Contrat Clic&Pay
Conditions Générales

Les conditions générales du contrat Clic&Pay sont composées :
− (I) des conditions générales d'acceptation en paiement à distance sécurisé par cartes de paiement (VADS) ;
− (II) des conditions générales des Services Clic&Pay ;
− de l'Annexe 1 : Conditions spécifiques ;
− de l'Annexe 2 : Référentiel Sécuritaire Accepteur ;
− et de l'Annexe 3 : Charte « Protection et Sécurité de votre site Clic&Pay ».

Les présentes conditions générales, ensemble avec les conditions particulières ci-avant, constituent le « Contrat ».

I - CONDITIONS GÉNÉRALES D'ACCEPTATION EN PAIEMENT À DISTANCE SÉCURISÉ PAR CARTES DE PAIEMENT (VADS)

Les présentes Conditions Générales d'acceptation en paiement à distance sécurisé par cartes de paiement (VADS) comportent deux parties :

- **Une Partie 1** : Conditions Générales communes à tous les Schémas de cartes de paiement,
- **Une Partie 2** : Dispositions spécifiques à chaque Schéma de cartes de paiement.

PARTIE 1 : CONDITIONS GÉNÉRALES COMMUNES À TOUS LES SCHÉMAS

ARTICLE 1 - DÉFINITIONS

- 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.

- 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.

- 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. Dans le cadre des présentes, la Banque est l'Acquéreur de l'Accepteur.

- 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.

- Par « Règlement », il faut entendre le Règlement UE n °2015/751 du 29 avril 2015 relatif aux commissions d'interchange pour les opérations de paiement liées à une carte.

- 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.

- 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 États membres de l'Union Européenne, l'Islande, le Liechtenstein et la Norvège), elle porte au moins l'une des mentions suivantes :
− « Crédit » ou « Carte de crédit »,
− « Débit »,
− « Prépayé »,
− « Commercial »,
− ou l'équivalent dans une langue étrangère.

- Par « Catégorie de carte », on entend les catégories de Carte suivantes :
− carte de crédit,
− carte de débit,
− carte prépayée,
− carte commerciale.

- 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.

- 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). À 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'oeuvres 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). En outre, les frais de la procédure d'audit seront mis à la charge de l'Accepteur.

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'ACQUÉREUR

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).

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.

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. Inscrire 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 concernée) 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 10 h 00 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.

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 spécifiques figurant en annexe.
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 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.
Lors du paiement, l'Accepteur s'engage à 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.

ARTICLE 5 - MESURES DE SÉCURITÉ

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 sousjacente. 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 prévues dans un délai maximum de 6 (six) jours à compter de la transaction, 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, au plus tard 8 (huit) jours calendaires à compter de la demande par l'Acquéreur, 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 : MODALITÉS 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 ou d'un service, d'un don ou d'une cotisation réglé(e) par Carte doit, avec l'accord de son titulaire, être effectué au titulaire de la Carte utilisée pour l'opération initiale. L'Accepteur doit alors utiliser la procédure dite de « transaction crédit » 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 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, ou encore détecte un risque particulier de fraude.

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 : DURÉE ET RÉSILIATION 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 révèlerait 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 ;

9.2.7. d'une utilisation d'un Système d'Acceptation non agréé ou non approuvé,

9.2.8. d'une utilisation anormale ou détournée du Système d'Acceptation. 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 PRÉVENTION ET DE SANCTION PRISES PAR L'ACQUÉREUR

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 oeuvre 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 DONNÉES À CARACTÈRE 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 seules 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, aux coordonnées du service client indiquées dans les conditions générales du compte bancaire.

11.2.2. À 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 la Carte.

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 de la CNIL 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 oeuvre 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 COMPÉTENTS

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.

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.

ARTICLE 14 : LANGUE DU PRÉSENT CONTRAT

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

PARTIE 2 : DISPOSITIONS SPÉCIFIQUES À CHAQUE SCHÉMA

1. DISPOSITIONS SPÉCIFIQUES AUX SCHÉMAS VISA ET MASTERCARD

ARTICLE 1 - FONCTIONNEMENT DES SCHÉMAS

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'ACQUÉREUR

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.

ARTICLE 5 - PENALITES EN CAS DE COMPROMISSION

En cas de compromission (constitue une compromission un événement qui entraîne, directement ou indirectement, l'accès, la divulgation ou la manipulation non autorisé(e) des données des Cartes – ci-après dénommée « Compromission ») résultant d'un manquement de l'Accepteur et/ou d'un/de ses prestataires autre(s) que L'Acquéreur aux exigences du Référentiel Sécuritaire PCI DSS telles que décrites dans le document « ANNEXE 2 – REFERENTIEL SECURITAIRE ACCEPTEUR » annexé aux présentes, L'Acquéreur appliquera à l'Accepteur :

5.1 – Un forfait de 103 000 €,

5.2 – auquel viendra s'ajouter :

– une pénalité de 3€ par carte dans l'hypothèse où seul le numéro de Carte serait compromis ;

– ou une pénalité de 18€ par carte dans l'hypothèse où le numéro de la Carte ainsi que le cryptogramme visuel seraient compromis.

5.3 – Dans l'hypothèse où l'Accepteur ne régulariserait pas la situation dans le délai imparti par L'Acquéreur pour ce faire, cette dernière appliquera à l'Accepteur une pénalité supplémentaire de 25 000€ par jour de retard.

5.4 – Toutefois, dans le cas particulier où l'Accepteur répartit ses remises de paiements auprès d'au moins 3 (trois) acquéreurs, L'Acquéreur appliquera, en remplacement de la pénalité complémentaire prévue à l'article 5.2 supra un forfait complémentaire conformément à la grille ci-dessous

Forfait initial	50 000 €
Forfait complémentaire en cas de non régularisation dans les 90 jours	+ 30 000 €
Forfait complémentaire en cas de non régularisation dans les 120 jours	+ 50 000 €
Forfait complémentaire en cas de non régularisation dans les 150 jours	+ 50 000 €
Forfait complémentaire en cas de non régularisation dans les 180 jours	+ 75 000 €

5.5 – En cas de nouvelle Compromission imputable à l'Accepteur et/ou à un de/ses prestataires autre(s) que L'Acquéreur dans les 36 (trente-six) mois suivant le constat d'une Compromission résultant d'un manquement de sa part et/ou d'un de/ses prestataires autre(s) que L'Acquéreur, L'Acquéreur appliquera à l'Accepteur un forfait supplémentaire de 60 000€.

5.6 – L'inexécution des exigences issues du Référentiel Sécuritaire PCI DSS sera réputée définitive en cas de survenance d'une Compromission. Dès lors, les pénalités seront dues sans qu'une mise en demeure soit nécessaire. En outre, toutes les pénalités dues au titre d'une Compromission seront débitées sur le compte de l'Accepteur. L'Acquéreur informera au préalable celui-ci afin de lui permettre, le cas échéant, de constituer une provision suffisante.

2. DISPOSITIONS SPÉCIFIQUES AU SCHÉMA CB

ARTICLE 1 - DÉFINITION DU SCHÉMA 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

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.

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 DONNÉES À CARACTÈRE 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.

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 ; − Contacter le Délégué à la protection des données désigné par le GIE CB par courriel à protegezvosdonnees@cartes-bancaires.com.

ARTICLE 5 : MESURES DE PRÉVENTION ET DE SANCTION

5.1. Mesures de prévention et de sanction mises en oeuvre 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 oeuvre 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.

