BANQUE POPULAIRE
BOURGOGNE
FRANCHE-COMTÉ
www.bpbfc.banquepopulaire.fr

CONDITIONS GENERALES ET SPECIFIQUES DU CONTRAT D'ACCEPTATION EN PAIEMENT A DISTANCE SECURISE (VADS) PAR CARTE BANCAIRE

CONDITIONS GENERALES ET SPECIFIQUES DU CONTRAT D'ACCEPTATION EN PAIEMENT A DISTANCE SECURISE (VADS) PAR CARTE 5

PARTIE I. CONDITIONS GENERALES COMMUNES A TOUS LES SCHEMAS 5

Avertissement et prérequis indispensable pour recevoir des paiements à distance sécurisés 5

Article 1 : Définitions 5

Article 2 : Marques et Catégories de Cartes acceptées 6

Article 3 : Souscription du Contrat et convention de preuve 6

Article 4 : Obligations de l'Accepteur 6

Article 5 - Obligations de l'Acquéreur 8

Article 6 : Garantie de paiement 8

Article 7 : Mesures de sécurité 9

Article 8 - Mesures de prévention et de sanction prises par l'Acquéreur 9

Article 9 : Modifications du Contrat 10

Article 10 : Durée et résiliation du Contrat 10

Article 11 - Modalités annexes de fonctionnement 11

Article 12 : Secret bancaire et protection des données à caractère personnel 11

Article 13 : Non renonciation 11

Article 14 : Loi applicable/Tribunaux compétents 11

Article 15 : Langue du Contrat 12

Article 16 : Confidentialité 12

PARTIE II CONDITIONS SPECIFIQUES D'ACCEPTATION EN PAIEMENT A DISTANCE SECURISE PROPRES A CHAQUE SCHEMA 12

PARTIE II. 1 CONDITIONS SPECIFIQUES POUR LES OPERATIONS REALISEES SELON LE SCHEMA« CB » 12

Article préliminaire 12

Article 1 : Conditions liées à la garantie de paiement des opérations de paiement « CB » 12

Article 2 : Délai maximum de transmission des opérations de paiement « CB » à l'Acquéreur 12

Article 3 : Litiges commerciaux 12

Article 4 : Suspension et clôture du contrat pour le Schéma « CB » 12

Article 5 : Communication des Commissions Interbancaires de Paiement (interchange) de « CB » 12

PARTIE II.2 CONDITIONS SPECIFIQUES D'ACCEPTATION EN PAIEMENT A DISTANCE SECURISE POUR LES OPERATIONS REALISEES SELON LES SCHEMAS« VISA », « VISA ELECTRON » OU « VPAY » 13

Article préliminaire 13

Article 1 : Conditions liées à la garantie de paiement des opérations de paiement « Visa », « Visa Electron et « VPAY » 13

Article 2 : Suspension ou clôture du contrat à la demande des Schémas« Visa », « Visa Electron » ou « VPAY » 13

Article 3 : Acceptation des Cartes Visa, « Visa Electron » ou « VPAY » émises hors UE 13

Article 4 : Communication des Commissions Interbancaires de Paiement (interchange) de « Visa », « Visa Electron » ou « VPAY » 13

PARTIE II.3 Conditions spécifiques d'acceptation en paiement à distance sécurisé pour les opérations réalisées selon les Schémas « Mastercard » et « Maestro » 13

Article préliminaire 13

Article 1 : Conditions liées à la garantie de paiement des opérations de paiement « Mastercard » ou « Maestro ».13

Article 2 : Suspension ou clôture du contrat à la demande des Schémas « Mastercard » ou « Maestro » 13

Article 3 : Acceptation des Cartes « Mastercard » ou « Maestro » émises hors Union Européenne 13

Article 4 : Communication des Commissions Interbancaires de Paiement (interchange) de « Mastercard » ou « Maestro » 13

PARTIE II.4 CONDITIONS SPECIFIQUES D'ACCEPTATION EN PAIEMENT A DISTANCE SECURISE POUR LES OPERATIONS REALISEES SELON LES SCHEMAS « DINER'S CLUB INTERNATIONAL » OU « DISCOVER » 14

Article préliminaire 14

Article 1 : Conditions liées à la garantie de paiement des opérations de paiement « Diner's Club International » ou « Discover » 14

Article 2 : Suspension ou clôture du contrat à la demande des Schémas « Diner's Club International » ou « Discover » 14

Article 3 : Acceptation des Cartes « Diner's Club International » ou « Discover » émises hors Union Européenne ...14

CONDITIONS SPECIFIQUES AUX CONDITIONS GÉNÉRALES D'ADHÉSION AU SYSTÈME DE PAIEMENT À DISTANCE SÉCURISÉ PAR CARTE BANCAIRE..... 15

Préambule.....15

Article 1 : objet 15

Article 2 : Procédure de paiement sécurisé 3D Secure 15

Article 3 - Garantie du paiement 15

Article 4 : Délai de communication des justificatifs.....15

Article 5 : Conditions tarifaires 16

Article 6 : Obligations de l'accepteur.....16

Article 7 : La non utilisation du contrat 16

La non utilisation de ce contrat sur une période de 12 mois glissants.....16

CYBERPLUS PAIEMENT – VADE-MECUM (Version SystemPay du 01 12 2009) 17

Accès web «outil de gestion de caisse».....17

Paramètre : Capture Day 17

Les sites utilisant CyberPlus paiement.....17

Assistance téléphonique.....17

Acceptation du paiement 17

3 D Secure 18

Fraude 19

Paiement en plusieurs fois / Cartes privatives 19
CONVENTION DE SERVICE CYBERPLUS PAIEMENT 21
CONDITIONS GENERALES 21
1. Définitions 21
2. Objet de la convention de services 21
3. Présentation de la solution Cyberplus paiement 21
4. Conditions des fonctions de la solution Cyberplus paiement 24
5. Conditions des services additionnels 24
6. Documentation du service Cyberplus paiement 26
7. Obligations du client relatives au service Cyberplus paiement 26
8 Disponibilité du service Cyberplus paiement 28
9 Modification et évolution du service Cyberplus paiement 28
10 Assistance clients lors de l'exploitation du service Cyberplus paiement 28
11. Respect de la législation en vigueur 28
12. Droit de propriété intellectuelle 29
13. Confidentialité – secret bancaire 29
14. Conditions financières - facturation et règlement 29
15. Responsabilité de la banque populaire 30
16. Divers 30
17. Modification des conditions 30
18. Durée - suspension et résiliation du contrat 30
19. Entrée en vigueur - élection de domicile - droit applicable - Règlement des litiges 31
CONVENTION DE SERVICE PAIEMENT EXPRESS 32
CONDITIONS GENERALES 32
1 Définitions 32
2 Objet de la convention de services 32
3 Présentation de la solution paiement express 32
4 Conditions des fonctions de la solution paiement express 33
5 Conditions des services additionnels 34
6 Documentation du service paiement express 34
7 Obligations du client relatives au service paiement express 34
8 Disponibilité du service paiement express 35
9 Modification et évolution du service paiement express 35
10 Assistance clients lors de l'exploitation du service paiement express 35
11 Respect de la législation en vigueur 36
12 Droit de propriété intellectuelle 36
13 Confidentialité – secret bancaire 37
14 Conditions financières - facturation et règlement 37

15 Responsabilité de la banque populaire 37
16 Divers 37
17. Durée - suspension et résiliation du contrat 38
18 Entrée en vigueur - élection de domicile - droit applicable - règlement des litiges 38
ANNEXE 1 REFERENTIEL SECURITAIRE ACCEPTEUR 39
Exigence 1 (E1) : Gérer la sécurité du système commercial et de paiement au sein de l'entreprise 39
Exigence 2 (E2) : Gérer l'activité humaine et interne 39
Exigence 3 (E3) : Gérer les accès aux locaux et aux informations 39
Exigence 4 (E4) : Assurer la protection logique du système commercial et de paiement 39
Exigence 5 (E5) : Contrôler l'accès au système commercial et de paiement 39
Exigence 6 (E6) : Gérer les accès autorisés au système commercial et de paiement 39
Exigence 7 (E7) : Surveiller les accès au système commercial et de paiement 39
Exigence 8 (E8) : Contrôler l'introduction de logiciels pernicieux 40
Exigence 9 (E9) : Appliquer les correctifs de sécurité (patches de sécurité) sur les logiciels d'exploitation 40
Exigence 10 (E10) : Gérer les changements de version des logiciels d'exploitation 40
Exigence 11 (E11) : Maintenir l'intégrité des logiciels applicatifs relatifs au système commercial et de paiement 40
Exigence 12 (E12) : Assurer la traçabilité des opérations techniques (administration et maintenance) 40
Exigence 13 (E13) : Maintenir l'intégrité des informations relatives au système commercial et de paiement 40
Exigence 14 (E14) : Protéger la confidentialité des données bancaires 40
Exigence 15 (E15) : Protéger la confidentialité des identifiants – authentifiants des utilisateurs et des administrateurs 40
ANNEXE 2 PRESENTATION GENERALE DES REGLES PCI-DSS 41
ANNEXE 3 TABLEAU DES INTERCHANGES ET SCHEME FEES 42

BANQUE POPULAIRE
BOURGOGNE
FRANCHE-COMTÉ
www.bpbfc.banquepopulaire.fr

CONDITIONS GENERALES ET SPECIFIQUES DU CONTRAT D'ACCEPTATION EN PAIEMENT A DISTANCE SECURISE (VADS) PAR CARTE

Version BPCE du 1er juin 2017

PARTIE I.
CONDITIONS GENERALES COMMUNES A TOUS LES SCHEMAS

Avertissement et prérequis indispensable pour recevoir des paiements à distance sécurisés

Pour éviter, dans le commerce électronique (vente ou location) à distance ou pour le règlement à distance de dons ou cotisations, que tout tiers non autorisé accède aux données liées à la Carte et afin de limiter l'utilisation du seul numéro de Carte pour donner un ordre de paiement, les Schémas ont mis en place des procédures de sécurisation des ordres de paiement donnés à distance par les titulaires de Carte tel que le protocole 3D Secure, ainsi qu'un Référentiel de sécurité PCI DSS et un Référentiel Sécuritaire Accepteur.

Les procédures de sécurisation de paiement à distance consistent en l'authentification 3D Secure du titulaire de la Carte conformément aux spécifications établies par les Schémas (« Protocole 3D Secure »).

L'Accepteur qui ne souhaite pas souscrire à l'offre de plateforme technique e-commerce Cyberplus Paiement commercialisée par l'Acquéreur, doit s'assurer auprès du prestataire technique tiers qu'il choisit pour sa solution de paiement à distance que sa plateforme de service technique e-commerce inclut l'authentification 3D Secure du titulaire de la Carte, et que ce prestataire est en mesure de communiquer à l'Acquéreur et de recevoir de celui-ci toutes les informations nécessaires à la sécurisation des paiements à distance selon le Protocole 3D Secure. Si ledit prestataire ne communique pas les informations précitées à l'Acquéreur et/ou ne traite pas les informations renvoyées par l'Acquéreur, la procédure de sécurisation des paiements ne pourra pas être assurée et l'Accepteur en assumera la responsabilité.

L'Accepteur est également informé que les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité qu'il doit respecter et en particulier celles visées à l'article 7 des Conditions Générales.

Article 1 : Définitions

"Accepteur"
L' "Accepteur" peut être tout commerçant, tout prestataire de services, toute personne exerçant une profession libérale, toute association, toute collectivité publique 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.

"Acquéreur"
Par "Acquéreur", il faut entendre tout établissement de crédit ou de paiement habilité à organiser l'acceptation des Cartes portant la(les) Marque(s) d'un (des) Schéma(s).

"Schéma"
Par "Schéma", il faut entendre un schéma de cartes de paiement, soit un ensemble unique de règles et pratiques régissant l'exécution d'opérations de paiement liées à une carte tel que défini à l'article 2 du Règlement (UE) 2015/751 du Parlement européen et du Conseil du 29 avril 2015.

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

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

Les Marques pouvant être acceptées dans le cadre du présent Contrat sont celles indiquées dans les Conditions Particulières selon le(s) choix exprimé(s) par l'Accepteur.

"Carte(s)"
Par "Carte(s)", on entend un instrument de paiement qui permet à son titulaire d'initier une opération de paiement liée à une Carte. Elle porte une ou plusieurs Marques.

Lorsque la Carte est émise dans l'EEE, elle porte la mention de sa Catégorie, selon la classification indiquée ci-avant ou l'équivalent dans une langue étrangère.

"Catégories de carte"
Par "Catégories de Carte", on entend les catégories de Carte suivantes :
- crédit ou Carte de crédit,
- débit,
- prépayée,
- commerciale (Carte soumise aux règles commerciales du Chapitre III du Règlement (UE) 2015/751 du Parlement européen et du Conseil du 29 avril 2015).

"Système d'Acceptation"
Par "Système d'Acceptation", il faut entendre les logiciels, protocoles et équipements conformes aux spécifications définies par chaque Schéma et nécessaires à l'enregistrement, à la transmission et au traitement sécurisé des ordres de paiement par Carte portant l'une des Marques dudit Schéma. L'Accepteur doit s'assurer que le Système d'Acceptation a fait l'objet d'un agrément par l'entité responsable du Schéma, le cas échéant en consultant la liste des Systèmes d'Acceptation reconnus par l'entité responsable du Schéma.

"Contrat" ou "Présent Contrat"
Par "Contrat" ou "Présent Contrat", il faut entendre ensemble les Conditions Générales et Spécifiques du Contrat d'acceptation en paiement à distance sécurisé (VADS) par Carte, ainsi que les Conditions Particulières des contrats d'acceptation en paiement par Carte (« Condition Particulières ») convenues entre

l'Acquéreur et l'Accepteur, ainsi que leurs Annexes.

"Partie(s)"
Par "Partie(s)", il faut entendre l'Acquéreur et l'Accepteur.

"EEE"
Par "EEE", il faut entendre l'Espace Economique Européen, soit les Etats membres de l'Union Européenne, l'Islande, le Lichtenstein et la Norvège.

Article 2 : Marques et Catégories de Cartes acceptées

L'Accepteur choisit librement les Marques et Catégories de Cartes qu'il souhaite accepter comme moyen de paiement, sous réserve des Marques et Catégories de Cartes dont l'Acquéreur propose l'acceptation.

Les Marques et Catégories de Cartes acceptées au titre du présent Contrat sont celles qui ont été choisies par l'Accepteur dans les Conditions Particulières.

Article 3 : Souscription du Contrat et convention de preuve

3.1 Modalités de souscription du Contrat
L'Accepteur souscrit le Présent Contrat après avoir pris connaissance des Conditions Particulières, des Conditions Générales, des Conditions Spécifiques, de leurs Annexes.

