La réponse à la demande d'authentification forte ou à la demande d'exemption à l'authentification forte vous est systématiquement transmise dans le journal des transactions envoyé chaque matin. Elle est également disponible via le portail de gestion, onglet « Gestion des transactions », menu « Transactions ».

L'obtention du justificatif d'acceptation, visé à l'article 4 des Conditions Générales d'acceptation en paiement à distance sécurisé par cartes de paiement – Partie 1 – Conditions Générales communes à tous les schémas, se matérialise uniquement par la réponse « YES » à la demande d'authentification avec la présence d'un cryptogramme qui doit être obligatoirement transmis dans la demande d'autorisation qui suit.

À défaut d'obtention de ce justificatif d'acceptation, l'opération de paiement ne sera pas garantie si le titulaire de la Carte conteste l'ordre de paiement (le titulaire de la Carte peut contester ou répudier – c'est-à-dire nier être l'auteur – une transaction auprès de l'Émetteur, à tout moment, et ce, pendant les 13 (treize) mois qui suivent la date initiale de la transaction). Lorsque la Carte n'est pas émise par la Banque, les contestations relatives aux opérations sont matérialisées par un « impayé » adressé par l'Émetteur à la Banque.

La Banque pourra contrepasser le montant des opérations contestées par les titulaires de Carte pour lesquelles un justificatif d'acceptation n'a pas été obtenu.

#### Demande d'autorisation

À la suite de l'authentification forte ou de l'exemption à l'authentification forte du titulaire de la Carte, une autorisation doit être demandée pour chaque opération de paiement.



La demande d'autorisation doit comporter le cryptogramme visuel (s'il est présent) et les éléments relatifs à la demande d'authentification du titulaire de la Carte concernée.

### Matrice de responsabilité dans le cadre de 3DS V2

Dans le cadre de 3DS V2, les règles applicables en matière de responsabilité sont les suivantes :

		Votre Souhait		
		Pas de souhait	Frictionless	Authentification forte
Décision de l'Emetteur	Frictionless	Possibilité d'obtenir un justificatif d'acceptation (Opération de paiement garantie)	<b>Impossibilité d'obtenir un justificatif d'acceptation (Opération de paiement non garantie)</b>	Possibilité d'obtenir un justificatif d'acceptation (Opération de paiement garantie)
	Authentification forte	Possibilité d'obtenir un justificatif d'acceptation (Opération de paiement garantie)	Possibilité d'obtenir un justificatif d'acceptation (Opération de paiement garantie)	Possibilité d'obtenir un justificatif d'acceptation (Opération de paiement garantie)



## Annexe 4

### NOTE D'INFORMATION : ADHESION AU SYSTEME DE PAIEMENT A DISTANCE - WEBFACTURES

La Banque (Acquéreur) souhaite attirer l'attention du Client (Accepteur) sur un point important en matière de vente sur Internet. Pour les paiements effectués sur Internet via Webfactures le Client ne bénéficie d'une garantie de paiement en cas d'impayé émis pour contestation du porteur, qu'à condition de respecter l'ensemble des mesures de sécurité énoncées à l'article 5 des Conditions Générales du contrat d'acceptation en paiement à distance sécurisé par cartes.

Figurent, notamment, au titre de ces mesures de sécurité, l'obtention :

- d'une autorisation de la transaction,
- d'un justificatif d'Acceptation. Les conditions dans lesquelles ce justificatif d'Acceptation est obtenu sont décrites au point 2.3 de l'Annexe 1.

En cas de respect des mesures de sécurité, y compris l'obtention d'une autorisation de la transaction à l'exception de l'obtention du Certificat d'Acceptation, le paiement de la transaction sera garanti sauf en cas de réclamation du titulaire de la carte lorsque celui-ci conteste la réalité même ou le montant d'une transaction. Le titulaire de la carte dispose d'un délai maximum de 13 mois à compter de la date de débit pour contester une opération.

#### Recommandations concernant l'encaissement des transactions :

Ainsi, afin de limiter le risque de fraude et d'impayé dans le cadre de l'exécution du présent Contrat, la Banque recommande la plus grande vigilance vis-à-vis des transactions qui seront effectuées auprès du Client, notamment dans les cas suivants :

- si l'adresse de livraison est différente de l'adresse de résidence ou bien s'il s'agit d'une poste restante, d'un hôtel, d'un hôpital ou tout autre lieu à caractère public ;
- s'il s'agit de commandes répétitives émanant d'un même client, qui plus est si celui-ci est un nouveau client ;
- si il est demandé au Client, pour des montants importants, de fractionner la somme due (sans doute pour obtenir plus facilement une autorisation) ;
- si il s'agit d'un règlement effectué avec une carte étrangère pour une livraison vers un pays différent de celui de la carte ou bien si l'origine de la carte correspond à un pays dit « à risque » en matière de transactions internationales ;
- si le client propose une autre carte de paiement alors qu'une demande d'autorisation a été refusée sur une (ou plusieurs) carte(s) utilisée(s) précédemment.