5.2. Mesures de prévention et de sanction mises en oeuvre 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.

5.3. 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.

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

À 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 oeuvre 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 GÉNÉRALES DES SERVICES CLIC&PAY

Clic&Pay est une offre de services (également dénommée les « Services Clic&Pay ») consistant en la mise à disposition de l'Accepteur d'un ensemble de moyens logistiques et humains pour accueillir les paiements lors d'une vente électronique à distance conclue via Internet.

ARTICLE 1 - MOYENS NÉCESSAIRES À L'UTILISATION DES SERVICES CLIC&PAY

Clic&Pay repose sur une plate-forme de paiements sécurisée, élaborée à partir d'une solution de paiement sécurisée dont Lyra Network est propriétaire et qui met en oeuvre des formulaires adaptés au protocole de paiement par Carte et de certains autres moyens de payer (PayPal, American Express...) disponibles en option.

1.1. Pré-requis

L'utilisation de Clic&Pay 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.

L'accès à la plate-forme Clic&Pay se fait via l'utilisation d'un navigateur Internet présentant des normes de sécurité (cryptage notamment) nécessaires au-dit accès. L'Accepteur devra, en outre, mettre en place une liaison sécurisée avec la plate-forme, conformément aux instructions figurant dans les guides techniques qui sont mis à sa disposition. Cette liaison est établie par l'intermédiaire de redirections permettant la communication et l'échange de données entre l'Accepteur et la plate-forme Clic&Pay.

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.

1.2. Installation

L'Accepteur reçoit par e-mail, après l'ouverture de son Contrat, un identifiant lui permettant d'accéder à son outil de gestion en ligne (dénommé « Back- Office Marchand Clic&Pay »). A la première connexion, il lui sera demandé d'entrer son code de première connexion afin de changer nécessairement le mot de passe associé à son identifiant.

La documentation technique et fonctionnelle mise à sa disposition est disponible en libre accès à l'adresse : https:// clicandpay.groupecdn.fr/doc/fr-FR/

Le dialogue entre le site marchand de l'Accepteur et la plate-forme de paiement Clic&Pay s'effectue par un échange de données. Pour créer un paiement, ces données sont envoyées au moyen d'un formulaire HTML ou bien d'une API (interface de programmation applicative Web Services) via le navigateur de l'acheteur. A la fin du paiement, le résultat est transmis au site marchand de deux manières :

- automatiquement au moyen de notifications appelées URL de notification instantanée (également appelée IPN pour Instant Payment Notification),
- par le navigateur lorsque l'acheteur clique sur le bouton pour revenir au site marchand.

Pour assurer la sécurité des échanges, les données sont signées au moyen d'un certificat connu uniquement de l'Accepteur et de la plate-forme Clic&Pay.
Le certificat est propre à l'Accepteur et à l'environnement utilisé. Il permet, dans les conditions définies dans la documentation technique, d'assurer la confidentialité et l'intégrité des paiements et de vérifier l'identité de l'Acquéreur de la transaction. Chaque certificat est rattaché à un contrat de mise à disposition de la plate-forme de paiement et à un Accepteur.

L'Accepteur devra mettre en oeuvre les paramétrages décrits dans la documentation technique afin de mettre en place une liaison sécurisée avec la plate-forme Clic&Pay.

L'installation est effectuée par l'Accepteur ou un prestataire technique désigné par l'Accepteur. Il appartient à l'Accepteur de s'assurer que la personne en charge de l'installation dispose des compétences informatiques nécessaires.

Une assistance téléphonique ouverte tous les jours ouvrés (par « jour ouvré», on entend un jour du lundi au vendredi, hors jours fériés) de 9 heures à 18 heures et une assistance par courrier électronique (cf adresse indiquée dans la documentation technique et fonctionnelle) sont mises à disposition de l'Accepteur ou de son prestataire technique.

L'Acquéreur décline toute responsabilité quant à l'implémentation des Services Clic&Pay, en particulier en cas de bug, virus ou de dysfonctionnement du matériel de l'Accepteur consécutif à la mise en place des redirections requises, à moins de démontrer que ce fait est imputable à l'Acquéreur.

L'Accepteur a la garde juridique de son certificat. À cet égard, il s'engage notamment à le conserver de manière strictement confidentielle et à mettre en place toute mesure de sécurité nécessaire à sa protection.

1.3. Tests et passage en production

L'Accepteur peut effectuer des tests selon la procédure décrite dans la documentation technique mise à sa disposition (cf modalités décrites ci-dessus).

Lorsque l'Accepteur a interfacé la page de paiement de Clic&Pay avec son site marchand, qu'il a effectué et validé les tests de pré-production sur le compte de test, il peut alors activer son compte de production.

L'Acquéreur recommande de ne pas utiliser Clic&Pay pour le traitement de véritables opérations de paiement avant que les tests n'aient été réalisés avec succès.

ARTICLE 2 - DESCRIPTION DES SERVICES

Les Services Clic&Pay reposent sur un socle standard composé:

2.1. D'un service de paiement en ligne responsive Web design, (en français : conception de sites Web adaptatifs, c'est-à-dire s'adaptant aux différents canaux de communication comme les Smartphones et

tablettes) par Carte des Schémas CB, Visa, Mastercard ou via la solution technique Paylib, en option, par d'autres instruments de paiement, dans un environnement sécurisé par la technologie Transport Layer Security (TLS).

L'appel à la plate-forme Clic&Pay permet à l'Accepteur d'intégrer sur son site Internet des boutons permettant à l'internaute de sélectionner le type de moyens de payer qu'il souhaite proposer (Cartes des Schémas CB, Visa et Mastercard, Paylib et, en option, d'autres moyens de payer: American Express, Paypal, Prélèvement SEPA...). Une fois la solution de paiement sélectionnée, l'internaute est redirigé vers la page de saisie des informations de paiement correspondante.

2.1.1 Paiements par Carte

Lors d'une demande de paiement par Carte des Schémas CB, Visa, Mastercard, 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 comportant de 10 à 19 caractères.

Si l'un de ces contrôles se révèle négatif, l'acheteur est invité à recommencer. Après 3 tentatives infructueuses, la transaction est refusée.

Si les contrôles sont positifs, une demande d'authentification est effectuée, dans le cadre du programme 3D Secure. Si l'authentification est possible, l'internaute 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 sur l'outil de back-office dans le mode « 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 de l'acheteur sur la base des informations (numéro de Carte, date de validité et cryptogramme visuel) communiquées par l'acheteur.

L'Accepteur et l'acheteur sont informés en temps réel du résultat de la demande d'autorisation via un message informatique transmis sur le serveur de l'Accepteur et affiché sur l'écran de l'acheteur.

La transaction autorisée sera envoyée sous forme de remise à l'Acquéreur. À moins que l'Accepteur effectue un paramétrage différent, les remises sont adressées à l'Acquéreur le soir chaque jour ouvré (par « jour ouvré », on entend un jour du lundi au vendredi, hors jours fériés). En cas d'impossibilité d'envoi liée à un problème technique le soir même, la remise est envoyée dans les meilleurs délais.

2.1.2. Paiements par carte CB via le Service Paylib (service non disponible en standard dans l'offre Clic&Pay Lite)

L'Accepteur peut utiliser la plate-forme Clic&Pay pour accepter les paiements par Cartes CB au moyen de la solution technique Paylib (ci-après le « Service Paylib »).

Installation/désinstallation

Le Service Paylib est intégré à la plate-forme Clic&Pay. Pour proposer ce service à ses clients, l'Accepteur peut avoir à l'activer ou le désinstaller en réalisant les paramétrages mentionnés dans le guide technique mis à sa disposition.