La souscription du Contrat peut être réalisée, soit en agence, en présence d'un conseiller, soit à distance si cette possibilité est offerte, notamment par internet via l'espace client de la banque en ligne de l'Acquéreur.

3.2 Convention de preuve en cas de souscription au contrat par internet
De convention expresse entre les Parties, en cas de souscription à distance par internet, les enregistrements électroniques constituent la preuve de la souscription au présent Contrat. En cas de conflit, les enregistrements électroniques produits par l'Acquéreur prévaudront sur ceux produits par l'Accepteur, à moins que ce dernier ne démontre l'absence de fiabilité ou d'authenticité des documents produits par l'Acquéreur.

Article 4 : Obligations de l'Accepteur

L'Accepteur s'engage à :

4.1 Connaître et respecter les lois et règlements, les dispositions professionnelles ainsi que les bonnes pratiques applicables aux ventes et prestations réalisées à distance, au commerce électronique et notamment aux échanges utilisant les réseaux et les différents terminaux de communication (TV, téléphonie mobile, ordinateur…), et, le cas échéant, aux jeux d'argent et de hasard et/ou de paris, et aux réceptions de dons et règlements de cotisations.

Il reconnaît qu'il doit commercialiser les produits ou prestations de services faisant l'objet d'un paiement à distance sécurisé en se conformant à ces dispositions, notamment fiscales, et à celles qui pourront intervenir.

Lorsque son activité implique des jeux d'argent, de hasard et/ou de paris il s'engage à obtenir toute autorisation et/ou agrément de l'autorité compétente, à respecter les limites autorisées par la loi, et à refuser d'une personne légalement incapable une prise d'enjeux et/ou de paris et/ou une carte de crédit.

4.2 Utiliser le(s) Système(s) d'acceptation en s'abstenant de toute activité illicite, et notamment pénalement sanctionnée telle que, et sans que la liste soit limitative :
- la mise en péril de mineurs, d'actes de pédophilie ;
- les actes de contrefaçon d'œuvres protégées par un droit de propriété intellectuelle ;
- les actes de contrefaçon de moyens ou d'instruments de paiements ;
- le non-respect de l'utilisation des données personnelles collectées ;
- les atteintes aux systèmes de traitement automatisé des données ;
- les actes de blanchiment et de fraude ;
- le non-respect des dispositions relatives aux jeux d'argent et de hasard, aux courses de chevaux, aux loteries ;
- le non-respect des dispositions relatives à l'exercice des professions règlementées.

4.3 Signaler immédiatement à l'Acquéreur :
- toute modification affectant sa forme juridique ou concernant ses représentants légaux ;
- toute modification de son activité, notamment de l'ajout d'une ou plusieurs branches d'activité, la cessation d'une ou plusieurs branches d'activités et plus généralement de tout événement modifiant les conditions d'exercice de son activité.

4.4 Signaler au public l'acceptation des Marques, Catégories de Cartes qu'il accepte ou qu'il refuse, par l'apposition 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.

4.5 Accepter les paiements à distance sécurisés effectués avec les Cartes telles que listées dans les Conditions Particulières en contrepartie d'actes de vente ou de fournitures de prestations de services offerts à sa clientèle et qu'il fournit ou qu'il réalise lui-même.

Ne pas collecter au titre du présent Contrat une opération de paiement pour laquelle il n'a pas lui-même reçu le consentement du titulaire de Carte.

4.6 Dans le cas d'une opération de paiement effectuée avec une Carte co-badgée, c'est-à-dire portant le logo de deux ou plusieurs Marques, permettre au titulaire de la Carte de choisir la Marque. Il est rappelé à l'Accepteur qu'il peut sélectionner prioritairement la Marque indiquée à l'article 1 des Conditions Particulières, sous réserve de laisser la possibilité au titulaire de la Carte de passer outre, et de sélectionner une autre Marque.

4.7 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.

Respecter les montants maximum indiqués par l'Acquéreur pour l'acceptation d'une opération de paiement par carte, et précisés dans les Conditions Particulières.

4.8 S'identifier clairement dans la transmission de ses enregistrements à l'Acquéreur par le numéro d'immatriculation (pour la France le SIRET et le code activité NAF/APE) que l'INSEE lui a attribués ou comme Entité dûment habilitée à recevoir des

dons ou percevoir des cotisations. Si l'Accepteur n'est pas immatriculable, il doit utiliser un numéro d'identification spécifique, fourni par l'Acquéreur.

4.9 Afin que le titulaire de la Carte n'ait pas de difficulté à vérifier et identifier les opérations de paiement qu'il a effectuées, vérifier avec l'Acquéreur la conformité des informations transmises pour identifier son point d'acceptation. Ces informations doivent indiquer une dénomination commerciale ou sociale (pour les dons et cotisations) connue des titulaires de Carte et permettre d'identifier le point d'acceptation concerné et de dissocier ce type de paiement des autres types de paiement (ex : automate et règlement en présence physique du titulaire de la Carte).

4.10 Transmettre les enregistrements des opérations de paiement à l'Acquéreur, dans le délai maximum précisé à l'article 7 « Mesures de sécurité», sauf dispositions contraires précisées dans les Conditions Spécifiques relatives à chaque Schéma.

Le délai de remise de la « transaction crédit » ne peut excéder trente (30) jours calendaires à compter de la date de l'opération de paiement initiale, sauf dispositions contraires précisées dans les Conditions Spécifiques relatives à chaque Schéma.

Au-delà d'un délai maximum indiqué dans les Conditions Spécifiques à chaque Schéma, après la date de l'opération, l'encaissement des opérations de paiement n'est plus réalisable.

4.11 Régler, selon les Conditions Particulières convenues avec l'Acquéreur et selon les Conditions Générales, les commissions, frais, pénalités éventuelles et, d'une manière générale, toute somme due au titre de l'acceptation des Cartes et du fonctionnement du Schéma concerné.

4.12 Utiliser obligatoirement un Système d'Acceptation conforme aux spécifications du Schéma concerné par l'opération de paiement et les procédures de sécurisation des ordres de paiement, donnés à distance par les titulaires de Cartes, proposées par l'Acquéreur.

A cet effet, l'Accepteur organise la traçabilité adéquate des informations liées au paiement à distance.

4.13 Respecter le Référentiel Sécuritaire Accepteur figurant en annexe des Conditions Particulières et le Référentiel Sécuritaire PCI DSS consultable sur le site pcisecuritystandards.org, dont une présentation générale figure également en annexe des Conditions Particulières.

Prévoir, dans ses relations contractuelles avec les tiers, tels que les prestataires de services techniques ou sous-traitants intervenant dans le traitement et le stockage des données liées à l'utilisation des Cartes, que ces derniers s'engagent à respecter les mêmes exigences et règles sécuritaires et acceptent que les audits visés à l'article 4.14 soient réalisés dans leurs locaux et que les rapports puissent être communiqués comme précisé dans cet article.

Déclarer annuellement et en cas de changement, à l'Acquéreur, lesdits prestataires techniques ou sous-traitants. A défaut, l'Accepteur s'expose à des pénalités telles qu'indiquées aux Conditions Particulières.

4.14 Permettre à l'Acquéreur et/ou au(x) Schéma(s) concerné(s) de faire procéder aux frais de l'Accepteur dans ses locaux ou ceux de ses prestataires, à la vérification et/ou au contrôle périodique par un tiers indépendant du respect tant des clauses du présent Contrat et ses annexes, que des exigences et règles sécuritaires visées à l'article 4.13. Cette vérification, appelée "procédure d'audit", peut intervenir à tout moment dès la conclusion du présent Contrat et/ou pendant sa durée et s'inscrit dans le respect des procédures de contrôle et d'audit définies par le Schéma concerné.

L'Accepteur autorise la communication du rapport en résultant à l'Acquéreur et au(x) Schéma(s) concerné(s).

Au cas où le rapport d'audit révélerait un ou plusieurs manquements aux Contrat ou exigences et règles sécuritaires, le Schéma peut demander à l'Acquéreur de procéder à une résiliation du contrat d'acceptation.

4.15 En cas de compromission et si la non-conformité aux exigences et règles sécuritaires est confirmée par le Schéma ou un tiers indépendant, des frais forfaitaires à l'ouverture du dossier de compromission ainsi qu'un montant par Carte compromise seront applicables à l'Accepteur. Ces frais et montants sont indiqués dans les Conditions Particulières.

4.16 Mettre en œuvre dans le délai imparti par l'Acquéreur les mesures destinées à résorber un taux d'impayés anormalement élevé ou une utilisation anormale de Cartes perdues, volées ou contrefaites ou pour remédier à tout autre manquement au regard du présent Contrat.

A défaut, l'Acquéreur peut procéder, pour des raisons de sécurité, sans préavis et dans les conditions prévues à l'article 8.2 des Conditions Générales, à une suspension de l'acceptation des Cartes portant certaines Marques par l'Accepteur.

En cas de taux de fraude anormalement élevé, notamment au regard du volume d'affaires réalisé par l'Accepteur, de l'augmentation des opérations mises en impayés suite à réclamation du Titulaire de la Carte, d'utilisation anormalement élevée de Cartes perdues, volées ou contrefaites ou dont les données ont été usurpées, l'Acquéreur est fondé à ne créditer le compte de l'Accepteur qu'après l'encaissement définitif des opérations de paiement.

L'Acquéreur est également autorisé à ne créditer le compte de l'Accepteur qu'après encaissement définitif en cas d'opérations présentant un caractère inhabituel ou exceptionnel.
L'Acquéreur en informe l'Accepteur par tout moyen à sa convenance, ladite mesure prenant effet immédiatement. Les opérations de paiement seront alors portées sur un compte d'attente spécialement ouvert à cet effet, distinct et autonome du compte de l'Accepteur, pour n'être portées au crédit de ce dernier qu'après encaissement définitif par l'Acquéreur. Les fonds portés au crédit du compte d'attente demeurent indisponibles.

Dans les mêmes hypothèses, l'Acquéreur peut après avoir dans un premier temps inscrit une ou plusieurs opérations au compte de l'Accepteur, dès lors que le paiement n'est pas encore définitif et selon les mêmes modalités que celles définies aux alinéas précédents, procéder à la contrepassation desdites opérations afin de les inscrire sur le compte d'attente.

4.17 Les Schémas peuvent appliquer des pénalités aux Acquéreurs, calculées sur des bases identiques quel que soit l'Acquéreur, notamment :

- en cas de dépassement d'un certain nombre et/ou taux d'impayés généré(s) chez l'Accepteur, des pénalités mensuelles peuvent être appliquées après mise en demeure restée infructueuse.

- en cas de dépassement d'un certain nombre et/ou taux de fraude généré(s) chez l'Accepteur. A titre d'exemple, des pénalités allant jusqu'à 50% du montant de la fraude cumulée des 6 derniers mois peuvent être appliquées.
- lorsque l'Accepteur dépasse un certain nombre de factures crédits,
- en cas de non-respect des obligations d'information de l'Acquéreur relatives à l'activité de l'Accepteur (ajout, modification, arrêt),
- en cas d'exercice par l'Accepteur d'une activité illicite comme précisé à l'article 4.2 des présentes Conditions Générales ou non-conforme avec les règles édictées par les Schémas.

L'Accepteur accepte expressément de prendre en charge ces pénalités et autorise l'Acquéreur à les prélever sur le compte désigné aux Conditions Particulières.

L'Accepteur reconnait avoir été informé que l'exercice de certaines activités peut être interdit, ou soumis à restrictions ou autorisations par les Schémas.

4.18 Dans le cas où il propose des paiements récurrents, à savoir des 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, l'Accepteur s'engage à :

- respecter les règles relatives au stockage des données à caractère personnel ou liées à l'utilisation de la Carte définies par la délibération de la CNIL n°2013-358 du 14 novembre 2013,
- s'assurer que le titulaire de la Carte a consenti à ce que les données liées à sa Carte soient utilisées pour effectuer des paiements récurrents et, à ce titre, recueillir du titulaire de la Carte les autorisations et/ou mandats nécessaires à l'exécution des paiements 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.

4.19 Informer dans les meilleurs délais l'Acquéreur en cas de fonctionnement anormal du Système d'Acceptation et de toutes autres anomalies.

4.20 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 10 des Conditions Générales.

4.21 Garantir l'Acquéreur, et, le cas échéant, les Schémas, contre toute conséquence dommageable pouvant résulter pour eux du manquement aux obligations visées au présent article.

Article 5 - Obligations de l'Acquéreur

L'Acquéreur s'engage à :

5.1 Fournir à l'Accepteur, selon les choix qu'il exprime, les informations le concernant directement sur le fonctionnement du(des) Schéma(s) sélectionné(s) dans les Conditions Particulières et son (leur) évolution, les Catégories de Cartes et les Marques acceptées par lui, les frais applicables à chacune des Catégories de cartes et Marques acceptées par lui, y compris les commissions d'interchange et les frais versés au(x) Schéma(s).

5.2 Mettre à la disposition de l'Accepteur les informations relatives aux procédures de sécurisation des opérations de paiement.

Dans le cas où l'Accepteur a souscrit à l'offre de plateforme technique e-commerce Cyberplus Paiement commercialisée par l'Acquéreur, fournir à l'Accepteur les informations sur les procédures applicables à l'acceptation des paiements à distance sécurisés référencées par les Schémas, que l'Accepteur doit utiliser obligatoirement, ainsi que leurs évolutions éventuelles. Ces informations figurent dans le contrat de service relatif à cette offre.

5.3 Respecter le choix de la Marque et de la Catégorie de Carte utilisés pour le paiement au point d'acceptation conformément au choix de l'Accepteur, sauf avis contraire du titulaire de la Carte.

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

5.5 Indiquer et facturer à l'Accepteur les commissions à acquitter, séparément pour chaque Catégorie de Carte et chaque Marque selon les différents niveaux d'interchange.

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

5.6 Créditer le compte de l'Accepteur des sommes qui lui sont dues, selon les conditions du présent Contrat.

5.7 Ne pas débiter, au-delà du délai maximum de vingt-quatre (24) mois à partir de la date du crédit initial porté au compte de l'Accepteur, les opérations non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.

5.8 Selon les modalités convenues avec l'Accepteur, communiquer au moins une fois par mois, les informations suivantes pour la période écoulée :

- 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 le montant de la commission d'interchange.

L'Accepteur peut demander que ces informations relatives aux opérations exécutées soient regroupées par Marque, application de paiement, Catégorie de Carte et par taux de commission d'interchange applicable à l'opération de paiement.

5.9 Communiquer chaque début d'année un relevé dit Relevé Annuel des Frais d'Encaissement par Carte (RAFEC), qui récapitule pour l'année écoulée les frais du (des) Schéma(s), les commissions de service payées par l'Accepteur et les commissions d'interchange par Marque et Catégorie de Carte.