Dès lors qu'une transaction semble suspecte au Client, la Banque l'invite soit à proposer à son propre client un autre moyen de paiement, soit à annuler la transaction via l'outil de gestion Webaffaires Gestion - Webfactures.

Pour aider le Client à lutter contre la fraude, la Banque lui conseille de mettre en place les outils sécuritaires qui vous lui sont proposés dans les Conditions Particulières du présent Contrat.

#### Recommandations concernant Webaffaires Gestion - Webfactures :

Webaffaires Gestion - Webfactures permet d'annuler une transaction totalement ou partiellement avant son envoi en compensation dès lors que la fonction Annulation (et non Validation) est sélectionnée, c'est-à-dire tant que le délai de capture n'est pas atteint. Par défaut, le délai de capture est fixé à zéro, ce qui signifie que les transactions sont transmises à la banque du porteur le soir même. Si le Client a besoin d'allonger le délai lui permettant d'annuler une transaction, il doit demander le paramétrage d'un délai de capture supérieur à zéro sans que celui-ci puisse être supérieur à 6 jours.

#### Informations concernant les journaux :

Le journal de transactions, reçu quotidiennement par e-mail, et le journal des opérations ne se substituent pas aux relevés de compte. Seuls les relevés de compte permettent de confirmer que les transactions envoyées en compensation ont bien été créditées. Le Client est invité à contrôler régulièrement ses relevés de compte afin de vérifier les opérations portées au crédit de son compte.

**Crédit du Nord** - SA au capital de EUR 890 263 248 - Siège Social : 28, place Rihour - 59800 Lille - Siège Central : 59, boulevard Haussmann - 75008 Paris - SIREN 456 504 851 - RCS Lille - N° TVA FR83 456 504 851 - Société de courtage d'assurances immatriculée à l'ORIAS sous le N° 07 023 739. **Banque Courtois** - Société Anonyme à Directoire et Conseil de Surveillance au capital de EUR 18 399 504 - SIREN 302 182 258 - RCS Toulouse - N° TVA FR15 302 182 258 - Siège Social : 33, rue de Rémusat - BP 40107 - 31001 Toulouse Cedex 6 - Société de courtage d'assurances immatriculée à l'ORIAS sous le N° 07 023 867. **Banque Kolb** - Société Anonyme à Directoire et Conseil de Surveillance au capital de EUR 14 099 103 - SIREN 825 550 098 - RCS Epinal - N° TVA FR37 825 550 098 - Siège Social : 1 et 3, place du Général de Gaulle - BP 1 - 88501 Mirecourt Cedex - Direction Centrale : 2, place de la République - BP 50528 - 54008 Nancy Cedex. Société de courtage d'assurances immatriculée à l'ORIAS sous le N° 07 023 859. **Banque Laydernier** - Société Anonyme à Directoire et Conseil de Surveillance au capital de EUR 24 788 832 - SIREN 325 520 385 - RCS Annecy - N° TVA FR87 325 520 385 - Siège Social : 10, avenue du Rhône - 74997 Annecy Cedex 09 - Société de courtage d'assurances immatriculée à l'ORIAS sous le N° 07 023 972. **Banque Nuger** - Société Anonyme à Directoire et Conseil de Surveillance au capital de EUR 11 444 581 - SIREN 855 201 463 - RCS Clermont-Ferrand - N° TVA FR88 855 201 463 - Siège Social : 5, place Michel de l'Hospital - 63000 Clermont-Ferrand - Société de courtage d'assurances immatriculée à l'ORIAS sous le N° 07 023 937. **Banque Rhône-Alpes** - Société Anonyme à Directoire et Conseil de Surveillance au capital de EUR 12 562 800 - SIREN 057 502 270 - RCS Grenoble - N° TVA FR82 057 502 270 - Siège Social : 20 et 22, boulevard Edouard Rey - BP 77 - 38041 Grenoble Cedex 9 - Siège Central : 235, Cours Lafayette - 69451 Lyon Cedex 06 - Société de courtage d'assurances immatriculée à l'ORIAS sous le N° 07 023 988. **Banque Tarneaud** - Société Anonyme à Directoire et Conseil de Surveillance au capital de EUR 26 702 768 - SIREN 754 500 551 - RCS Limoges - N° TVA FR69 754 500 551 - Siège Social : 2 et 6, rue Turgot - 87011 Limoges Cedex. Société de courtage d'assurances immatriculée à l'ORIAS sous le N° 07 023 953. **Société Marseillaise de Crédit** - Société Anonyme à Directoire et Conseil de Surveillance au capital de EUR 24 471 936 - SIREN 054 806 542 - RCS Marseille - N° TVA FR79 054 806 542. Siège Social : 75, rue Paradis - 13006 Marseille - Société de Courtage d'Assurances immatriculée à l'ORIAS sous le N° 07 019 357.

Groupe Crédit du Nord  PLUS LOIN, AVEC VOUS

Banque  
Courtois

Banque  
Kolb

Banque  
Laydernier

Banque  
Nuger

Banque  
Rhône-Alpes

Banque  
Tarneaud

Société  
Marseillaise de Crédit

Crédit  
du Nord