Description du Service Paylib

Le Service Paylib est un outil technique permettant à un acheteur, ayant préalablement adhéré au Service Paylib, de stocker de façon sécurisée les références de sa (d'une de ses) Carte(s) afin de réaliser des opérations de paiement par Carte sur Internet (via un PC, une tablette ou un téléphone mobile) avec une authentification sécurisée sans le contraindre à ressaisir à chaque opération les données de sa Carte. Les données de la Carte utilisées pour un paiement réalisé par le biais du Service Paylib sont traitées par la banque du titulaire de la Carte. Ces données ne circulent pas sur Internet.

L'appel à la plate-forme Clic&Pay permet à l'Accepteur d'intégrer sur son site Internet un bouton permettant à l'internaute de choisir d'effectuer son paiement par le biais du Service Paylib. Le parcours du Service Paylib se substitue à la phase de saisie des données Carte (numéro de la Carte, date de fin de validité et cryptogramme visuel) par l'acheteur.

Lors d'une demande de paiement réalisé par le biais du Service Paylib, l'acheteur est redirigé vers une page de saisie de son identifiant et de son mot de passe Paylib (ci-après ensemble les « Codes personnels »). Ses Codes personnels sont ensuite contrôlés.

Si l'un des contrôles se révèle négatif, l'acheteur est invité à recommencer. Après 3 (trois) tentatives infructueuses, la transaction est refusée. Si les contrôles sont positifs, une demande d'authentification est effectuée dans le cadre du Service Paylib. Si l'authentification est possible, l'acheteur est invité à confirmer le paiement en suivant les procédures prévues par sa banque.

La réponse à la demande d'authentification générée par le Service Paylib est systématiquement transmise, quelle qu'en soit l'issue, à l'Accepteur, par redirection internet sécurisée TLS (Transport Layer Security). Le résultat de cette demande d'authentification est disponible dans l'outil de back-office dans le mode « consultation de transaction » et/ou dans le journal des transactions envoyé chaque matin.

Puis une demande d'autorisation est réalisée auprès de la banque de l'acheteur sur la base des informations communiquées par Paylib (numéro de Carte, date de validité et jeton prouvant l'authentification de l'acheteur (CAVV).

L'acheteur est informé en temps réel du résultat de la demande d'autorisation via un message informatique transmis sur son écran. Il est ensuite basculé sur la plate-forme Clic&Pay sur laquelle figure une nouvelle information sur le statut de la transaction « Carte ».

Les opérations de paiement réalisées par le biais du Service Paylib sont garanties dans les mêmes conditions que pour tous les paiements par Carte, telles que détaillées dans les Conditions Générales - Partie 1, à l'exception des vérifications de la période de validité, du type de Carte utilisé et du cryptogramme visuel (CVX2) qui ne sont pas exigées de l'Accepteur.

Les autres fonctionnalités du Service Clic&Pay restent applicables à un paiement par Carte effectué par le biais du Service Paylib.

Référencement et marques

L'Accepteur dont le Service Paylib est activé autorise l'Acquéreur et Paylib Services (enregistrée sous le numéro 522 048 032 RCS Paris) à citer à titre de référence, comme utilisateur du Service Paylib, le nom, le logo, la marque et un lien vers le site Internet de l'Accepteur (notamment sur le site www.paylib.fr).

La marque et le logo Paylib étant déposés, ils ne peuvent être utilisés sans l'autorisation préalable et écrite de l'Acquéreur. 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 Paylib sur les pages réservées au paiement dans le cadre de la mise en place du Service Paylib.

2.1.3. Paiements par carte via la fonctionnalité de paiement en 1 clic (service non disponible dans l'offre Clic&Pay Lite)

2.1.3.1. Description de la fonctionnalité de paiement en 1 clic Le paiement en 1 clic offre la possibilité à l'Accepteur de proposer à ses clients d'enregistrer les données de leur Carte (numéro de la Carte et date d'expiration) CB, Visa, Visa Electron, V PAY, Mastercard, Maestro, American Express, si l'Accepteur est affilié au(x) Schéma(s) concerné(s), à partir d'une page de paiement, afin de simplifier le règlement de leurs prochains achats.

Le paiement en 1 clic est décrit dans une documentation technique spécifique mise à disposition des Accepteurs, accessible sur le site documentaire : https://clicandpay.groupecdn.fr/doc/fr-FR/

Paramétrages

Afin que ses clients n'aient pas à ressaisir leur numéro de Carte lors de paiements ultérieurs sur son site, l'Accepteur a la possibilité de leur proposer de l'enregistrer. Pour ce faire, l'Accepteur devra envoyer une requête de paiement en indiquant qu'il souhaite enregistrer les données bancaires à la fin du paiement. Il fournit alors l'identifiant de compte client (ou alias) associé au moyen de

paiement utilisé par le biais d'un enrichissement du champ « vads_identifier ». Cet identifiant sera ensuite utilisé dans chaque requête de paiement.

Le détail technique de ces opérations de paramétrage figure dans la documentation technique mise à disposition des Accepteurs, accessible sur le site documentaire : https://clicandpay.groupecdn.fr/doc/fr-FR/.

Dans le cas où l'identifiant est associé à une Carte expirée, alors de manière automatique, la plate-forme Clic&Pay propose à l'acheteur de renseigner les nouvelles données bancaires afin de réaliser le paiement et mettre à jour l'alias qui lui est associé.

Il appartient à l'Accepteur d'attribuer à ses clients les numéros qui sont renseignés dans le champ « vads_identifier ». L'Accepteur est responsable de l'exactitude des numéros qu'il utilise pour effectuer les paramétrages visés ci-dessus.

L'Accepteur s'engage, en outre, à faire ses meilleurs efforts pour qu'en aucune circonstance le numéro attribué à un client ne soit renseigné dans la requête de paiement concernant un autre client.

Cinématique d'enregistrement du numéro de Carte sur le site de l'Accepteur Si chaque paramétrage visé au paragraphe « Paramétrages » ci-dessus, le client concerné pourra, à partir de la page de paiement Clic&Pay, choisir d'enregistrer sa Carte. Pour ce faire, le client devra cocher une case à côté de laquelle la mention suivante sera insérée :

Le commerçant auprès duquel vous effectuez votre achat en ligne a choisi une banque du Groupe Crédit du Nord. Si vous le souhaitez, les données de votre carte bancaire peuvent être conservées de manière sécurisée et utilisées lors de prochains paiements sur le site Internet de ce commerçant.

La Banque du Groupe Crédit du Nord concernée collecte les données relatives à votre carte bancaire (numéro de la carte et date d'expiration) afin de faciliter vos prochains paiements sur le site Internet du commerçant. Ces données ne sont pas destinées à être utilisées à des fins de prospection commerciale. Elles pourront être communiquées, en tant que de besoin, au regard de la finalité mentionnée ci-dessus au commerçant, aux banques du Groupe Crédit du Nord et au(x) sous-traitant(s) des banques du Groupe Crédit du Nord établi(s) dans l'Union Européenne. Les transferts de données rendus nécessaires interviennent dans des conditions et sous des garanties propres à assurer la protection de vos données personnelles.