Article 6 : Garantie de paiement

6.1 Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité, visées dans les Conditions Particulières et leurs annexes, aux articles 4 et 7 des présentes Conditions Générales ainsi qu'aux Conditions Spécifiques à chaque Schéma.

6.2 Toutes les mesures de sécurité sont indépendantes les unes des autres. Ainsi, l'autorisation donnée par le système Acquéreur d'autorisation ne vaut garantie que sous réserve du respect des autres mesures de sécurité.

6.3 En cas de non-respect d'une seule de ces mesures, les opérations de paiement ne sont réglées que sous réserve de bonne fin d'encaissement et ce, en l'absence de contestation.

6.4 L'Accepteur autorise expressément l'Acquéreur à débiter d'office son compte du montant de toute opération de paiement non garantie.

Article 7 : Mesures de sécurité

7.1 La procédure de sécurisation de paiement à distance consiste en l'authentification 3D Secure du titulaire de la Carte conformément aux spécifications établies par les Schémas (« Protocole 3D Secure »).

L'Accepteur qui ne souhaite pas souscrire à l'offre de plateforme techniques e-commerce Cyberplus Paiement commercialisée par l'Acquéreur, doit s'assurer auprès du prestataire technique tiers qu'il choisit pour sa solution de paiement à distance que son offre de plateforme de services techniques e-commerce inclut l'authentification 3D Secure du titulaire de la Carte, et que ce prestataire est en mesure de communiquer à l'Acquéreur et de recevoir de celui-ci toutes les informations nécessaires à la sécurisation des paiements à distance selon le Protocole 3D Secure. Si ledit prestataire ne communique pas les informations précitées à l'Acquéreur et/ou ne traite pas les informations renvoyées par l'Acquéreur, la procédure de sécurisation des paiements ne pourra pas être assurée et l'Accepteur en assumera la responsabilité.

7.2 L'Accepteur doit informer immédiatement 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, dysfonctionnements du Système d'Acceptation...) ;

7.3 Lors du paiement, l'Accepteur s'engage à :

7.3.1 Appliquer la procédure de sécurisation des ordres de paiement à distance évoquée en avertissement ainsi qu'à l'article 7.1 des présentes Conditions Générales.

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

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

- le cas échéant, la période de validité (fin et éventuellement début),
- la Marque du Schéma qui doit être l'une de celles choisies dans les Conditions Particulières.

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

7.3.5 Obtenir une autorisation d'un montant identique à l'opération. Une opération pour laquelle l'autorisation a été refusée par le système Acquéreur d'autorisation n'est jamais garantie.

7.4 Après le paiement, l'Accepteur s'engage à :

7.4.1 Transmettre les enregistrements des opérations de paiement à l'Acquéreur dans le délai maximum de trois (3) jours calendaires à compter de la date de l'opération de paiement. Au-delà de ce délai, les opérations de paiement ne seront réglées que sous réserve de bonne fin d'encaissement.

S'assurer que les opérations de paiement ont bien été imputées au compte dans les délais et selon les modalités prévus dans les Conditions Particulières.

L'Accepteur ne doit transmettre que les enregistrements électroniques des opérations pour lesquelles un ordre de paiement a été donné à son profit.

Toute opération ayant fait l'objet d'une autorisation transmise par l'Acquéreur signataire du présent Contrat doit être obligatoirement remise à ce dernier.

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

7.4.3 Communiquer, à la demande de l'Acquéreur, tout justificatif des opérations de paiement dans les huit (8) jours calendaires à compter de la date de la demande présentée par l'Acquéreur. Si l'Accepteur ne communique pas le justificatif, ou le communique au-delà du délai ci-dessus, il s'expose à un impayé.

7.4.4 Ne pas stocker sous quelque forme que ce soit le cryptogramme visuel des Cartes.

7.4.5 Prendre toutes les précautions utiles 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 de paiement par Carte ainsi que le contrôle de l'accès à celles-ci et ce, conformément aux prescriptions de la loi "Informatique et Libertés" du 6 janvier 1978 et notamment de son article 34.

7.4.6 Les mesures de sécurité et de prévention des risques énumérées au présent article pourront être modifiées et complétées pendant toute la durée du présent Contrat, selon la procédure prévue à l'article 9.

Article 8 - Mesures de prévention et de sanction prises par l'Acquéreur

8.1 Avertissement

8.1.1 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 un avertissement valant mise en demeure précisant les mesures à prendre pour remédier au manquement constaté ou résorber le taux d'impayés anormalement élevé.

8.1.2 Si l'Accepteur n'a pas remédié au manquement ayant justifié l'avertissement ou n'a pas mis en œuvre les mesures destinées à résorber le taux d'impayés constaté, l'Acquéreur peut soit procéder à une suspension de l'acceptation des Cartes, soit résilier de plein droit avec effet immédiat le présent Contrat dans les conditions précisées aux articles 8.2 et 10 des présentes

Conditions Générales.

8.2 Suspension de l'acceptation

8.2.1 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. Elle est notifiée par tout moyen et doit être motivée. Son effet est immédiat.

Elle peut s'accompagner d'un avertissement, voire d'une réduction du seuil de demande d'autorisation de l'Accepteur.

La suspension ne porte pas préjudice à la faculté des Parties de résilier le Contrat conformément à la procédure visée à l'article 10 des présentes Conditions Générales. Notamment, l'Accepteur pourra, en cas de suspension, résilier le Contrat avec effet immédiat.

8.2.2 La suspension peut être décidée en raison notamment :

- d'un ou plusieurs manquement(s) aux clauses du Contrat et notamment aux exigences sécuritaires, qui serait(ent) révélé(s) au terme de la procédure d'audit visée à l'article 4 des présentes Conditions Générales ;
- 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,
- d'une participation à des activités frauduleuses, notamment d'une utilisation anormale de Cartes perdues, volées ou contrefaites,
- d'un refus d'acceptation répété et non motivé de la (des) Marque(s) et/ou Catégorie(s) de Carte qu'il a choisie(s) d'accepter ou qu'il doit accepter,
- de plaintes répétées d'autres membres ou partenaires d'un Schéma et qui n'ont pu être résolues dans un délai raisonnable,
- de retard volontaire ou non motivé de transmission des justificatifs,
- d'un risque aggravé en raison des activités de l'Accepteur.

8.2.3 L'Accepteur s'engage alors à restituer à l'Acquéreur, le cas échéant, 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 concernées.

8.2.4 La période de suspension peut s'étendre sur une période de six (6) mois, 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 en paiement de proximité par Cartes avec un autre acquéreur de son choix.

8.2.5 A tout moment, l'Accepteur peut présenter ses observations sur la suspension.

Article 9 : Modifications du Contrat

9.1 L'Acquéreur peut modifier à tout moment les dispositions du Contrat, après en avoir informé l'Accepteur avant la date d'entrée en vigueur des nouvelles dispositions.

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, si celui-ci est mis à disposition par l'Acquéreur, suite à un dysfonctionnement.
- des modifications sécuritaires telles que :
  - la suppression de l'acceptabilité de certaines Cartes,
  - la suspension de l'acceptabilité de Cartes portant certaines Marques.

9.2 Les nouvelles conditions entrent en principe 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 tout autre support durable.

9.3 Ce délai peut exceptionnellement être réduit en cas de modification(s) motivée par des raisons sécuritaires, notamment lorsque l'Acquéreur constate dans le Point d'acceptation une utilisation anormale de Cartes perdues, volées ou contrefaites.

9.4 Dans les délais visés au présent article, l'Accepteur peut résilier le présent Contrat s'il refuse les modifications opérées, dans les conditions prévues à l'article 10 des présentes Conditions Générales. A défaut de résiliation dans ces délais, les modifications lui seront opposables.

9.5 Le non-respect des nouvelles conditions techniques ou sécuritaires, dans les délais impartis, peut entraîner la suspension de l'acceptation des Cartes du Schéma concerné voire la résiliation du présent Contrat par l'Acquéreur, selon les dispositions prévues à cet effet aux articles 8.2 et 10 des présentes Conditions Générales, et aux Conditions Spécifiques du Schéma concerné.

Article 10 : Durée et résiliation du Contrat

10.1 Le présent Contrat est conclu pour une durée indéterminée, sauf accord contraire des Parties.

10.2 L'Accepteur ou l'Acquéreur peuvent chacun, et à tout moment, sans justificatif, 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 à l'autre Partie d'une lettre recommandée avec demande d'avis de réception.

Lorsque cette résiliation fait suite à un désaccord sur les modifications prévues à l'article 9 des présentes Conditions Générales, elle prendra effet à l'issue du délai visé à cet article pour l'entrée en vigueur des modifications.

Lorsque cette résiliation fait suite à une cessation d'activité de l'Accepteur, cession ou mutation du fonds de commerce, elle prend effet immédiatement.

Lorsque la résiliation intervient à la demande d'un Schéma ou de l'Acquéreur lui-même, pour des raisons de sécurité ou de fraude, notamment pour l'une des raisons visées aux articles 4 et 7 des présentes Conditions Générales, elle pourra prendre effet immédiatement. Selon la gravité des faits concernés, cette résiliation immédiate peut intervenir à la suite d'un avertissement et d'une mesure de suspension de l'acceptation prévus à l'article 8 des présentes Conditions Générales.

10.3 En cas de résiliation, l'Accepteur garde la faculté d'accepter les Cartes de tout Schéma avec tout autre Acquéreur de son choix.

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

10.4 L'Accepteur sera tenu de restituer à l'Acquéreur les dispositifs techniques et sécuritaires, le Système d'Acceptation et les documents en sa possession dont l'Acquéreur est propriétaire.

Sauf dans le cas où il a conclu un ou plusieurs autres contrats d'acceptation, l'Accepteur s'engage à retirer immédiatement de son Point d'acceptation et de ses supports de communication tout signe d'acceptation des Cartes, ou Marques des Schémas concernés.

Article 11 - Modalités annexes de fonctionnement

11.1 Réclamation
Toute réclamation de l'Accepteur doit être justifiée et 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.

Toutefois, ce délai est réduit à quinze (15) jours calendaires à compter de la date de débit en compte, en cas d'opération non garantie, notamment en cas d'impayé.

11.2 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 produits par l'Acquéreur ou le Schéma prévaudront sur ceux produits 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 dont les Cartes sont concernées.

11.3 Remboursement ou Transaction crédit
Le remboursement partiel ou total d'un achat d'un bien ou d'un service réglé par Carte doit, avec l'accord de son titulaire, être effectué avec les données de la Carte utilisée pour l'opération initiale. L'Accepteur doit alors utiliser la procédure dite de "Transaction crédit" en effectuant, dans le délai prévu par l'article 4 des présentes Conditions Générales, la remise de la "Transaction crédit" 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.

Article 12 : Secret bancaire et protection des données à caractère personnel

12.1 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.

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

En application des articles 32, 38, 39 et 40 de la loi du 6 janvier 1978 relative à la loi "Informatique et Libertés" modifiée par la loi du 6 août 2004, il est précisé que :

- Les informations relatives à l'Accepteur, collectées par l'Acquéreur nécessaires pour l'exécution des ordres de paiement transmis et leur sécurisation, ne seront utilisées et ne feront l'objet de diffusion auprès d'entités tierces que pour les seules finalités de traitement des Opérations de paiement par Carte, données en exécution du présent Contrat, ou pour répondre aux obligations légales et réglementaires, l'Acquéreur étant à cet effet, de convention expresse, délié du secret bancaire.

L'Accepteur, personne physique, ou la personne physique le représentant ou sur laquelle portent les données à caractère personnel ci-dessus recueillies, a le droit d'en obtenir communication, et le cas échéant, d'en exiger la rectification et de s'opposer, pour des motifs légitimes, à ce qu'elles fassent l'objet d'un traitement ou à leur utilisation à d'autres fins que celles citées ci-dessus, auprès de l'Acquéreur.

A l'occasion de l'exécution des ordres de paiement donnés par Carte, l'Accepteur peut avoir accès à différentes données à caractère personnel concernant notamment les Titulaires de la Carte, à savoir le numéro de la Carte, sa date de fin de validité, sans que cette liste soit exhaustive, dont il doit garantir la sécurité et la confidentialité conformément aux dispositions du présent Contrat. .

L'Accepteur ne peut utiliser ces données à caractère personnel que pour l'exécution des ordres de paiement par Carte.
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. Il s'assure également de l'existence et de la mise en œuvre de dispositifs de protection et de contrôle des accès physiques et logiques à ces données.

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

12.3 Les dispositions de la loi pour la confiance dans l'économie numérique du 21 juin 2004 obligent l'Accepteur à recueillir le consentement exprès et préalable du titulaire de Carte lors de toute utilisation de son adresse mail et de son numéro de mobile à des fins de prospection commerciale.

L'Accepteur s'engage à chaque envoi d'une nouvelle proposition commerciale à informer le Titulaire de la Carte de sa possibilité de se désabonner et des modalités y afférentes. L'Accepteur s'engage enfin à respecter ces dispositions et à supprimer de ses propres bases de données, les données personnelles du Titulaire de la Carte si ce dernier en fait la demande auprès de l'Accepteur, l'Acquéreur étant déchargé de toute responsabilité en cas de non-respect de ces obligations légales et réglementaires par l'Accepteur.

Article 13 : 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 14 : 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.

Article 15 : Langue du Contrat

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

Article 16 : Confidentialité

Chacune des deux Parties ne communiquera aucune information et ne publiera aucun communiqué en relation avec l'existence des Conditions Générales, Particulières et Spécifiques, et de leurs annexes ou leur contenu sans l'accord préalable de l'autre Partie, sauf si la communication de l'information ou la publication du communiqué est rendue obligatoire par une disposition légale ou règlementaire s'imposant à la partie concernée, ou pour répondre à une demande d'une autorité judiciaire ou administrative (gouvernementale, bancaire, fiscale ou autre autorité réglementaire similaire).

PARTIE II
CONDITIONS SPECIFIQUES D'ACCEPTATION EN PAIEMENT A DISTANCE SECURISE PROPRES A CHAQUE SCHEMA

PARTIE II. 1
CONDITIONS SPECIFIQUES POUR LES OPERATIONS REALISEES SELON LE SCHEMA« CB »

Article préliminaire

Les règles ci-après s'appliquent lorsque le titulaire de la Carte et l'Accepteur sont d'accord pour réaliser l'opération de paiement par carte selon les règles du Schéma « CB ».

Article 1 : Conditions liées à la garantie de paiement des opérations de paiement « CB »

La garantie de paiement est conditionnée par le respect des conditions prévues au Présent Contrat.

Article 2 : Délai maximum de transmission des opérations de paiement « CB » à l'Acquéreur

L'Accepteur s'engage à transmettre à l'Acquéreur les opérations de paiement réalisées selon les règles du Schéma CB dans un délai maximum de 6 mois.

Ce délai de 6 mois est un délai distinct du délai conditionnant la Garantie de paiement prévu aux articles 6 et 7 des Conditions Générales.

Article 3 : Litiges commerciaux

L'Accepteur s'engage à faire son affaire personnelle de tous litiges de nature commerciale ou autre, ou/et de leurs conséquences financières, pouvant survenir avec des clients, adhérents ou donateurs, concernant des biens et services, cotisations ou dons ayant été réglés par Carte au titre du présent Contrat.

Article 4 : Suspension et clôture du contrat pour le Schéma « CB »

4.1 Le Schéma « CB » 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 du Schéma « CB ». Elle est précédée, le cas échéant, d'un avertissement à l'Accepteur, voire d'une réduction de son seuil de demande d'autorisation. Cette suspension est notifiée par l'envoi d'une lettre recommandée et motivée, avec demande d'avis de réception. Son effet est immédiat. Elle peut être décidée en raison notamment :

- d'une utilisation anormale de Cartes perdues, volées ou contrefaites,
- d'une utilisation d'un Système d'acceptation non agréé,
- d'un risque de dysfonctionnement important du Schéma « CB »,
- en cas de comportement frauduleux de la part de l'Accepteur responsable du Point d'acceptation.

4.2 L'Accepteur s'engage alors à restituer, le cas échéant, à l'Acquéreur le Système d'acceptation, les dispositifs techniques et sécuritaires du Schéma « CB » et les documents en sa possession dont l'Acquéreur est propriétaire, et à retirer immédiatement de son Point d'acceptation tout signe d'acceptation des Cartes « CB » ou de la Marque « CB ».

4.3 La période de suspension est au minimum de 6 mois, éventuellement renouvelable.

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

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

Article 5 : Communication des Commissions Interbancaires de Paiement (interchange) de « CB »

Les taux de commissions interbancaires pratiqués par le Schéma« CB » sont publics et consultables sur son site internet du Schéma« CB », http://www.cartes-bancaires.com/.

PARTIE II.2
CONDITIONS SPECIFIQUES D'ACCEPTATION EN PAIEMENT A DISTANCE SECURISE POUR LES OPERATIONS REALISEES SELON LES SCHEMAS« VISA », « VISA ELECTRON » OU « VPAY »

Article préliminaire

Les règles ci-après s'appliquent lorsque le titulaire de la Carte et l'Accepteur sont d'accord pour réaliser l'opération de paiement par carte selon les règles des Schémas « VISA », « Visa Electron » ou « VPAY ».

Article 1 : Conditions liées à la garantie de paiement des opérations de paiement « Visa », « Visa Electron et « VPAY »

La garantie de paiement est conditionnée par le respect des conditions du Présent Contrat.

Seuil d'autorisation : Quel que soit le montant de l'opération de paiement, une demande d'autorisation doit systématiquement être faite pour une opération de paiement réalisée selon les Schémas « Visa », « Visa Electron » ou « VPAY », que ce soit une carte étrangère ou française, qu'elle soit co-badgée avec un autre Schéma ou non.

Article 2 : Suspension ou clôture du contrat à la demande des Schémas« Visa », « Visa Electron » ou « VPAY »

Les Schémas Visa, « Visa Electron » ou « VPAY » peuvent dans certains cas (cf. article 4 des Conditions Générales) se retourner vers l'Acquéreur pour que celui-ci exige de son Accepteur qu'il respecte les règles des Schémas « Visa », « Visa Electron » ou « VPAY », faute de quoi l'Acquéreur sera dans l'obligation de résilier le présent Contrat.

Article 3 : Acceptation des Cartes Visa, « Visa Electron » ou « VPAY » émises hors UE

Les Cartes des Schémas « Visa », « Visa Electron » ou « VPAY » émises par un émetteur situé hors de l'EEE sont systématiquement acceptées par l'Accepteur si celui-ci accepte au moins un type de Carte des Schémas Visa, «Visa Electron » ou « VPAY ».

Article 4 : Communication des Commissions Interbancaires de Paiement (interchange) de « Visa », « Visa Electron » ou « VPAY »

Les taux de commissions d'interchange pratiqués par les Schémas « Visa », « Visa Electron » ou « VPAY »sont publics et consultables sur le site internet : www.visa-europe.fr.

PARTIE II.3
Conditions spécifiques d'acceptation en paiement à distance sécurisé pour les opérations réalisées selon les Schémas « Mastercard » et « Maestro »

Article préliminaire

Les règles ci-après s'appliquent lorsque le titulaire de la Carte et l'Accepteur sont d'accord pour réaliser l'opération de paiement par Carte selon les règles des Schémas « Mastercard » et « Maestro ».

Article 1 : Conditions liées à la garantie de paiement des opérations de paiement « Mastercard » ou « Maestro »

La garantie de paiement est conditionnée par le respect des conditions prévues au Présent Contrat.

Seuil d'autorisation : Quel que soit le montant de l'opération de paiement, une demande d'autorisation doit systématiquement être faite pour une opération de paiement réalisée selon les Schémas Mastercard ou Maestro.

Article 2 : Suspension ou clôture du contrat à la demande des Schémas « Mastercard » ou « Maestro »

Les Schémas Mastercard ou Maestro peuvent dans certains cas (cf. article 4 des Conditions Générales) se retourner vers l'Acquéreur pour que celui-ci exige de son Accepteur qu'il respecte les règles des Schémas Mastercard ou Maestro, faute de quoi l'Acquéreur sera dans l'obligation de résilier le présent Contrat.

Article 3 : Acceptation des Cartes « Mastercard » ou « Maestro » émises hors Union Européenne

Les Cartes des Schémas Mastercard ou Maestro émises par un émetteur situé hors de l'EEE sont systématiquement acceptées par l'Accepteur si celui-ci accepte au moins un type de Carte des Schémas Mastercard ou Maestro émise dans l'Union Européenne.

Article 4 : Communication des Commissions Interbancaires de Paiement (interchange) de « Mastercard » ou « Maestro »

Les taux de commissions d'interchange pratiqués par les Schémas Mastercard ou Maestro sont publics et consultables sur le site internet : www.mastercard.com

PARTIE II.4
CONDITIONS SPECIFIQUES D'ACCEPTATION EN PAIEMENT A DISTANCE SECURISE POUR LES OPERATIONS REALISEES SELON LES SCHEMAS « DINER'S CLUB INTERNATIONAL » OU « DISCOVER »

Article préliminaire

Les règles ci-après s'appliquent lorsque le titulaire de la Carte et l'Accepteur sont d'accord pour réaliser l'opération de paiement par Carte selon les règles des Schémas « Diner's Club International » ou « Discover ».
Les règles du Schéma « DISCOVER » s'appliquent aux opérations réalisées avec des Cartes agréées DISCOVER telles que BC Global Card, RUPAY, ELO.

Article 1 : Conditions liées à la garantie de paiement des opérations de paiement « Diner's Club International » ou « Discover »

La garantie de paiement est conditionnée par le respect des conditions prévues au Présent Contrat.

Seuil d'autorisation : Quel que soit le montant de l'opération de paiement, une demande d'autorisation doit systématiquement être faite pour une opération de paiement réalisée selon les Schémas « Diner's Club International » ou « Discover » ;

Article 2 : Suspension ou clôture du contrat à la demande des Schémas « Diner's Club International » ou « Discover »

Les Schémas « Diner's Club International » ou « Discover » peuvent dans certains cas (cf. article 4 des Conditions Générales) se retourner vers l'Acquéreur pour que celui-ci exige de son Accepteur qu'il respecte les règles des Schémas « Diner's Club International » ou « Discover », faute de quoi l'Acquéreur sera dans l'obligation de résilier le présent Contrat.

Article 3 : Acceptation des Cartes « Diner's Club International » ou « Discover » émises hors Union Européenne

Les Cartes des Schémas « Diner's Club International » ou « Discover »émises par un émetteur situé hors de l'EEE sont systématiquement acceptées par l'Accepteur si celui-ci accepte au moins un type de Carte des Schémas « Diner's Club International » ou « Discover » émise dans l'Union Européenne.

BANQUE POPULAIRE
BOURGOGNE
FRANCHE-COMTÉ
www.bpbfc.banquepopulaire.fr

CONDITIONS SPECIFIQUES AUX CONDITIONS GÉNÉRALES D'ADHÉSION AU SYSTÈME DE PAIEMENT À DISTANCE SÉCURISÉ PAR CARTE BANCAIRE

Préambule

L'Accepteur a signé avec l'Acquéreur une convention de service CyberPlus Paiement/Paiement Express (plateforme Systempay) ayant pour objet la sécurisation des paiements à distance via Internet par cartes bancaires selon une procédure conforme au protocole 3DSecure référencé par le GIE "CB".

Chaque accès à la plateforme Systempay fait l'objet d'une demande d'autorisation facturée selon le tarif détaillé dans les conditions particulières du présent contrat.
A ce titre, l'Accepteur utilise le moyen technique CyberPlus Paiement/Paiement express mis à sa disposition par l'Acquéreur pour recevoir des paiements à distance via Internet sécurisés par cartes bancaires.

L'Accepteur est donc en mesure de recevoir des paiements à distance sécurisés par cartes en contrepartie d'actes de vente ou de fournitures de services qu'il réalise lui-même.
A ce titre, dans le cadre de sa politique de gestion des risques, l'Accepteur peut juger nécessaire d'appliquer des mesures de restriction d'acceptation. Dans ce cas, l'Accepteur agit sous sa propre responsabilité en prenant l'initiative du paramétrage de cette fonction.

Article 1 : objet

Les présentes Conditions Particulières complètent les Conditions Générales d'adhésion au système de paiement à distance sécurisé ont pour objet de déterminer les conditions d'application de la garantie telles que définies à l'article 4 des Conditions Générales du présent contrat qu'elles complètent, ainsi que de définir les conditions tarifaires de l'adhésion au système de paiement à distance sécurisé.

Article 2 : Procédure de paiement sécurisé 3D Secure

2.1 Enregistrement de l'Accepteur

La mise en œuvre du paiement sécurisé nécessite un enregistrement préalable 3DSecure de l'Accepteur auprès des réseaux VISA et MASTERCARD.
L'acceptation des paiements sécurisés est conditionnée par la confirmation de l'enregistrement 3D Secure de L'Accepteur par l'Acquéreur. Cette confirmation se matérialise par l'envoi d'un courriel à l'adresse communiquée par l'Accepteur, ce dernier s'engageant à informer sans délai l'Acquéreur de toute modification de cette adresse, ainsi que de toute indisponibilité de cette dernière.

2.2 Moyen technique mis à disposition de L'Accepteur par l'Acquéreur

L'Accepteur doit utiliser le moyen technique CyberPlus Paiement/Paiement Express – 3DSecure – mis à sa disposition par l'Acquéreur pour recevoir des paiements à distance par Internet sécurisés 3DSecure par cartes bancaires.
L'utilisation de ce moyen technique transfère à la Banque Emettrice de la Carte le soin d'authentifier le Titulaire de la Carte.

2.3 Authentification du porteur par la Banque Émettrice de la Carte

Ce moyen technique repose sur un système d'authentification du Titulaire de la Carte par la Banque Emettrice de la Carte.
En cas d'échec ou d'absence d'authentification, la transaction sera abandonnée et ne donnera donc pas lieu à demande d'autorisation.

2.4 Demande d'autorisation

Une autorisation doit être demandée à chaque transaction de paiement sécurisé 3D Secure quels que soient le montant et le type de carte.
La demande d'autorisation doit comporter le cryptogramme visuel et les éléments relatifs à l'authentification du Titulaire de la Carte.
La présence du cryptogramme visuel dans la demande d'autorisation est obligatoire pour tout paiement par Internet sécurisé 3D Secure. Il doit donc être systématiquement transmis lors d'une demande d'autorisation à la Banque Emettrice de la Carte.

2.5 Délai de transmission des opérations de paiement

La réglementation interbancaire, dans le cadre des opérations couvertes par le présent contrat, fixe un délai maximum de 07 jours (délai à préciser par chaque Acquéreur) au-delà duquel L'Accepteur s'expose à recevoir un impayé pour remise tardive.

Article 3 - Garantie du paiement

3.1 Conditions

Le strict respect de l'ensemble des conditions définies à l'article 2 des présentes Conditions Particulières et de celles de l'article 4 des Conditions Générales du présent Contrat conditionne l'obtention de la garantie du paiement.

3.2 Information sur l'existence de la garantie

L'Acquéreur met à disposition de l'Accepteur un indicateur dans le Journal des opérations de paiement (journal de fonds) du moyen technique CyberPlus Paiement/Paiement Express – Version 7 et supérieures – qui lui permet de s'assurer que l'opération de paiement bénéficie de la garantie 3D Secure.
L'information communiquée à l'Accepteur se traduit par trois messages différents :
YES : l'opération de paiement est garantie dans le cadre des conditions définies à l'article 2 ci-dessus et de celles de l'article 5 des Conditions Générales du présent Contrat.
NO : l'opération de paiement n'est pas garantie,
UNKNOWN : les informations relatives à l'opération de paiement en retour de la Banque Émettrice de la Carte ne permettent pas de déterminer si la garantie s'applique. Le règlement de l'opération de paiement ne se fera que sous bonne fin d'encaissement et ce, en l'absence de contestations.

3.3 Litige commercial

Le litige commercial est indépendant de l'opération de paiement. Il doit être réglé directement entre L'Accepteur et le Titulaire de la Carte concernée.

Article 4 : Délai de communication des justificatifs

Si L'Acquéreur en fait la demande, l'Accepteur s'engage à lui fournir tout justificatif des opérations de paiement dans un délai de 7 jours calendaires à compter de la demande de l'Acquéreur.
Passé ce délai, le compte de L'Accepteur pourra être débité du montant de l'opération de paiement concernée en application de l'article 5.1 et 5.4.3 des Conditions Générales.

Article 5 : Conditions tarifaires

Les conditions tarifaires sont indiquées sur la grille détaillée en première page de ce contrat et s'applique à partir du 3ième mois après la date de signature du contrat.

Article 6 : Obligations de l'accepteur

L'Accepteur « CB » s'engage à :

6.1 Utiliser le présent contrat que pour le seul et unique SIREN précisé ci-dessus et le seul et unique site Internet précisé dans la grille figurant sur la première page de ce contrat.

6.2 Informer préalablement et formellement la banque du souhait de toute modification de son objet social ou de toute extension de la nature des produits ou services vendus à distance (signalés sur la ligne « Activités réelles détaillées » indiquée dans la grille figurant sur la première page de ce contrat.