Vous disposez d'un droit d'accès, de rectification, d'effacement, de limitation du traitement ainsi que du droit à la portabilité de vos données. Vous pouvez également vous opposer, sous réserve de justifier d'un motif légitime, à ce que vos données fassent l'objet d'un traitement. Cette opposition pourra entraîner l'impossibilité de fournir le service de conservation des données de votre carte bancaire. Ces droits peuvent être exercés auprès du Groupe Crédit du Nord par courrier électronique à l'adresse suivante par courrier postal à l'adresse suivante : CREDIT DU NORD - Direction de la Qualité et des Relations Clientèle - Service Consommateurs - 59 boulevard Haussmann - 75008 - PARIS ou auprès de votre commerçant par le biais de son site Internet.

Le client pourra décider d'attribuer un nom à cette Carte (alias).

Les données ne sont enregistrées que si l'opération de paiement est réalisée. Dans ce cas, une confirmation de l'enregistrement des données est ajoutée au message affiché sur l'écran du client et rappelant les données de la transaction.

Cinématique de paiement avec une Carte préalablement enregistrée Si chaque paramétrage visé au paragraphe « Paramétrages » ci-dessus est effectué, le client pourra, à partir de la page de paiement Clic&Pay, accéder à une liste de Cartes (affichant la marque de la Carte ainsi que le numéro tronqué de la Carte ou le nom qu'il a attribué à la Carte) à partir de laquelle il pourra sélectionner la Carte avec laquelle il souhaite effectuer son paiement. Les données relatives à la Carte sélectionnée seront pré-remplies dans les champs correspondant de la page de paiement.

Pour donner son ordre de paiement, il suffira alors au client de saisir le cryptogramme visuel de la Carte puis de valider cet ordre de paiement au moyen de la solution d'authentification forte proposée par sa banque, si cette dernière le lui demande.

La plate-forme Clic&Pay effectuera ensuite les contrôles nécessaires à l'enregistrement de cet ordre.

Le fait que l'ordre de paiement ait été donné en utilisant la fonctionnalité de paiement en 1 clic sera mentionné dans les journaux de transactions qui sont adressés à l'Accepteur.

Gestion des comptes clients

L'Accepteur s'engage, par ailleurs, à permettre à ses clients de demander à tout moment, par l'intermédiaire de son site Internet, la suppression de chaque Carte dont le numéro a été enregistré.

Pour ce faire, l'Accepteur devra, dans les meilleurs délais et, au plus tard, le 3e jour ouvré (par « jour ouvré » on entend un jour du lundi au vendredi, hors jours fériés) à compter de la demande du client, procéder à cette suppression par l'intermédiaire de son Back-Office Clic&Pay.

2.1.3.2. Stockage des données

L'Acquéreur s'engage à conserver les données enregistrées de manière strictement confidentielle et à adopter des mesures de protection de ces données conformes au standard « Payment Card Industry Data Security Standards » (PCI DSS).

L'Accepteur autorise l'Acquéreur à confier à un sous-traitant, s'engageant à assurer de la même manière la confidentialité des données, tout ou partie de l'exécution du paiement en 1 clic, y compris le stockage des données.

Chaque Partie s'engage à respecter l'ensemble de la réglementation française et européenne applicable en matière de protection des données à caractère personnel (en particulier du Règlement (UE) 2016/679 du 27 avril 2016 sur la protection des données à caractère personnel) et notamment, à effectuer les formalités nécessaires au traitement des données et à respecter le droit d'opposition au traitement des données concernant des personnes physiques.

2.1.3.3. Arrêt de la fonctionnalité de paiement en 1 clic

Chaque Partie pourra à tout moment, en respectant un préavis de 2 (deux) mois, mettre fin aux dispositions relatives à cette fonctionnalité, sans qu'il soit nécessaire d'accomplir aucune autre formalité que l'envoi d'une lettre recommandée avec demande d'avis de réception.

Les autres services Clic&Pay seront poursuivis dans les mêmes conditions.

Il est précisé qu'en cas d'arrêt de la fonctionnalité de paiement en 1 clic, pour quelque raison que ce soit, les numéros de Carte enregistrés par les clients ne pourront pas être transmis à l'Accepteur. L'Accepteur fera son affaire d'informer les clients de l'arrêt de cette fonction.

2.2. D'un Back-Office Clic&Pay

Le Back-Office Clic&Pay permet notamment à l'Accepteur, de consulter, créer, annuler partiellement ou totalement, ou rembourser partiellement ou totalement des transactions effectuées sur son site et de paramétrer l'envoi des remises à l'Acquéreur (certaines de ces fonctions ne sont pas disponibles dans l'offre Clic&Pay Lite). L'accès au Back-Office Clic&Pay n'est possible qu'au moyen d'un identifiant et d'un mot de passe. L'identifiant est envoyé à l'adresse électronique indiquée dans le Contrat de prestation Clic&Pay. Le mot de passe est transmis dans un deuxième e-mail adressé à l'Accepteur. L'Accepteur doit prendre toutes les mesures propres à assurer la confidentialité de son identifiant et de son mot de passe.

Le Back-Office Clic&Pay comporte également un outil d'administration des règles de lutte contre la fraude (dénommé « Module de gestion de risque avancée »), un outil de gestion des utilisateurs (accessible sous réserve de l'autorisation préalable de l'Acquéreur). Le module de gestion de risque avancée (cf. article 2.5 ci-dessous) : il permet à l'Accepteur de gérer les règles de lutte contre la fraude qui pourront s'appliquer à l'un ou plusieurs des moyens de payer de sa boutique, conformément aux instructions figurant dans les guides techniques dont il peut disposer.

L'outil de gestion des utilisateurs : il permet notamment à l'Accepteur de créer, modifier, activer ou désactiver un utilisateur, et de gérer les droits de l'ensemble des utilisateurs.

2.3. D'outils de reporting

Un journal des transactions contenant l'ensemble des transactions de paiement effectuées par les clients est transmis quotidiennement par courrier électronique à l'Accepteur.

Deux journaux de rapprochement peuvent également être transmis quotidiennement (service disponible en option uniquement dans l'offre Clic&Pay Corporate) :

− le Journal de Rapprochement Bancaire (JRB) , permet de rapprocher les montants crédités ou débités sur le compte de l'Accepteur des transactions initialement saisies.
− le Journal de Rapprochement des Impayés (JRI) , permet de rapprocher les impayés débités du compte bancaire de l'Accepteur des transactions initialement saisies.

À cette fin, l'Accepteur autorise l'Acquéreur via le document figurant à la suite du Contrat Clic&Pay à mettre chaque jour à la disposition de Lyra Network les différentes données enregistrées portant sur les transactions traitées et les impayés reçus.

Dans l'hypothèse où l'Accepteur est titulaire de plusieurs Contrats de prestation (autrement dit, dispose de plusieurs sites), il pourra recevoir chaque jour deux journaux de fonds par contrat.

Les données autres que bancaires transitant par Internet ne sont pas protégées et peuvent être falsifiées. Par conséquent, une partie du contenu des journaux de fonds n'est pas garanti et la responsabilité de l'Acquéreur ne pourra donc être engagée à ce titre.

2.4. De modules de paiement open Source (service non disponible dans l'offre Clic&Pay Lite)

L'Accepteur peut télécharger à partir du site : https:// clicandpay.groupecdn.fr/doc/fr-FR/

Les CMS gratuits disponibles utilisés lors de la conception de son site marchand et compatibles avec le module de paiement Clic&Pay. Les modalités d'installation comprennent une documentation complète ainsi que les sources techniques du module de paiement Clic&Pay.

2.5. D'outils sécuritaires via le Module de gestion de risque avancée (service non disponible dans l'offre Clic&Pay Lite)

Les contrôles opérés sur les transactions doivent être paramétrés par l'Accepteur, via son Back-Office Clic&Pay , en vue de déclencher les actions suivantes :

− bloquer une transaction (entraîne le refus immédiat du paiement) ;

− déclencher ou désactiver (sous réserve d'acceptation de l'Accepteur) le recours au dispositif 3D Secure pour le paiement concerné ; − lever une alerte (avertit l'Accepteur selon des cas définis pour mettre en oeuvre certains traitements spécifiques ou lancer des vérifications complémentaires sur la/les transaction(s) concernée(s) comme par exemple, la mise en attente d'une livraison) ;

− valider manuellement une transaction (permet de bloquer temporairement la remise du paiement afin de vérifier la transaction et décider ou non sa validation ou son annulation si cette dernière est jugée à risque).

Les critères pris en compte par le Module de gestion de risque avancée sont de différentes natures :

− critères issus des données du paiement (informations sur la transaction comme le montant, la devise, le panier, l'acheteur, le pays, l'adresse IP, l'e-mail ...) ;

− critères issus de l'analyse du type de Carte (CB, Visa, Mastercard, ...), du produit de la carte (consommateur, commerciale, prépayée), du pays émetteur ;

− critères issus du résultat de 3D Secure (enrôlement du titulaire de la Carte, statut d'authentification) ;

− critères issus du résultat de l'autorisation (code retour de l'autorisation, résultat du transfert de responsabilité) ;

− listes grises pour bloquer le paiement (peuvent être établies sur des Cartes, des adresses IP, des codes BIN, les pays émetteurs de la Carte et le pays des adresses IP).

L'Accepteur a accès à la configuration des contrôles en temps réel via son Back-Office Clic&Pay :

− Contrôles sur le résultat 3D Secure

- paiement 3D Secure avec un titulaire de Carte dont l'authentification ne peut pas être vérifiée
- Carte non-enrôlée au programme 3D Secure
- paiement 3D Secure avec une Carte dont l'enrôlement ne peut pas être vérifié • transfert de responsabilité

− Contrôle sur le montant

- contrôle sur le montant (permet de déclencher une(des) action(s) lorsque la transaction est comprise entre un montant minimum et un montant maximum

− Contrôles sur le moyen de paiement

- contrôle des cartes commerciales
- contrôle des cartes commerciales suivant leur provenance
- contrôle des cartes prépayées
- contrôle des cartes à autorisation systématique
- contrôle des e-Carte-Bleue

− Contrôles sur le panier

- contrôle sur le nombre de produits du panier
- contrôle des produits du panier

− Contrôles sur le pays

- contrôle du pays de l'acheteur (adresse de facturation)
- contrôle du pays de livraison
- contrôle de la variété des pays
- contrôle sur des produits Carte provenant de certains pays
- contrôle des pays pour les paiements par prélèvement SEPA

Un ordre de priorité est défini entre certaines actions, comme par exemple :

− l'action « refuser une transaction » est prioritaire sur l'action « valider manuellement »
− l'action « activer 3D Secure » annule les actions de type « désactiver 3D Secure ».

Par ailleurs, l'Accepteur a la possibilité de souscrire l'option « Gestion des risques sur-mesure ». Cette option lui permettra d'obtenir une analyse des transactions par des experts de la fraude aux fins de création et mise en place de règles sécuritaires spécifiques à son activité.

ARTICLE 3 - PARTICULARITÉS DE CLIC&PAY POUR LES AUTRES SOLUTIONS DE PAIEMENT ET AUTRES OPTIONS

3.1. Acceptation d'autres moyens de payer (non disponible en standard dans l'offre Clic&Pay Lite)

L'Accepteur peut, en option, demander à utiliser la plate-forme Clic&Pay pour accepter des moyens de payer autres que des Cartes des Schémas CB (en ce compris via le Service Paylib), Visa et Mastercard : prélèvement SEPA, Cartes du Schéma American Express, cartes privatives, PayPal, e-Chèques Vacances, etc.

L'accès à certains de ces services nécessite la conclusion d'un contrat spécifique avec un Prestataire de Services de Paiement.

3.1.1. Installation

Pour proposer l'un de ces moyens de payer à ses clients, l'Accepteur doit réaliser les paramétrages exposés dans le guide technique dédié mis à sa disposition.

3.1.2. Description des services optionnels

Pour les cartes privatives, les fonctions du service de paiement en ligne sont détaillées dans la documentation technique mise à disposition de l'Accepteur.

Pour les autres moyens de payer, Clic&Pay consiste à rediriger les clients de l'Accepteur, qui sélectionnent le moyen de payer, soit vers la page de paiement du PSP proposant ce moyen de payer (étant précisé que cette page de paiement n'est pas hébergée par l'Acquéreur), soit vers la page de paiement dédiée.

L'Accepteur dispose également d'un outil de gestion et d'outils de reporting tels que décrits à l'article 2. Toutefois, seules les fonctions de l'outil de gestion et les outils reporting mentionnés dans le guide technique pour chaque moyen de payer seront mis à la disposition de l'Accepteur.

3.2. Autres options

En fonction des besoins exprimés par l'Accepteur, la Banque pourra lui proposer d'autres options.

ARTICLE 4 - OBLIGATIONS DE L'ACQUÉREUR

L'Acquéreur s'engage à :

− mettre à la disposition de l'Accepteur les services décrits à l'article 2 et, en option, à l'article 3 ;

− assurer la maintenance des logiciels utilisés dans le cadre des Services Clic&Pay ;

− en cas de dysfonctionnement des moyens de télécommunication mis en oeuvre par l'Acquéreur, à intervenir pour rétablir le service dans les meilleurs délais ;

− mettre en oeuvre dans les délais prévus par le GIE « CB » les évolutions demandées par la communauté des établissements de crédit et de paiement relatives :

- au paiement par Carte, conformément aux règles opérationnelles et aux normes applicables en matière de vente 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 GIE « CB ».

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

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

ARTICLE 5 - OBLIGATIONS DE L'ACCEPTEUR

L'Accepteur s'engage à :

− collaborer activement et régulièrement avec l'Acquéreur dans l'intérêt du bon fonctionnement des Services Clic&Pay ;

− se doter des moyens nécessaires à la bonne exécution de Clic&Pay et à utiliser les moyens mis à sa disposition conformément à ce qui est prévu au présent Contrat ;

− s'assurer que les paramétrages des Services Clic&Pay qu'il réalise ainsi que les utilisations qu'il en fait, répond à ses besoins. En cas de doute, l'Accepteur prendra contact avec l'Acquéreur ;

− concernant l'ensemble des Services Clic&Pay mis à sa disposition, à ne pas les utiliser pour un autre usage que celui prévu par le présent Contrat, à ne pas les décompiler en dehors de l'exception prévue à l'article L.122-6-1 du Code de la propriété intellectuelle, à respecter les consignes d'utilisation, à installer les mises à jour fournies par l'Acquéreur dans un délai maximum de 6 (six) mois et à informer l'Acquéreur en cas de dysfonctionnement ; − respecter les règles de protection et sécurité des Services Clic&Pay figurant en Annexe 3 ainsi que toute autre mesure de protection dont l'Acquéreur informerait l'Accepteur.