6.3 Supprimer ou provisionner des paiements reçus sans livraison complète des produits ou services payés. Pour des raisons de sécurité ou de disponibilité des produits, le client peut être amené à NE PAS LIVRER la commande de l'acheteur. Dans ce cas le commerçant à l'obligation de supprimer le paiement CB AVANT qu'il ne passe en compensation. Il lui suffit de faire régler par son développeur le « capture date » à 3 jours AU MOINS afin de lui laisser le temps matériel de supprimer le paiement manuellement dans l'interface « Office » de Cyberplus Paiement/Paiement Express (voir le Manuel) ou automatiquement par l'option « validation ». A DEFAUT les sommes perçues indûment doivent être systématiquement et immédiatement provisionnées sur un compte BPBFC dédié.

6.4 Impayés et Fraude : La Banque se réserve la possibilité de provisionner, si nécessaire et sans préavis, le montant de impayés potentiels détectés, ou des commandes encaissées non livrées, notamment si l'article 2.3 n'a pas été respecté. L'accepteur s'engage à lutter contre la fraude dont son point d'acceptation pourrait être victime, notamment en mettant en œuvre sans délais les mesures préconisées par le GIE Carte Bancaire, Visa, Mastercard ou la Banque.

6.5 Le non-respect de l'une des dispositions de l'article 2 pourra entrainer la clôture immédiate et sans préavis du ou des contrat(s) CB du Client et pourra donner lieu à la facturation des éventuels frais engendrés par l'absence de respect des obligations de l'accepteur : notamment les pénalités du GIE., de Visa, de Mastercard et tous autres frais divers induits y compris les impayés et frais à venir sur les encaissements déjà réalisés « sauf bonne fin »

Article 7 : La non utilisation du contrat

La non utilisation de ce contrat sur une période de 12 mois glissants pourra entrainer sa clôture immédiate à l'initiative de la banque et sans préavis.

CYBERPLUS PAIEMENT – VADE-MECUM
(Version SystemPay du 01 12 2009)

Ce document est un complément d'information. Il ne remplace pas les conditions particulières et générales du contrat

Accès web «outil de gestion de caisse»

L'OUTIL DE GESTION DE CAISSE est l'interface web qui vous permet de piloter Cyberplus Paiement.
https://systempay.cyberpluspaiement.com/vads-merchant/

Vous avez reçu par mail, votre identifiant et votre mot de passe pour accéder à l'Outil Gestion de Caisse.
Grâce à cet accès, vous pouvez, selon les fonctions choisies dans le formulaire d'inscription commerçant, visualiser l'historique de vos transactions des 6 derniers mois mais aussi annuler partiellement ou totalement un paiement avant son envoi en banque, valider partiellement ou totalement un paiement pour l'envoyer en banque, rembourser partiellement ou totalement une transaction, la dupliquer ou la créer, gérer des abonnements ou vos paiements en «n» fois sans frais, paramétrer l'envoi ou le téléchargement des journaux de reporting des transactions, etc...
Cet outil de gestion vous permet également d'effectuer les paramétrages nécessaires au bon fonctionnement de votre boutique.
Vous disposez également dans la rubrique aide d'une documentation commerciale et technique téléchargeable.
Les fonctionnalités sont décrites par exemple dans le manuel utilisateur de l'outil de gestion de caisse.
Les journaux sont décrits dans « le descriptif des journaux de reporting » etc…
Astuce : Un client vous commande trois articles mais vous n'en avez que deux en stock ! Avec son accord et grâce à l'outil Gestion de Caisse, vous pouvez diminuer le paiement pour qu'il corresponde aux articles livrés. Lorsque vous aurez reçu votre réassort et expédierez le reste de la commande, vous pourrez alors dupliquer une transaction à partir de votre historique et donc réitérer le paiement en modifiant le montant correspondant au solde de la commande. Dans ce cas, une nouvelle demande d'autorisation bancaire aura lieu et le paiement ne sera pas 3 D Secure (voir paragraphe 3 D Secure).
Si votre mot de passe n'est plus valide, vous devez contacter directement les équipes Back-office Cyberplus Paiement en contactant le 01 58 32 23 57 ou envoyant un mail à l'adresse cyberplus.paiement@paiements.natixis.fr. Votre nouveau mot de passe vous sera envoyé sur l'adresse courriel de l'utilisateur concerné.

Paramètre : Capture Day

Le CAPTURE DAY est un champ informatique vital du paramétrage de Cyberplus Paiement. Il permet de ne pas envoyer directement la transaction CB de votre client au système bancaire. La transaction est mise en suspend pendant x jours. Elle est par la suite automatiquement ENVOYEE ou DETRUITE selon l'option choisie dans le paramétrage.
Exemple : Dans certains cas, vous avez l'obligation de supprimer le paiement avant qu'il ne passe dans le circuit bancaire :
- pour des raisons sécuritaires, lorsque par exemple vous subissez des commandes suspectes ou frauduleuses et que vous décidez de ne pas livrer la marchandise,
- ou pour des raisons de disponibilité, lorsque par exemple vous n'avez plus en stock les articles commandés par votre client internaute.

En réglant vous-même ou en faisant régler par votre Développeur/intégrateur, le Capture Day sur 3 jours au moins (1) **(Maximum 6 jours)**, votre transaction est « levée » et vous avez le temps matériel de valider/supprimer manuellement le paiement avant qu'il ne soit traité en banque, grâce à votre « accès web GESTION DE CAISSE » et donc de ne pas être crédité de sommes pour lesquelles vous n'avez pas expédié la marchandise. A défaut les sommes perçues indûment doivent être systématiquement, immédiatement et spontanément provisionnées sur un compte BPBFC dédié et isolé.
Astuce : Réglez le paramètre sur « 3 jours » si vous êtes certains d'être en mesure d'intervenir dans ces délais et visualisez L'historique des commandes.
Si vous avez choisi l'option **« VALIDATION »** vous devez valider tous les paiements. Les paiements non validés seront éliminés au bout de « X » jours selon la durée du « capture day » choisi.
Si vous avez choisi l'option **« ANNULATION »** vos commandes seront automatiquement envoyées en banque au terme du « capture day » choisi et c'est alors à vous d'annuler volontairement une commande pendant la durée du capture day.
(1) Obligation contractuelle du service Cyberplus Paiement

Les sites utilisant CyberPlus paiement

Vous ne devez utiliser votre Cyberplus Paiement que pour les seuls et uniques Siren et sites internet précisés sur votre contrat.
Toute modification ou rajout ainsi que tout changement d'activité devront être signalés et acceptés par la Banque (1)
(1) Obligation contractuelle du « contrat carte bancaire commerçant ».
Cyberplus Paiement – Le Vade-Mecum 2/4
Astuce : Envoyez une lettre recommandée avec AR lors de toute évolution de l'objet social et préalablement à tout souhait d'utiliser Cyberplus Paiement sur un autre site ou sur une autre version du site.

Assistance téléphonique

Votre interlocuteur principal reste votre conseiller(e) de clientèle habituel dans votre Agence.
L'assistance commerciale est joignable au 01 58 32 23 57 ou cyberplus.paiement@natixis.fr
L'assistance technique est joignable au 0820 125 972 (du lundi au vendredi de 9 h à 18h) ou supportvad@lyra-network.com

Acceptation du paiement

Cyberplus paiement vérifie au moment du paiement :
1. Que la transaction est bien autorisée par la banque de votre client internaute c'est à dire que sa carte bancaire existe et que l'opération est autorisée et solvable (*).
2. Que la transaction dispose bien de la garantie 3DS. Garantie en cas de contestation pour Fraude (colonnes
« Transaction Condition » et « 3D_LS » du journal de fonds) (*)
(*) Voir descriptif détaillé des journaux de reporting
NB : Une transaction peut très bien être « valide » et donc être autorisée par la Banque du porteur de la carte (Code Response : 00 (*) sans pour autant disposer de la garantie 3 DS.
Dans ce cas, c'est la législation de la vente à distance traditionnelle qui fait foi. En tant que commerçant, vous n'avez pas de garantie

du paiement en cas de contestation et de demande d'annulation par le porteur de carte.

3 D Secure

3D Secure est un programme de sécurisation des transactions de paiement en ligne conçu et mis en place par les réseaux internationaux Visa et MasterCard et également appliqué par le Groupement des Cartes Bancaires.

3D Secure pour les « porteur CB » :
Historiquement, lors d'un paiement sur un site marchand internet, l'internaute renseignait les informations qu'il trouvait sur sa Carte Bancaire (numéro de carte, date de validité et cryptogramme visuel).
Cette opération ne permettait pas de vous garantir qu'il s'agissait d'un paiement effectué par le vrai porteur de la carte ou par un fraudeur.
Depuis l'élargissement de 3 D Secure à la France au 01 octobre 2008, les banques françaises sont en train de mettre en place des systèmes d'authentification de leurs porteurs de carte.
Ces nouvelles procédures permettent de mieux sécuriser les paiements sur Internet en demandant aux titulaires des cartes de s'authentifier au moment d'un paiement sur un site marchand lui-même 3 D Secure et qui présente au moment du paiement les logos "**Verified by Visa**" et "**Mastercard Secure code**".
Les méthodes d'authentification sont laissées aux libres choix des banques des internautes. (Identifiant, mot de passe, date de naissance, code reçu par SMS, boitier générant un code d'accès ...)
Par exemple, le porteur de carte peut, après avoir saisi son numéro de carte sur votre Cyberplus Paiement, voir apparaitre une page web de sa propre banque pour valider son paiement. Sa banque lui demande alors de s'authentifier en tapant un mot de passe. Les transactions notées en code 75 dans votre journal de fonds ont été refusées parce que le nombre de tentatives de saisi du numéro de carte a été dépassé par votre client internaute ou parce qu'il n'a pas réussi à s'authentifier comme le demande justement sa banque.
Important : Analysez bien la situation lorsqu'un internaute vous indique qu'il n'a pas été informé par sa banque ou qu'il n'a pas réussi à s'authentifier au moment du paiement. Il s'agit peut-être d'un fraudeur qui n'ayant pas les informations pour s'authentifier, vous contacte directement pour vous demander de créer vous-même la transaction avec votre Back Office. Dans cette configuration de création de transaction, il n'y aura pas de demande d'authentification du porteur et donc pas de garantie de paiement. (Voir paragraphe 3 D Secure du côté des cybercommerçants).
Pour résumer, le principe de 3D-Secure porteur est de demander à l'internaute de s'authentifier au moment du paiement afin de limiter l'utilisation frauduleuse de son numéro de carte bancaire.
Les internautes qui n'arriveraient plus à effectuer un paiement avec leur carte doivent ainsi s'adresser à leur banque (émettrice de la carte) pour connaître la procédure d'authentification décidée par celle-ci.
Chaque Banque décide de la mise en place et du choix du protocole d'authentification de ses porteurs de cartes, de la date de mise en place et de la communication faite à ses clients titulaires de cartes bancaires.
Les internautes peuvent également trouver les explications sur le site internet de leur banque.
Cyberplus Paiement – Le Vade-Mecum 3/4
Exemple de communication si vos clients internautes vous interrogeaient :
« Les réseaux VISA et MASTERCARD ont mis au point la norme 3 D Secure pour vous protéger lors d'un achat sur internet contre les utilisations frauduleuses de votre carte bancaire.
*Ainsi, lorsque vous effectuez un paiement sur un site marchand faisant apparaître les logos "**Verified by Visa**" et "**MastercardSecure code**», vous saisissez comme habituellement les informations contenues sur votre carte bancaire.*
Ensuite, vous êtes redirigé vers le site de votre banque sur lequel il vous est demandé de vous authentifier afin de valider le règlement de l'achat. Votre banque vérifie ainsi que vous être le porteur légitime de la carte.
La méthode d'authentification est laissée au libre choix de votre banque. Cela peut être la demande de saisie de votre date de naissance, la saisie d'un mot de passe, celle d'un code reçu par SMS ou un autre système...
Si vous n'arrivez pas à vous identifier, vous devez vous adresser à votre banque ou consulter son site internet pour vérifier la procédure d'authentification qu'elle a décidé de mettre en place.
Ce service est généralement gratuit et vous protège contre l'utilisation de votre carte bancaire à votre insu ».

3D Secure du côté des Cybercommerçants :
De votre coté en tant que cybercommerçant, vous êtes informé de la garantie d'un paiement par la mention « YES » ou « OUI » dans la colonne « 3D_LS » de votre journal des transactions qui vous est envoyé par courriel suite au paramétrage effectué par vos soins ou disponible en téléchargement.
Cette information est également consultable sur votre accès Office Cyberplus Paiement.
Pour rappel, 3 D Secure vous protègent contre la réception d'impayés motifs "utilisation frauduleuse de la carte éligible à 3DS".
- 3 D Secure ne fonctionne pas pour certaines transactions faites avec des cartes étrangères de types professionnelles.
- 3 D Secure ne vous garantit pas contre tous les autres motifs de fraude non éligibles à 3 D Secure ou autres types d'impayés.
- 3 D Secure ne fonctionne pas lorsque le paiement a été créé par vous-même, lorsque vous utilisez les boutons « création d'une transaction » via votre accès OFFICE.
- 3 D Secure ne fonctionne pas pour les paiements dupliqués par vous-même ou effectués en plusieurs fois.
- La colonne "Transaction Condition" de votre Journal de fonds, vous indique si le porteur de carte a été authentifié 3 D Secure (3 D SUCCES) Dans ce cas précis, il ne pourra pas y avoir d'émission d'impayé pour motif fraude.
- L'activation du service et la garantie de paiement pour chaque transaction vous seront indiqués par la mention « YES » ou « oui » dans la colonne « 3D_LS » de votre journal des transactions qui vous est envoyé par courriel.
- Un " NO" ou « non » ou "aucune indication" dans la colonne " 3D LS" ou « garantie 3 D SECURE » vous indiquent que la garantie ne vous est pas acquise. C'est alors la règlementation de la VAD par carte bancaire qui s'applique.
(Voir toutes les modalités dans votre contrat Cyberplus Paiement et dans votre contrat de vente à distance internet avec Cyberplus Paiement)
- 3 D Secure ne fonctionne pas avec Cyberplus Paiement BASIC.
- Pour les contrats Cyberplus Paiement PREMIUM, il y a nécessité d'effectuer des développements techniques complémentaires à la charge du client pour bénéficier du programme 3 D Secure. Les modalités de mise en pratique et le dispositif d'accompagnement sont indiqués dans le contrat accepteur CB VAD internet avec Cyberplus Paiement.
Cyberplus Paiement PREMIUM non disponible en SYSTEMPAY au 01/12/2009)
- Même si Cyberplus Paiement vous propose une « garantie 3 D Secure », nous vous rappelons que vous devez toujours

analyser vos commandes et annuler le paiement avant son envoi en banque et ne pas expédier la marchandise en cas de suspicion de fraude. Dans la négative et notamment si votre taux de fraude dépassait des standards définis par VISA et MASTERCARD, ces organismes pourraient d'autorité suspendre ou annuler la protection
3 D Secure ou demander d'autres modification de votre contrat.