ARTICLE 6 - RESPONSABILITÉ DE L'ACQUÉREUR

6.1. L'Acquéreur est responsable de la bonne exécution des prestations, objet des présentes Conditions Générales. L'Acquéreur assume une obligation de mise en oeuvre en ce qui concerne la réception des informations. La responsabilité de l'Acquéreur, limitée aux dommages directs, ne pourra être recherchée que s'il est établi qu'il a commis une faute ou s'est rendu coupable d'une négligence. De convention expresse entre les Parties, est notamment considéré comme préjudice indirect, tout préjudice commercial, perte de chiffre d'affaires, de bénéfice, de commande ou de clientèle.

6.2. Les réclamations relatives aux opérations bancaires peuvent être effectuées dans les conditions prévues au I des Conditions Générales - Partie 1. Au cas où la responsabilité de l'Acquéreur serait retenue, les Parties conviennent expressément que, toutes sommes confondues, l'Acquéreur ne sera pas tenu de payer un montant supérieur aux sommes payées par l'Accepteur au titre des Services Clic&Pay au cours des 12 (douze) derniers mois. Les réclamations relatives au fonctionnement de la plate-forme de paiement ou de l'ensemble des logiciels doivent être formulées dans un délai d'un an, sous peine de prescription des actions afférentes.

6.3. Au cas où la responsabilité de l'Acquéreur serait retenue pour les services techniques, les Parties conviennent expressément que, toutes sommes confondues, l'Acquéreur ne sera pas tenu de payer un montant supérieur aux sommes payées par l'Accepteur au titre du présent Contrat au cours des 12 (douze) derniers mois.

6.4. La responsabilité de l'Acquéreur ne pourra jamais être engagée :
− pour tout dommage lié au non respect par l'Accepteur des préconisations d'installation des logiciels, et tout dommage lié à leur utilisation ; − pour tout dommage lié au fait que les services ne sont pas conformes à des besoins spécifiques envisagés par l'Accepteur ;
− pour tout dommage lié au non respect par l'Accepteur de dispositions légales ou du droit des tiers sur son site Internet ;
− pour tout dommage lié à l'inexécution de ses obligations tenant à un cas de force majeure.

Outre les cas habituellement retenus par la jurisprudence française, les Parties conviennent expressément de considérer comme cas de force majeure : les grèves totales ou partielles des prestataires de la Banque, les intempéries, les épidémies, incendies, tempêtes, inondations, dégâts des eaux, les blocages des réseaux de télécommunications et tous autres cas indépendants de la volonté expresse des Parties empêchant l'exécution normale du Contrat.

ARTICLE 7 - PROTECTION DES DONNÉES À CARACTÈRE PERSONNEL

Le terme « Données à caractère personnel » signifie toute information relative à une personne identifiée ou identifiable, directement ou indirectement, en particulier par référence à un numéro d'identification ou à un ou plusieurs élément(s) spécifique(s) la concernant.

L'Acquéreur et l'Accepteur s'engagent 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'Acquéreur et l'Accepteur s'engagent à collaborer activement afin de permettre l'accomplissement des formalités leur incombant et, le cas échéant, obtenir les autorisations des autorités de protection des données compétentes (en particulier s'agissant du module de gestion de risque avancée). Les Parties s'abstiennent de toute action susceptible de mettre l'autre Partie en situation de manquement à la loi précitée. Par ailleurs, l'Accepteur, s'engage notamment à :

− se conformer à l'obligation d'information des personnes telle que prévue par l'article 32 de la loi n°78-17 du 6 janvier 1978 précitée et faire figurer au pied de tout questionnaire ou formulaire, y compris électronique, les mentions légales prévues par ledit article, dont les modalités d'exercice des droits d'accès, de rectification et d'opposition, les éventuels transferts de données hors de l'Espace Économique Européen. Notamment, les Titulaires de Cartes dont les Données à caractère personnel ont été recueillies doivent pouvoir disposer des droits d'accès, de rectification, d'effacement, d'opposition, de limitation ainsi que du droit à la portabilité auprès de l'Accepteur. À cet égard, l'Accepteur s'engage d'ores et déjà à leur permettre d'exercer ces droits ;

− prendre, et s'assurer que son personnel et toute personne agissant pour son compte prend, dans la mesure nécessaire au respect de ses obligations contractuelles, toute mesure nécessaire pour préserver et faire respecter l'intégrité, la sécurité et la confidentialité des Données à caractère personnel ;

− satisfaire avec diligence par écrit aux demandes d'information de l'Acquéreur, dans un délai de 5 (cinq) jours ouvrés (par « jour

ouvré », on entend un jour du lundi au vendredi, hors jours fériés) à compter de la demande, afin de lui permettre de répondre (i) aux demandes d'exercice de leurs droits présentées par les personnes concernées ou (ii) aux demandes présentées par les autorités de protection des données ou par ses délégués à la protection des données (Data Protection Officer) ;

− informer sans délai l'Acquéreur de toute demande relative aux Données à caractère personnel.

ARTICLE 8 - DROITS DE PROPRIÉTÉ INTELLECTUELLE

Il n'y a pas de transfert des droits de propriété intellectuelle sur l'ensemble des logiciels (versions actuelles et futures) et les documentations mis à disposition de l'Accepteur par l'Acquéreur 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 de l'ensemble des logiciels susvisées 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 de l'ensemble des logiciels 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 de l'ensemble des logiciels et la reproduction de l'ensemble des logiciels en résultant, la correction desdits éléments par soimême ou par des tiers des éventuelles anomalies des éléments de l'ensemble des logiciels, la mise sur le marché à titre onéreux ou gratuit. L'Accepteur est responsable de l'ensemble des services, informations, signes, images ou de toutes autres données figurant sur son site Internet.

ARTICLE 9 - SUSPENSION DES SERVICES

L'Acquéreur se réserve la possibilité à tout moment, sans préavis et sans formalité particulière, de suspendre l'accès à tout ou partie des fonctionnalités de la plate-forme Clic&Pay ou de fermer l'accès à la plate-forme 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.

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 la nécessité d'une part, de vérifier la qualité et l'exhaustivité de ses sauvegardes informatiques, d'autre part, de réaliser des sauvegardes multiples. Pour sa part, et sous réserve du respect de ces obligations de sauvegarde par l'Accepteur, l'Acquéreur s'engage à reconstituer dans les meilleurs délais les documents et fichiers qui 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 l'Acquéreur hormis cette reconstitution.

ARTICLE 11 - SÉCURITÉ

La sécurité du paiement entre le poste acheteur de l'internaute et le service de paiement Clic&Pay repose sur la mise en oeuvre d'une technologie sécurisée appelée Transport Layer Security (TLS). Les informations relatives au paiement sont systématiquement chiffrées 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 Schémas (GIE « CB », Visa, Mastercard, American Express...).

La plate-forme de paiement sécurisée qui assure le Traitement des données des cartes bancaires répond aux exigences du standard PCI-DSS.

Le transport des informations entre l'Accepteur, l'Acquéreur et la plate-forme de paiement Lyra Network est effectué par l'intermédiaire d'un réseau de transmission de données qui n'est pas géré par l'Acquéreur. Elle n'assume donc aucune responsabilité en ce qui concerne le transport des informations.

ARTICLE 12 - CONVENTION SUR LA 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 GIE « CB » prévaudront sur ceux produits par l'Accepteur « CB », à moins que ce dernier ne démontre l'absence de fiabilité ou d'authenticité des documents produits par l'Acquéreur ou le GIE « CB ».

ARTICLE 13 - APPROBATION DES DOCUMENTS

Tous documents, comptes rendus, rapports d'analyse fonctionnelle ou organique, applications 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 15 (quinze) jours de leur réception. L'Accepteur s'oblige, en conséquence, à les examiner avec tout le soin et la diligence requis.