Fraude

Cyberplus Paiement est basé sur un contrat de vente à distance CB. La réglementation protège le porteur de carte et lui permet d'annuler une transaction **jusqu'à 1 an** après la transaction bancaire, en cas d'utilisation frauduleuse de sa carte.
Cette contestation du porteur peut se concrétiser par un impayé sur votre compte du montant de la transaction et des frais de gestion des impayés, de la part de la banque.
Si vous le souhaitez, c'est alors à vous en tant que commerçant, d'entamer une procédure judiciaire auprès de votre client et de prouver que vous avez bien expédié la marchandise ou délivré le service au vrai porteur de carte.

Les tentatives de fraude sont souvent liées à des commandes massives et/ou répétées, effectuées le plus souvent avec des cartes étrangères et/ou à destination de l'étranger.
En tant que commerçant, la demande d'autorisation ne vous garantit pas contre les impayés.
Les transactions validées 3DS seront garanties en cas de contestation **pour les motifs fraude définis dans votre contrat**, mais ne le sont pas pour les autres motifs : Ex. lorsque le client précise que la marchandise expédiée n'est pas conforme à la commande ou est détériorée (se référer aux modalités de garantie 3 DS dans votre contrat accepteur CB VAD internet
Cyberplus Paiement).
Astuce : En cas de doute, n'hésitez pas à exiger un paiement préalable par virement (pas de chèques !). Pour les commandes étrangères c'est une excellente précaution (et la seule réellement efficace).
Lorsque vous avez une commande, avant d'expédier vos produits, vérifiez bien le plus possible de paramètres :
Cyberplus Paiement – Le Vade-Mecum 4/4
- Les coordonnées postales de l'acheteur : sont-elles « propres » ? (pas de boite postale, poste restante, camping, Hôtel etc. …). Et vérifiez les (annuaires, sociétés de vérification, courrier réel préalable à la livraison etc. …)
- Les coordonnées téléphoniques : Attention aux N° de portables seuls, vérifiez sur l'annuaire les numéros de téléphone fixe, appelez même directement et demandez à parler à la personne qui a passé la commande.
- Les coordonnées mails : privilégiez les adresses classiques (prénom + nom + FAI). Attention aux adresses gratuites
(Hotmail, Voilà, Google etc. …).
- demander dans la mesure du possible une signature à la livraison.
- analyser vos commandes, leurs pertinences, la logique des articles commandés.
- vérifier la cohérence entre l'adresse IP de l'internaute, fournie par Cyberplus Paiement et l'adresse de livraison et de facturation etc....
- analyser l'historique des commandes. N'expédiez pas une commande refusée dans un premier temps, par exemple pour motif « 43 » « carte volée » ; puis réitérée immédiatement par le fraudeur et acceptée par CyberPlus paiement à partir d'un nouveau numéro de carte.
- refuser toute commande répétée et fractionnée.
- soyez vigilant lorsque les commandes sont multiples ou effectuées avec des cartes étrangères et/ou livrables à l'étranger.
www.fia-net.com est un tiers de confiance, que vous pouvez contacter de façon indépendante et qui vous permet de détecter les commandes frauduleuses et donc de garantir dans les limites de leur contrat, votre CA.

Paiement en plusieurs fois / Cartes privatives

Duplication
Dans Cyberplus Paiement, vous avez déjà la possibilité de programmer en automatique plusieurs paiements successifs.
L'internaute se connecte et est débité par exemple d'un premier tiers, puis automatiquement (ou manuellement), le système demandera un second et un troisième paiement par exemple.
Attention, il s'agit de demandes **d'autorisations successives**. En tant que commerçant, vous n'êtes pas donc certain d'avoir un accord à la seconde ou troisième transaction.
Les paramètres de la Duplication sont déjà disponibles dans la documentation technique que possède votre développeur.
Attention, les duplications n'apparaissent pas dans le journal des transactions. (Voir avec le Développeur)
Seul, le premier paiement peut être authentifié 3 D Secure. Les paiements successifs seront non 3 D Secure.
Il ne peut pas y avoir de duplication à partir d'une transaction initiale faite par une carte de type e-cb ou un porteur 3 DS.
- www.1euro.com : Cyberplus Paiement Systempay n'est pas compatible 1euro.com au 01/12/2009
- Cartes privatives : Les cartes privatives Cetelem, Cofinoga, Diner's… ne sont pas compatibles au 01/12/2009.
- Cyberplus Paiement SYSTEMPAY est compatible AMEX
Si vous souhaitez accepter des paiements effectués avec des cartes AMERICAN EXPRESS, vous devez contacter directement AMEX en tant que CYBER commerçant. Une fois affilié, vous devrez nous transmettre votre n° d'affiliation et nous même le transmettrons aux équipes techniques.
Sous un délai d'environ 10 jours ouvrés, le service vous sera ouvert.
Vous devez en parallèle (ou votre Développeur) "appeler" le logo de la carte privative en question, disponible dans la documentation technique pour le faire apparaître sur le site.
Ce service peut être rajouté en cours de vie du contrat.

Autres informations et recommandations importantes
Vous pouvez trouver des informations sur le commerce électronique sur le site Internet du gouvernement www.internet.gouv.fr et notamment sur :
- La Loi sur la Confiance dans l'Economie Numérique (LEN)
- La loi Châtel dite « pour le développement de la concurrence au service des consommateurs est applicable depuis le 01 juin
2008 qui vous oblige entre autre à :
- Indiquer, avant la conclusion du contrat, la date limite à laquelle vous vous engagez à livrer le bien ou exécuter la prestation de services
- Fournir des coordonnées téléphoniques permettant d'entrer effectivement en contact avec vous
- Mettre en place des moyens de communication qui ne supportent que des coûts de communication, à l'exclusion de tout coût supplémentaire spécifique permettant (...) de suivre l'exécution de sa commande, d'exercer son droit de rétractation ou de faire jouer la garantie
- Indiquer "l'existence d'un droit de rétractation, et ses limites éventuelles ou, dans le cas où ce droit ne s'applique pas, l'absence d'un droit de rétractation
- Lorsque le droit de rétractation est exercé, rembourser le consommateur de la totalité des sommes versées, dans les meilleurs délais

CNIL : déclaration systématique de votre site (Loi Informatique et Libertés" du 6 janvier 1978 modifiée par la loi du 6 août 2004) www.cnil.fr.
Vous devez également apposer sur votre site tout un ensemble d'informations pour vos clients (conditions générales de vente, droit de rétractation, protection des données personnelles, droit de rectification, adresse physique de l'entreprise, tel, coordonnées du SAV etc. …)
Cyberplus Paiement – Le Vade-Mecum 5/4
Savez-vous par exemple, que vous devez conserver pendant 10 ans vos factures et paramètres d'une commande supérieure à 120 €, et que vous devez en assurer le libre accès à votre client ? (Décret du 18 fév. 2005).
D'une manière générale, il vous convient de prendre tous les renseignements et mesures nécessaires afin d'être en parfaite harmonie avec la loi et les règlements en vigueur à ce jour et de rester très vigilant au sujet des évolutions réglementaires à venir.
Astuce : Demandez les conseils d'un avocat spécialisé et optez systématiquement pour un abonnement aux informations concernant le domaine du e-commerce. Adhérez à une association de commerçants de vente à distance http://www.fevad.com.

BANQUE POPULAIRE
BOURGOGNE
FRANCHE-COMTÉ
www.bpbfc.banquepopulaire.fr

CYBERPLUS PAIEMENT

CONVENTION DE SERVICE CYBERPLUS PAIEMENT

Version juin 2014

CONDITIONS GENERALES

1. Définitions

Toutes les définitions insérées dans les Conditions Générales du contrat d'acceptation en paiement à distance sécurisé, du contrat d'acceptation en paiement à distance à sécurité optionnelle et progressive, et du contrat d'acceptation en paiement à distance (ci-après « contrat d'acceptation en paiement à distance « classique » ») par cartes « CB » ou agréées « CB » sont applicables à la présente Convention.
Les définitions supplémentaires suivantes auront la signification qui suit :

Acheteur :
Désigne tout consommateur réalisant une opération d'achat à distance auprès du Client, Accepteur « CB »

Solution Cyberplus Paiement :
Désigne les offres commerciales du Service Cyberplus Paiement

Service Cyberplus Paiement :
Désigne l'ensemble des traitements et fonctionnalités liés à l'encaissement des paiements en vente à distance et intégrés dans la Solution Cyberplus Paiement.

Formulaire d'Inscription Client :
Désigne le document d'enregistrement et de paramétrage des conditions du Service Cyberplus Paiement souscrites par le Client auprès de la Banque Populaire. Il fait partie des Conditions Particulières de la présente convention.

2. Objet de la convention de services

La Banque Populaire propose à ses clients commerçants ou entreprises, Accepteurs « CB » (ci-après le ou les « Client(s) »), réalisant des ventes à distance, une solution d'encaissement des ordres de paiement par carte donnés à distance à leur profit, ainsi qu'un ensemble de traitements et fonctionnalités associés, désignés sous le nom de « Service Cyberplus Paiement ».
Les présentes Conditions Générales ont pour objet de définir les modalités techniques et juridiques selon lesquelles la Banque Populaire permet au Client de bénéficier de la Solution Cyberplus Paiement.

L'adhésion à la Solution Cyberplus Paiement est effectuée par la signature du Formulaire d'Inscription Client. Par cette signature, le Client accepte les présentes Conditions Générales, souscrit à l'une des trois offres Cyberplus Paiement et, le cas échéant, aux services additionnels mentionnés dans son Formulaire d'Inscription Client, et s'engage à respecter les instructions du Kit documentaire visé à l'article 6 ci-après. Le Formulaire d'Inscription Client et les présentes Conditions Générales constituent la présente convention, ci-après dénommée la « Convention ».
Elle annule et remplace toute autre convention qui aurait pu être signée entre les Parties, relative à la Solution Cyberplus Paiement.

3. Présentation de la solution Cyberplus paiement

La Solution Cyberplus Paiement se décline en trois offres commerciales correspondant chacune à un canal de vente à distance :

- L'offre **Cyberplus Paiement ACCESS** s'adresse aux Clients qui pratiquent une activité de vente à distance dite « classique » (téléphone, télécopie, ou courrier). Ils disposent d'un OUTIL DE GESTION DE CAISSE doté d'un accès sécurisé à partir duquel ils pourront saisir les données de carte bancaire de leurs Acheteurs. Ces données sont enregistrées et stockées sur le Serveur sécurisé de la Solution Cyberplus Paiement.
- L'offre **Cyberplus Paiement NET** permet aux Clients qui pratiquent une activité de vente à distance dite « en ligne » (toute interface PC fixe ou portable, Smartphone ou tablette disposant d'une connexion internet permettant d'afficher la page de paiement de la Solution Cyberplus Paiement), de proposer un formulaire de paiement en ligne à leurs Acheteurs internautes à partir de leur boutique en ligne pour enregistrer les données de leur carte bancaire.
- L'offre **Cyberplus Paiement MIX** est destinée aux Clients pratiquant à la fois une activité de vente à distance « classique » et/ou une activité de vente « en ligne » et qui recherchent une solution de paiement s'intégrant dans le processus de commande au sein de leur système d'information.

3.1 La Solution Cyberplus Paiement ACCESS

CYBERPLUS PAIEMENT ACCESS

Cette Solution requiert la signature d'un contrat d'acceptation en paiement à distance « classique ».

La Solution Access comprend :

- **L'acceptation des moyens de paiement suivants :**
  - cartes bancaires : CB, VISA et MASTERCARD et MAESTRO,
  - cartes privatives (1) : American Express, Cofinoga, Cetelem, JCB
  - e-carte bleue

- **L'outil de gestion de caisse**
  - consultation des opérations de paiement,
  - suivi du fichier des remises bancaires,
  - possibilité de saisir, valider, consulter, annuler, modifier, rembourser et dupliquer une opération de paiement,
  - capacité d'exporter les transactions sous format XLS, XML ou CSV.

- **Les canaux de vente**
  - vente à distance « classique »
    - téléphone
    - télécopie
    - catalogue papier
    - courrier
    - email.

- **Les typologies de paiement (1)** :
  - paiement à l'acte,
  - paiement en « n » fois,
  - paiement différé,

- **La sécurité de la Solution Cyberplus Paiement Access :**
  - certification PCI-DSS,
  - accès sécurisé à l'outil de gestion de caisse par identifiant et mot de passe,
  - renouvellement des mots de passe tous les trois (3) mois,
  - envoi des identifiants et mots de passe par email (avec saisie du code de première connexion obligatoire).

Les services additionnels

Ces services sont optionnels et comprennent :

- Mail avec lien pour paiement
- Suivi Client
- Contrôle Risques
- Gestion Bancaire Simplifiée (sous forme visuelle uniquement)
- Gestion Utilisateurs

Le détail de ces services est disponible sur le site www.cyberpluspaiement.com.

(1) Liste non exhaustive, reportez-vous à la fiche produit pour connaître toutes les cartes privatives et/ou typologie de paiement disponibles ou consultez votre conseiller Banque Populaire

3.2 La Solution Cyberplus Paiement NET

CYBERPLUS PAIEMENT NET

Cette Solution requiert la signature d'un contrat d'acceptation en paiement à distance sécurisé ou d'un contrat d'acceptation en paiement à distance à sécurité optionnelle et progressive.

La Solution Cyberplus Paiement NET comprend :

- **Le formulaire de paiement**
  - affichage des cours de change en devises (contre-valeur),
  - affichage des pages de paiement en multi-langues (8 langues) (1),
  - affichage dynamique pour les mobiles et les tablettes,
  - restitution sur le ticket de paiement de l'Acheteur des échéances en cas de paiement en « n » fois,
  - personnalisation du logo du Client,
  - prise en charge du protocole 3DS, le cas échéant selon les critères d'application dudit protocole choisis par le Client, et sous sa responsabilité, dans le cadre d'un contrat d'acceptation en paiement à distance à sécurité optionnelle et progressive.

- **L'acceptation des moyens de paiement suivants :**
  - cartes bancaires : CB, VISA et MASTERCARD et MAESTRO,
  - cartes privatives (2) : American Express, Cofinoga, Cetelem, JCB
  - e-carte bleue,

- **L'outil de gestion de caisse**
  - consultation des opérations de paiement,
  - suivi du fichier des remises bancaires,
  - possibilité de valider, consulter, annuler, modifier, rembourser une opération de paiement,
  - capacité d'exporter les transactions sous format XLS, XML ou CSV.

- **Les canaux de vente**
  - vente en ligne **(site internet)**
    - boutique en ligne depuis une connexion Internet (poste fixe, mobile et tablette connectés à Internet).