ARTICLE 14 - RÉFÉRENCEMENT ET MARQUES

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.

La marque Clic&Pay By Groupe Crédit du Nord et celle de l'Acquéreur étant déposées, elles ne peuvent être utilisées sans l'autorisation préalable et écrite de l'Acquéreur. 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 Clic&Pay et de l'Acquéreur, sur les pages réservées au paiement dans le cadre de la mise en place de la solution Clic&Pay. Dans le cas où l'Accepteur utilise les éléments du logo, la mise en exploitation de Clic&Pay se fait après accord de l'Acquéreur.

ARTICLE 15 - CONDITIONS FINANCIÈRES

Les conditions financières sont déterminées dans les Conditions Particulières du Contrat Clic&Pay ou dans tout autre document approuvé par les Parties. Sauf disposition contraire, les prix sont exprimés hors taxes, hors éventuels frais de transport et d'expédition.

Lorsque les conditions financières font référence au tarif en vigueur selon la brochure tarifaire applicable à l'Accepteur, ce tarif peut être modifié selon les modalités prévues dans les conditions générales de fonctionnement du compte sur lequel les opérations sont facturées.

Les sommes dues au titre de Clic&Pay sont débitées sur le compte de l'Accepteur. L'abonnement mensuel est débité au début de chaque mois.

Tout mois commencé est entièrement dû.

Dans le cas où des frais ou commissions ne seraient pas réglés dans les 30 (trente) jours de leur exigibilité, l'Acquéreur, après une relance de l'Accepteur par lettre recommandée avec demande d'avis de réception restée vaine pendant 8 (huit) jours, aura la faculté de suspendre les Services Clic&Pay jusqu'au règlement des sommes dues, sans que cette suspension puisse être considérée comme une résiliation de Contrat du fait de l'Acquéreur ouvre un quelconque droit à indemnisation pour l'Accepteur. En outre, à compter du 31e (trente et unième) jour, la somme due portera intérêt au taux de 3 fois le taux d'intérêt légal sans qu'une mise en demeure préalable ne soit nécessaire.

ANNEXE 1 - CONDITIONS SPÉCIFIQUES

Les présentes Conditions spécifiques du Contrat Clic&Pay viennent s'ajouter aux dispositions du Contrat Clic&Pay.

1. ACCEPTATION DES CARTES AUTRES QUE LES CARTES DES SCHÉMAS CB, VISA ET MASTERCARD

Pour pouvoir accepter des Cartes telles que des Cartes American Express, l'Accepteur doit conclure un contrat d'acceptation avec le Schéma concerné.

Les règlements des transactions par American Express sont effectués dans les conditions convenues dans ce contrat.

2. JUSTIFICATIF D'ACCEPTATION

En adhérant aux Services Clic&Pay, 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 Clic&Pay 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 Back-Office Clic&Pay, menu « Gestion » / onglet « Transactions en cours ».

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 du I des Conditions Générales - Partie 1 : Acceptation en paiement à distance sécurisé (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 contre-passer le montant des opérations contestées par les titulaires de Carte pour lesquelles un justificatif d'acceptation n'a pas été obtenu.

3. MODALITÉS PARTICULIÈRES DE PAIEMENT À DISTANCE PAR CARTES DES SCHÉMAS CB, VISA OU MASTERCARD

3.1. Dispositions communes à l'ensemble des modalités particulières

Les modalités particulières de paiement à distance par Cartes des Schémas CB, Visa ou Mastercard visées au présent article sont accessibles sur demande expresse de l'Accepteur et sous réserve de l'acceptation de l'Acquéreur.

L'Accepteur reconnaît avoir été informé que ces modalités ne constituent pas un mode normal d'utilisation du Système d'Acceptation et accepte de supporter les risques y afférents.

3.2. La création à partir d'un numéro de Carte

L'Accepteur peut transmettre à l'Acquéreur une opération de paiement qu'il a constituée à partir des données que son client lui communique par téléphone, fax, e-mail ou autre canal de communication. Pour constituer une transaction, l'Accepteur doit obtenir le numéro de la Carte, sa date de validité et le cryptogramme visuel. L'Accepteur s'engage à ne constituer que des opérations pour lesquelles un ordre de paiement par Carte lui a été préalablement donné.

Par dérogation à l'article 4 du I des Conditions Générales - Partie 1 : Acceptation en paiement à distance sécurisé (VADS) par cartes de paiement, les paiements à distance réalisés selon ces modalités ne sont pas garantis en cas de contestation du titulaire de la Carte.

3.3. L'annulation

L'Accepteur peut annuler totalement ou partiellement une transaction avant que celle-ci ne soit transmise à l'Acquéreur.

L'accepteur s'engage à obtenir l'accord du titulaire de la Carte avant d'annuler totalement ou partiellement une opération. Par dérogation à l'article 4 du I des Conditions Générales - Partie 1 : Acceptation en paiement à distance sécurisé (VADS) par cartes de paiement, les opérations partiellement annulées ne sont pas garanties si le titulaire de la Carte conteste le montant de l'opération.

3.4. Le paiement différé supérieur à 6 jours

L'Accepteur peut prévoir, par l'intermédiaire de Clic&Pay, de transmettre à l'Acquéreur une opération de plus de 6 (six) jours après qu'elle ait été effectuée. Dans ce cas, la demande d'autorisation pour le montant total de l'opération est effectuée avant la transmission de l'opération à l'Acquéreur.

Par dérogation à l'article 4 du I des Conditions Générales - Partie 1 : Acceptation en paiement à distance sécurisé (VADS) par cartes de paiement, les paiements à distance réalisés selon ces modalités ne sont pas garantis en cas de contestation du titulaire de la Carte.

Release - cmn_ContratClicPay - 21/07/2021

ANNEXE 2 - RÉFÉRENTIEL SÉCURITAIRE 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 oeuvre et contrôlées.
Le pare-feu doit être mis à jour systématiquement lorsque des vulnérabilités sont identifiées sur ses logiciels (logiciel pare-feu et logiciel d'exploitation) et corrigeables.
Le serveur supportant le pare-feu doit être doté d'un outil de contrôle de l'intégrité.
Le pare-feu doit assurer l'enregistrement des accès et des tentatives d'accès dans un journal d'audit. Celui-ci doit être analysé quotidiennement.

EXIGENCE 5 (E5) : CONTRÔLER L'ACCÈS AU SYSTÈME COMMERCIAL ET 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 PERNICIEUX

Les procédures et les responsabilités de gestion ayant trait à la protection anti-virus et à la restauration des données et des logiciels en cas d'attaque par virus doivent être définies et formalisées.
L'installation et la mise à jour régulière des logiciels de détection et d'élimination des virus doivent être effectuées sur la totalité des machines ayant accès au système commercial et d'acceptation.
La vérification anti-virus doit être exécutée quotidiennement sur la totalité des machines.

EXIGENCE 9 (E9) : APPLIQUER LES CORRECTIFS DE 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.