- **Les typologies de paiement (2)**
  - paiement à l'acte,
  - paiement en « n » fois,
  - paiement différé,

- **La sécurité de la Solution Cyberplus Paiement :**
  - certification PCI-DSS,
  - accès sécurisé à l'outil de gestion de caisse par identifiant et mot de passe,
  - renouvellement des mots de passe tous les trois (3) mois,
  - envoi des identifiants et mots de passe par email (avec saisie du code de première connexion obligatoire),
  - génération d'un certificat d'authentification de chaque site ou boutique du Client
    - génération du certificat en temps réel
  - garantie des paiements dans les conditions du protocole 3DS o restitution en temps réel vers le site ou boutique du Client de l'existence ou non de la

garantie,

- affichage en temps réel de l'existence ou non de la garantie à partir de l'outil gestion de caisse,
- restitution en différé de l'existence ou non de la garantie dans les journaux de transactions.

(1) Allemand, anglais, chinois, espagnol, italien, japonais, portugais et français
(2) Liste non exhaustive, reportez-vous à la fiche produit pour connaître toutes les cartes privatives et/ou typologie de paiement disponibles ou consultez votre conseiller Banque Populaire

Les services additionnels

Ces services sont optionnels et comprennent :

- *Mail avec lien pour paiement*
- *Gestion personnalisation avancée*
- *Suivi Client,*
- *Contrôle Risques,*
- *Gestion Bancaire Simplifiée (sous forme visuelle et fichiers),*
- *Gestion Compte Client*
- *Gestion Utilisateurs*

Le détail de ces services est disponible sur le site www.cyberpluspaiement.com.

3.3 La Solution Cyberplus Paiement MIX

CYBERPLUS PAIEMENT MIX

Cette Solution requiert la signature d'un contrat d'acceptation en paiement à distance sécurisé et/ou de la signature d'un contrat d'acceptation en paiement à distance « classique » ou d'un contrat d'acceptation en paiement à distance à sécurité optionnelle et progressive.

La Solution Cyberplus Paiement MIX comprend :

3.3.1 Pour la vente à distance en ligne

Avec la Solution Cyberplus Paiement MIX, le Client a le choix entre deux types de configuration pour gérer **le paiement en ligne** :

- **soit le formulaire de paiement Cyberplus Paiement MIX**
  - utilisation du formulaire de paiement en HTTP POST,
  - affichage des cours de change en devises (contre-valeur),
  - affichage des pages de paiement en multi-langues (8 langues) (1),
  - affichage dynamique pour les mobiles et les tablettes,
  - restitution sur le ticket de paiement de l'Acheteur des échéances en cas de paiement en « n » fois,
  - personnalisation du logo du Client,
  - prise en charge du protocole 3DS, le cas échéant selon les critères d'application dudit protocole choisis par le Client, et sous sa responsabilité, dans le cadre d'un contrat d'acceptation en paiement à distance à sécurité optionnelle et progressive.
- **soit le formulaire de paiement de son site marchand (URL du Client)**
  - utilisation de web services (protocole SOAP),
  - gestion des différentes fonctions liées au paiement sécurisé
    - création
    - validation
    - modification
    - remboursement
    - duplication
    - interrogation
  - mise à disposition des outils permettant l'utilisation du protocole 3DS.

(1) Allemand, anglais, chinois, espagnol, italien, japonais, portugais et français

3.3.2 Pour la vente à distance classique

Avec la Solution Cyberplus Paiement MIX, le Client a le choix entre deux types de configuration pour gérer **le paiement à distance « classique »** :

- **soit à partir de son système d'information**
  - utilisation de web services (protocole SOAP),
  - gestion des différentes fonctions liées au paiement sécurisé
    - création
    - validation
    - modification
    - remboursement
    - duplication
    - interrogation
- **soit avec l'OUTIL GESTION DE CAISSE**
  - consultation des opérations de paiement,
  - suivi du fichier des remises bancaires,
  - possibilité de saisir, valider, consulter, annuler, modifier, rembourser et dupliquer une transaction,
  - capacité d'exporter les opérations de paiement sous format XLS, XML ou CSV.

3.3.3 Les canaux de vente

- vente à distance « classique »
  - téléphone,
  - fax,
  - catalogue papier,
  - courrier,
  - email,
  - Logiciel métier interne (logiciel de commande),
  - SVI (serveur vocal interactif),
  - Call center (plate-forme téléphonique),
  - Centre de saisie (plate-forme de saisie).
- vente en ligne **(site internet)**
  - Boutique en ligne depuis une connexion Internet (poste fixe, mobile et tablette connectés à Internet).

3.3.4 L'acceptation des moyens de paiement suivants :

- cartes bancaires : CB, VISA et MASTERCARD et MAESTRO,
- cartes privatives (1) : American Express, Cofinoga, Cetelem, JCB,
- e-carte bleue

3.3.4 Les typologies de paiement (1)

- paiement à l'acte,
- paiement en « n » fois,
- paiement différé,

3.3.5 La sécurité

- certification PCI-DSS,
- accès à l'outil de gestion de caisse par identifiant et mot de passe,
- renouvellement des mots de passe tous les trois (3) mois,
- envoi des identifiants et mots de passe par email (avec saisie du code de première connexion obligatoire),
- gestion de certificat pour l'authentification de chaque canal,
    - génération du certificat en temps réel,
- garantie des paiements dans les conditions du protocole 3DS,
    - restitution en temps réel dans la réponse automatique,
    - affichage en temps réel à partir de l'outil gestion de caisse,
    - restitution en différé dans les journaux de transactions.

(1) Liste non exhaustive, reportez-vous à la fiche produit pour connaître toutes les cartes privatives et/ou typologie de paiement disponibles ou consultez votre conseiller Banque Populaire.

Les services additionnels

Ces services sont optionnels et comprennent :

- Mail avec lien pour paiement
- Gestion personnalisation avancée
- Suivi Client
- Contrôle Risques
- Gestion Bancaire Simplifiée (sous forme visuelle et fichiers)
- Gestion Compte Client
- Gestion Utilisateurs

Le détail de ces services est disponible sur le site www.cyberpluspaiement.comwww.cyberpluspaiement.com.

4. Conditions des fonctions de la solution Cyberplus paiement

4.1 Paiement diffère

Le Client a la possibilité de choisir le délai de rétention des paiements effectués via le Service Cyberplus Paiement avant remise en banque.
Le Client définit librement ce délai dans l'OUTIL DE GESTION DE CAISSE. Par défaut, le délai de remise en banque est paramétré au jour de l'opération de paiement.

4.2 Validation manuelle des paiements

Par défaut, l'envoi en remise des paiements dont la sécurisation est assurée par le Service Cyberplus Paiement est automatique.
Le Client a la possibilité de confirmer cet envoi en remise de façon manuelle.
Le Client signifie librement son choix (validation automatique ou manuelle) dans l'OUTIL DE GESTION DE CAISSE.
Dans le cas où le Client sélectionne « validation manuelle », chaque demande de paiement sécurisé en ligne effectuée par ses Acheteurs doit être validée à l'aide de la fonction « valider » présente dans l'OUTIL DE GESTION DE CAISSE.

La Banque Populaire ne pourra donc être tenue responsable par le Client ou par tout tiers de la non réalisation d'un règlement consécutif à un défaut de validation en mode manuel ainsi que des conséquences qui pourraient en découler.

4.3 Paiement en plusieurs fois

Le Client a la possibilité de faire bénéficier ses Acheteurs d'un service de paiement en plusieurs fois par carte "CB" ou agréée "CB" (ex : VISA ou MasterCard).
Le Client doit communiquer le détail des échéances à son Acheteur préalablement à la validation de la commande.
Par ailleurs, la carte de son Acheteur doit être compatible avec cette option (date d'expiration suffisamment lointaine).
Le paiement par e-Carte Bleue n'est pas autorisé dans le cadre de ce service.
Si le Client a souscrit au service additionnel « Suivi Client », l'e-mail de confirmation de paiement est adressé à l'Acheteur lors de la première échéance et il comporte un échéancier de paiement précisant les dates et montants des prochaines échéances.
La Banque Populaire fournit le service de sécurisation exclusivement pour le premier paiement. Elle ne pourra être tenue pour responsable par le Client ou son Acheteur du fait que la banque dudit Acheteur refuse d'honorer les demandes de paiements en plusieurs fois.

4.5 Affichage multi-devises

Ce service permet au Client de proposer à ses propres clients un paiement dans une devise autre que l'euro.
Le Client est informé que les paiements par carte dont la sécurisation est assurée par le Service Cyberplus Paiement s'effectuent selon les modalités prévues dans les accords conclus entre la Banque Populaire et les réseaux internationaux (ex : Visa, MasterCard …).
Aux termes de ces accords, la compensation des paiements réalisés sur le site internet du Client dans une devise étrangère acceptée par lui se fera en euros en application du taux de change en vigueur à la date de traitement de l'opération de paiement et appliqué par le réseau international dont la marque figure sur la carte utilisée pour le paiement, Le produit de ce paiement sera imputé sur un compte dont la devise de tenue de compte est l'euro.

Le Client reconnaît qu'il est seul responsable, pour les différentes devises applicables, de l'indication du taux de conversion des paiements effectuées en devises étrangères qu'il a paramétré sur son site internet, la Banque Populaire n'étant responsable ni de la conversion, ni du taux de change appliqué.

5. Conditions des services additionnels

5.1 Personnalisation avancée

Le service de Personnalisation avancée permet au Client de modifier en toute autonomie les aspects graphiques et textuels du formulaire de paiement par défaut ou standard, selon sa propre charte visuelle à partir de l'OUTIL GESTION DE CAISSE de Cyberplus Paiement. Cette interface permet la création ou l'importation de plusieurs formulaires de paiement par boutique permettant au Client de les gérer dynamiquement selon ses temps forts commerciaux (ex : page dédiée pour Noël). Le service permet la prévisualisation des formulaires à la fois en mode web et mobile et une mise en ligne en temps réel depuis l'OUTIL GESTION DE CAISSE.
L'utilisation de ce service par le Client s'effectue sous réserve du respect par ce dernier des stipulations figurant à l'article 11 des présentes.

Le Client assume également la pleine et entière responsabilité de la personnalisation de son formulaire de paiement et s'engage à prendre à sa charge toutes les conséquences que pourraient avoir, à l'égard de la Banque Populaire, une utilisation de ce service non conforme à la loi.

5.2 Mail avec lien pour paiement

Le service Mail avec lien pour paiement permet au Client de transmettre à ses Acheteurs, sous sa seule responsabilité, des courriers électroniques ponctuels intégrant dans le corps des messages un lien URL pointant vers le formulaire de paiement Cyberplus Paiement.
Le Client peut opter pour ce service, afin de transmettre des messages électroniques afférents à un produit, un service, une cotisation, un règlement de facture ou une proposition contractuelle, quelle qu'en soit la nature, et de permettre à ses Acheteurs, destinataires de ce courrier électronique, de procéder éventuellement à un paiement par carte.
Le Client est seul responsable du respect des lois et règlements applicables aux ventes et prestations réalisées à distance, ainsi que celles applicables au commerce électronique. Il reconnaît qu'il doit se conformer à ces dispositions ou à celles qui pourront intervenir et, le cas échéant, se soumettre aux dispositions relatives aux dons et règlement de cotisations qui lui sont applicables.

5.2.1 Gestion du contenu de l'e-mail et envoi aux Acheteurs

Insertion d'un lien URL vers le formulaire de paiement Cyberplus Paiement

Via l'OUTIL GESTION DE CAISSE, le Client peut paramétrer sous sa seule responsabilité les caractéristiques de l'ordre de paiement associé au lien URL inséré dans l'e-mail (durée, montant et devise) et modifier le texte par défaut proposé par le service Mail avec lien pour paiement. Une fois ces étapes de paramétrages terminées, le Client peut procéder à l'envoi depuis le Service Cyberplus Paiement des e-mails de façon unitaire dans la limite de 100 adresses saisies depuis l'OUTIL GESTION DE CAISSE.
La Banque Populaire s'engage à insérer dans le courrier électronique rédigé par le Client, un lien URL pointant vers le formulaire de paiement Cyberplus Paiement, afin de permettre à tout Acheteur destinataire d'un message de donner éventuellement un ordre de paiement.

5.2.2 Génération de liens URLs par le service Cyberplus Paiement et gestion des envois d'e-mails par le Client

Via l'utilisation de Web services, le Client peut demander la génération de liens URL. A cette fin, le Client adresse les caractéristiques de l'ordre de paiement au service Cyberplus Paiement qui lui restitue un lien URL correspondant (durée, montant et devise). Une fois le lien récupéré, le Client peut procéder à la gestion du contenu de l'e-mail et à son envoi depuis ses propres outils à partir de son système d'information ou celui d'un tiers.
La Banque Populaire s'engage à produire le lien URL comportant les caractéristiques de l'ordre de paiement pointant sur le formulaire de paiement Cyberplus Paiement, mais ne pourra être tenue responsable du contenu de l'e-mail.

5.2.3 Licéité du contenu du message

Le Client est seul responsable des informations contenues dans ses messages adressés à ses Acheteurs.
En tant que diffuseur et non éditeur des messages, la Banque Populaire n'assurera aucun contrôle sur la licéité du contenu des messages du Client.
Le Client s'engage à ce que les messages émis respectent la réglementation en vigueur (respect des bonnes mœurs, de l'ordre public, interdiction de toute forme de manifestation raciste…).
Le Client s'engage également à respecter les droits de la personnalité et le droit de la propriété intellectuelle d'autrui. Il déclare notamment posséder les droits de reproduction et de représentation de l'image des personnes et des œuvres intellectuelles, textes, éléments graphiques, artistiques, sonores présents dans les messages.
Par ailleurs, le Client s'engage aussi à respecter la législation propre au commerce, à la vente à distance, à la consommation et à la protection des données nominatives et à ne pas se recommander de la Banque Populaire auprès de ses Acheteurs.

5.2.4 Licéité de l'émission du message

Le Client est seul responsable des adresses électroniques utilisées dans le cadre du service Mail avec lien pour paiement.
À cet égard, il s'assure notamment que la personne à laquelle il adresse ce message, l'a expressément et préalablement autorisé à recevoir des courriers électroniques de cette nature et qu'elle a été dûment informée de ses droits.
Le Client s'engage à respecter l'ensemble de la réglementation relative à la prospection par courrier électronique et au Code des postes et télécommunications et plus particulièrement les dispositions de l'article L34-5 dudit code.
La Banque Populaire ne saurait être tenue pour responsable de toutes communications ou de tout envoi d'un courrier électronique sans le consentement préalable et exprès du destinataire, des conséquences résultant d'un problème ou défaut d'acheminement des messages adressés par le Client à ses propres Acheteurs, dont la liste des adresses électroniques a été communiquée à la Banque Populaire dans le cadre du service Paiement par e-mail.
La Banque Populaire garantit au Client qu'aucun usage commercial ne sera fait par celle-ci des données et notamment des adresses électroniques transmises par le Client à la Banque Populaire dans le cadre du service Mail avec lien pour paiement.