EXIGENCE 16 (E16) : RESPECTER LE STANDARD « Payment Card Industry - Data Security System » PCI-DSS

En souscrivant le contrat Clic&Pay, vous adhérez également à ce standard intitulé PCI DSS dont le détail peut être obtenu sur le site internet 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 - CLIC&PAY

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

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.	✓ Rapport de conformité suite à un audit réalisé par un QSA[2] (Qualified Security Assessor) ou une ressource interne agréée auditeur PCI-DSS ✓ Scan de vulnérabilité par un ASV[3] (Approved Scan Vendor) ✓ Formulaire d'attestation de conformité Obligation	→ Annuelle → Trimestrielle
Niveau 2	Accepteur ayant un volume annuel de transactions Visa ou Mastercard compris entre 1 000 000 et 6 000 000 transactions	✓ Questionnaire de self audit ✓ Scan de vulnérabilité par un ASV[3] (Approved Scan Vendor) ✓ Formulaire d'attestation de conformité 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 transactions	✓ Questionnaire de self audit ✓ Scan de vulnérabilité par un ASV[3] (Approved Scan Vendor) Obligation	→ Annuelle → Trimestrielle
Niveau 4	Accepteur ayant un volume annuel de transactions commerce électronique Visa ou Mastercard inférieur à 20 000 transactions	✓ Questionnaire de self audit ✓ Scan de vulnérabilité par un ASV[3] (Approved Scan Vendor) 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

− 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/qsa_companies.php

− Questionnaire de self audit et formulaire d'attestation de conformité disponibles sur le site PCI-DSS https://fr.pcisecuritystandards.org/minisite/env2/

Pour plus d'informations sur la sécurisation de vos données monétiques et les normes PCI : http://www.cartes-bancaires.com/IMG/pdf/PCIDSS.pdf

(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/env2/)

ANNEXE 3 - CHARTE : PROTECTION ET SÉCURITÉ DE VOTRE SITE CLIC&PAY

1. INFORMATIONS IMPORTANTES RELATIVES AU CERTIFICAT ET À LA SÉCURITÉ DES ÉCHANGES

Le dialogue entre le site marchand de l'Accepteur et la plate-forme de paiement Clic&Pay s'effectue par un échange de données. Pour créer un paiement, ces données sont envoyées au moyen d'un formulaire HTML via le navigateur de l'acheteur. A la fin du paiement, le résultat est transmis au site marchand de deux manières :

- automatiquement au moyen de notifications appelées URL de notification instantanée (également appelée IPN pour Instant Payment Notification) ;
- par le navigateur lorsque l'acheteur clique sur le bouton pour revenir au site marchand.

Pour assurer la sécurité des échanges, les données sont signées au moyen d'un certificat connu uniquement de l'Accepteur et de la plate-forme de paiement (cf article 1 du II des Conditions générales). Deux types de certificat sont mis à disposition :

- le certificat de test qui permet de générer la signature d'un formulaire en mode test.
- le certificat de production qui permet de générer la signature d'un formulaire en mode production.

2. RÈGLES ÉLÉMENTAIRES DE PROTECTION DU CERTIFICAT

L'intégrité des informations échangées est garantie par un échange de signatures numériques entre la plate-forme de paiement Clic&Pay et le site marchand de l'Accepteur.

Dès le premier paiement réalisé avec une Carte réelle, le certificat de production est masqué pour des raisons de sécurité. L'Accepteur s'engage à ne pas stocker son certificat dans un fichier facilement accessible et notamment via Internet. En cas de perte, l'Accepteur aura la possibilité d'en générer un nouveau depuis son Back-Office Clic&Pay (cf article 1 du II des Conditions générales).

Release - cmn_ContratClicPay - 21/07/2021

NOTE D'INFORMATION - ACCEPTATION EN PAIEMENT À DISTANCE SÉCURISÉ VIA CLIC&PAY

Vous venez de souscrire un Contrat Clic&Pay auprès de notre établissement, et nous vous en remercions. Nous espérons que l'accès au paiement par Carte sur Internet contribuera au développement de votre chiffre d'affaires. Aussi, afin que cette activité se déroule dans de bonnes conditions, nous souhaitons attirer votre attention sur un point important en matière de vente sur Internet.

Vous ne bénéficiez d'une garantie de paiement en cas d'impayé émis pour contestation du titulaire de la Carte, qu'à condition de respecter l'ensemble des mesures de sécurité énoncées à l'article 5 du I des Conditions Générales - Partie 1. Figurent, notamment, au titre de ces mesures de sécurité, l'obtention: − d'une autorisation de la transaction,

− et d'un justificatif d'acceptation. Les conditions dans lesquelles ce justificatif d'acceptation peut être obtenu sont décrites à l'article 2 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 d'une Carte peut contester ou répudier une transaction auprès de sa banque, à tout moment et ce, pendant les 13 (treize) mois qui suivent la date initiale de la transaction.

1 - RECOMMANDATIONS CONCERNANT L'ENCAISSEMENT DES TRANSACTIONS

Afin de limiter le risque de fraude et d'impayé, nous vous recommandons la plus grande vigilance vis-à-vis des transactions qui seront effectuées sur votre site, 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 l'on vous demande, pour des montants importants, de fractionner la somme due (sans doute pour obtenir plus facilement une autorisation) ; − s'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 vous 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 vous semble suspecte, nous vous invitons soit à proposer à votre client un autre moyen de paiement, soit à annuler la transaction à l'aide du Back-Office Clic&Pay.

Nous vous conseillons également de prévoir la saisie obligatoire de l'adresse e-mail de vos clients sur les bons de commande en ligne et d'envoyer systématiquement un accusé de réception afin de repérer les e-mails non délivrés.

2 - RECOMMANDATIONS CONCERNANT LES SERVICES CLIC&PAY

2.1. Généralités

Vous disposez aussi de la « remontée d'information du code ISO » de la Carte qui vous permet d'identifier le pays d'origine de la Carte utilisée sur votre site.
De plus, nous vous conseillons vivement de mettre en place les outils sécuritaires mis à votre disposition et détaillés dans le Contrat Clic&Pay.
Votre Back-Office Clic&Pay vous permet d'annuler une transaction totalement ou partiellement avant son envoi en compensation, 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 le soir même.
Si vous avez besoin d'allonger le délai vous permettant d'annuler une transaction, vous devez paramétrer un délai de capture supérieur à zéro.
Attention, au-delà de 6 (six) jours, la demande d'autorisation pour le montant total de l'opération n'est effectuée qu'avant la transmission de l'opération à la Banque.

2.2. Informations concernant la procédure de sécurisation des ordres de paiement.

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.

2.3. Pré-requis

La mise en oeuvre 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 Clic&Pay.

2.4. 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 oeuvre à partir des informations que vous avez collectées convoyées par Clic&Pay (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 Clic&Pay, 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.

2.5. 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.

2.6. 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.

2.7 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 :

		Pas de souhait	Frictionless	Authentification forte
DÉCISION DE L'ÉMETTEUR	Frictionless	Possibilité d'obtenir un justificatif d'acceptation (Opération de paiement garantie)	**Impossibilité d'obtenir un justificatif d'acceptation (Opération de paiement non garantie)**	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)

3 - INFORMATIONS CONCERNANT LES JOURNAUX

Les journaux de transactions, reçus quotidiennement par e-mail, 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. Nous vous invitons à contrôler régulièrement vos relevés de compte afin de vérifier les opérations portées au crédit de votre compte.

Pour tout renseignement complémentaire sur l'Offre Clic&Pay, vous pouvez téléphoner au **0811908204** (Service 0,06 € / min + prix appel) depuis la France ou au **0820902119** (Service 0,06 € / min + prix appel) depuis l'étranger, ou envoyer un mail à l'adresse suivante : support@clicandpay.groupecdn.fr.

D'autres informations utiles sont également accessibles sur le site : https://clicandpay.groupecdn.fr/doc/fr-FR/.

Nous espérons que ces recommandations seront de nature à améliorer la sécurité de vos opérations commerciales.