5.2.5 Responsabilités

Le Client s'engage à informer la Banque Populaire, par lettre recommandée avec accusé de réception de toutes plaintes, actions en justice, réclamations exercée par tout tiers, directement ou indirectement, liées à la diffusion des messages liés au service Mail avec lien pour paiement.
Le Client s'engage à assurer à ses frais la défense de la Banque Populaire dans le cas où cette dernière ferait objet d'une action en revendication relative aux données contenues dans les messages, et à prendre à sa charge l'indemnité due en réparation du préjudice éventuellement subi.

5.3 Contrôle risques

Ce service est constitué d'un ensemble de contrôles permettant au Client d'affiner sa gestion client en fonction de ses propres critères de risque. Le résultat des contrôles est restitué en temps réel dans l'OUTIL GESTION DE CAISSE par le biais d'un indicateur. Il existe également la possibilité de disposer de ces informations dans le journal des transactions. Il est possible de choisir, pour chaque contrôle, un mode de fonctionnement différent (filtre ou scoring).
La Banque Populaire ne saurait être tenue pour responsable des choix du Client concernant ses critères de risque. En souscrivant ce service additionnel, le Client reconnaît avoir reçu de la Banque Populaire la documentation relative au service et avoir été informé de la possibilité de recourir à l'Assistance Clients visée à l'article 10. Le Client reconnaît disposer des compétences nécessaires à son paramétrage et son utilisation.

5.4 Gestion compte client

Le service Gestion Compte Client offre la possibilité au Client de proposer un moyen de payer plus rapide et plus convivial à ses Acheteurs. Une fois le compte client créé de façon sécurisée sur la plate-forme de paiement, l'Acheteur n'a plus besoin de saisir les données de sa carte bancaire à chaque paiement.

L'Acheteur et le Client sont notifiés de la création du compte client et de l'identifiant qui lui est rattaché.
La conservation sécurisée des identifiants de ses Acheteurs est sous la responsabilité exclusive du Client

5.5 Gestion bancaire simplifiée

Ce service comprend le rapprochement bancaire et le rapprochement des impayés
Le service de rapprochement bancaire permet de faire le lien entre les commandes enregistrées sur les différents canaux de vente avec les règlements indiqués sur le relevé d'opérations cartes du Client. Ce service rapproche quotidiennement et automatiquement les commandes validées sur le site internet du Client ou tout autre canal de vente avec son relevé d'opérations cartes. Le résultat de ce rapprochement se matérialise par la restitution d'un indicateur disponible depuis l'OUTIL DE GESTION DE CAISSE et/ou sous forme de fichier.
Le rapprochement des impayés permet d'informer le Client, sous la forme d'un indicateur de type OUI ou NON, de la réception d'un impayé sur un paiement par carte. Ce service est disponible sous forme visuelle à partir de l'OUTIL GESTION DE CAISSE et/ou sous forme de fichier à l'identique de ce qui existe pour le rapprochement bancaire.

5.6 Gestion utilisateur

La gestion utilisateur permet à un Client de gérer, sous sa seule responsabilité, en toute autonomie les accès et les habilitations à l'OUTIL GESTION DE CAISSE pour chacun de ses collaborateurs. Il est disponible directement à partir de l'OUTIL DE GESTION DE CAISSE et repose sur la désignation d'un administrateur à partir du Formulaire d'Inscription Client.

5.7 Suivi client

Le service Suivi Client permet d'apporter d'avantage de personnalisation du service de paiement vis-à-vis des Acheteurs. Pour chaque paiement validé, un e-mail de confirmation personnalisé au logo de la Banque Populaire est adressé en temps réel au client pour l'informer du détail du paiement lié à sa commande. En cas de paiement en « n fois », un échéancier est présenté dans l'e-mail pour informer le client des dates et des montants des prochains paiements.

6. Documentation du service Cyberplus paiement

Dès réception du Formulaire d'Inscription Client composant les Conditions Particulières, la Banque Populaire adresse au Client un Kit documentaire intégrant les modalités techniques de mise en œuvre du Service Cyberplus Paiement. Les modalités de recettes et de passage en production sont décrites dans ce Kit documentaire.
Ce Kit est spécifique à la Solution Cyberplus Paiement souscrite par le Client auprès de la Banque Populaire.

6.1 Solution Cyberplus paiement Access

Le Kit documentaire ACCESS est composé des éléments suivants :
Un guide de démarrage,
- Un manuel utilisateur de l'outil de « gestion de caisse »,
- Un descriptif des journaux de reporting.

6.2 Solutions Cyberplus paiement Net et Mix

Les Kits documentaires NET et MIX sont composés des éléments suivants :
- Un guide de démarrage,
- Un guide d'implémentation de la page de paiement pour les paiements en ligne,
- Un kit d'images pour le formulaire de paiement en ligne,
- Un guide des cartes de test,
- Un guide d'implémentation standard des web services,
- Un manuel utilisateur de l'outil « gestion de caisse »,
- Un descriptif des journaux de reporting
- Un guide pratique commerçant :
  - Prise en main rapide de l'outil « gestion de caisse »,
  - Cinématique des transactions,
  - Garantie de paiement 3DSecure,
  - Suivi Client-Accepteur «CB» (service additionnel),
  - Gestion Bancaire Simplifiée en mode visuel (service additionnel),
  - Contrôle Risques (service additionnel).
- Un Procès-verbal de recette,

Un service de Support Technique et d'Assistance Clients tels que décrits aux articles 7.3.3 et 10 ci-dessous est à la disposition du Client.
Le Client s'engage à respecter les présentes Conditions Générales ainsi que les spécifications d'utilisation du Service Cyberplus Paiement telles que décrites dans la Documentation.
Le Client reconnaît disposer de la compétence nécessaire pour procéder aux vérifications et tests nécessaires tant lors de l'installation qu'au cours de l'utilisation du Service Cyberplus Paiement.
Pendant l'exécution du contrat, le Client reste gardien et seul responsable de ses matériels, logiciels, fichiers, programmes, informations ou bases de données.
Le Client est seul responsable de la gestion et du stockage du certificat de production de sa boutique en ligne. En cas de défaillance sécuritaire, la Banque Populaire ne peut être tenue pour responsable.
Le Client reconnaît que la Banque Populaire a satisfait à ses obligations de conseil et d'information concernant les caractéristiques essentielles et les modalités de fonctionnement de la Solution Cyberplus Paiement et/ou des services additionnels, eu égard aux besoins qu'il a exprimés.

7. Obligations du client relatives au service Cyberplus paiement

7.1 Mise en garde et conditions d'adhésion

Il appartient au Client de s'assurer notamment de l'adéquation de la Solution Cyberplus Paiement à ses propres besoins et de la possibilité, ainsi que de l'opportunité pour lui d'utiliser ce service.
Le Client est tenu de vérifier que son environnement informatique, en ce compris ses serveurs, systèmes d'exploitation, logiciels et ordinateurs ou ceux d'un tiers s'il a recourt à la sous-traitance, est en parfait état de fonctionnement afin de permettre à ses propres clients d'utiliser le Service Cyberplus Paiement.
Le Client reconnaît, par ailleurs, avoir été informé des risques inhérents à l'utilisation des réseaux internet et particulièrement, en termes de :
- Défaut de sécurité et de confidentialité dans la transmission, dans la réception des instructions et/ou des informations sur les demandes de paiement sécurisé ;
- Performance dans la transmission des messages, d'informations sur la demande de paiement sécurisé et d'exécution d'instructions ;
- Mise à jour différée de l'ensemble des informations sur les demandes de paiement sécurisé effectuées.

Le Client est informé que pour bénéficier du Service Cyberplus Paiement, il doit :
- être titulaire d'un compte bancaire ouvert auprès d'une Banque Populaire,
- avoir souscrit un contrat d'acceptation en paiement à distance

par cartes bancaires CB ou agréées CB en cours de validité avec Banque Populaire,

- le cas échéant, avoir souscrit auprès du réseau privatif concerné le contrat d'acceptation en paiement par carte nécessaire pour permettre à ses clients de payer avec une telle carte (ex : American Express …). La Banque Populaire décline toute responsabilité en cas de défaut de fourniture par le réseau privatif des identifiant et mot de passe correspondant au contrat souscrit, et en cas d'anomalie ou dysfonctionnement dans le traitement des ordres de paiement reçus dans le cadre dudit réseau privatif.

7.2 Sécurité

Le Client s'engage à mettre en œuvre et à faire mettre en œuvre les dispositifs (matériel, procédures...) permettant d'assurer la confidentialité et la sécurité des documents de spécifications techniques, les fichiers, les données, les éléments sécuritaires remis par la Banque Populaire dans le cadre de la présente Convention.

7.2.1 Confidentialité des identifiants du Client

La Banque Populaire propose au Client un accès sécurisé à l'OUTIL DE GESTION DE CAISSE.
Le Client s'engage à respecter et à faire respecter l'ensemble des obligations de sécurité, qui sont mises à sa charge, et notamment à conserver sous son contrôle exclusif et dans le respect des obligations de confidentialité à sa charge, les identifiant et mot de passe. Il s'engage également à modifier régulièrement son mot de passe.
Le Client est entièrement responsable de l'usage et de la conservation de son identifiant et de son mot de passe, ainsi que des conséquences d'une divulgation, même involontaire, à quiconque ou d'une usurpation. Toute utilisation des codes d'accès et mots de passe du Client sera réputée effectuée par ce dernier. L'identification et l'authentification du Client au moyen de l'utilisation de l'identifiant et mot de passe valent imputabilité des opérations effectuées au Client.
En cas de perte ou d'oubli, le Client peut demander l'attribution d'un nouvel identifiant et d'un nouveau mot de passe

7.2.2 Protection des fichiers et documents

Le Client se prémunira impérativement contre tous risques concernant les fichiers, programmes et autres documents confiés à la Banque Populaire en constituant un double de ceux-ci. Le Client se déclare à cet égard pleinement informé de ce que les supports informatisés présentent une fragilité et une fiabilité nécessitant, d'une part de vérifier la qualité et l'exhaustivité de ses sauvegardes, d'autre part de réaliser des sauvegardes multiples.
Le Client est informé qu'il fait son affaire de la conservation et de l'archivage des documents concernant sa clientèle et/ou son activité pendant la durée légale et/ou règlementaire fixée par les textes.

7.3 Moyens techniques d'accès au Service Cyberplus Paiement

7.3.1 Environnement informatique du Client

Le Client doit s'assurer que son site internet et son environnement informatique, en ce compris ses serveurs, systèmes d'exploitation, logiciels et ordinateurs, permettent l'installation et l'utilisation du Service Cyberplus Paiement.
En cas d'hébergement de son site internet par un tiers, le Client doit s'assurer auprès de son hébergeur de la compatibilité de son environnement informatique avec le serveur Cyberplus Paiement.
Le Client s'engage à activer les fonctionnalités nécessaires à l'utilisation du Service Cyberplus Paiement, dans les meilleurs délais ou à les désactiver en cas de suspension, quelles qu'en soient les causes.
Dans le cadre de l'évolution du Service Cyberplus Paiement, le Client est informé que la Banque Populaire se réserve le droit de modifier, à tout moment, les spécifications techniques et caractéristiques du Service Cyberplus Paiement. Dans cette hypothèse, le Client sera préalablement informé par la Banque Populaire des modifications techniques substantielles.

7.3.2 Installation sur l'environnement informatique du Client

Le Service Cyberplus Paiement ne peut être utilisé que sur l'environnement informatique du seul site internet du Client précisé lors de la souscription dans son Formulaire d'Inscription Client.
Préalablement à tout changement d'activité et/ou d'URL concernant son site internet, le Client sollicitera l'accord de la Banque Populaire. En outre le Client s'assurera de la compatibilité de son nouvel environnement informatique et/ou de son nouveau site internet avec le Service Cyberplus Paiement.
Toute modification ou adaptation de l'environnement informatique et/ou du site internet, nécessaire à l'utilisation du Service Cyberplus Paiement, reste à la charge du Client et s'effectue sous sa seule responsabilité.
En tout état de cause, la Banque Populaire ne saurait supporter aucune conséquence liée à l'impossibilité totale ou partielle d'utiliser le Service Cyberplus Paiement, à la suite d'une modification de l'environnement informatique du Client ou d'une incompatibilité de systèmes informatiques.
Le Service Cyberplus Paiement s'appuie sur deux guides d'implémentation :

- Guide d'implémentation du formulaire de paiement,
- Guide d'implémentation standard Web service (uniquement pour l'offre commerciale Cyberplus paiement MIX).

Concernant les droits de propriété intellectuelle et la confidentialité, le Client s'engage à respecter scrupuleusement les dispositions des articles 12 et 13 de la présente Convention. Il s'engage également à respecter la documentation de service fournie par la Banque Populaire et à informer immédiatement cette-dernière en cas de dysfonctionnement du Service Cyberplus Paiement.

7.3.3 Support Technique à l'intégration du Service Cyberplus Paiement

Le Client pourra, dès signature du Formulaire d'Inscription Client, solliciter le Support Technique pour obtenir une aide à l'intégration des éléments nécessaires au Service Cyberplus Paiement :

Le Support Technique est assuré par la société partenaire LYRA NETWORK du lundi au vendredi **de 9h00 à 18h00.**
Tél. : 0811 363 364 (numéro Azur – coût d'un appel local depuis un poste fixe). **E-mail :** supportvad@lyra-network.com.

Le Client peut bénéficier de ce service à compter de la date de signature du Formulaire d'Inscription Client, en cas de problèmes ou de questions lors de l'interfaçage de son site internet au serveur Cyberplus Paiement.

7.3.4 Présentation du SITE INTERNET et /ou des messages

Sauf en cas d'option pour la personnalisation de sa page de paiement, le Client s'engage à faire figurer sur la page d'accueil de son site internet, ainsi que sur les messages qu'il adresse à partir de son site internet l'ensemble des informations relatives au Service Cyberplus Paiement.
A cet égard, le Client s'engage à y faire figurer :

- les Signes Distinctifs mis à sa disposition par la Banque Populaire pour l'utilisation du Service Cyberplus Paiement et, le cas échéant des Services Additionnels,

- les logos utilisés pour l'authentification 3-D Secure, tels que notamment Verified by Visa, Mastercard Secure code.

Le Client s'engage à communiquer à la Banque Populaire l'URL de son site internet via le Formulaire d'Inscription Client et à valider l'activation de la connexion au Service Cyberplus Paiement de la Banque Populaire et, le cas échéant, aux Services Additionnels.
Les parties s'engagent à coopérer pour la mise en place de tout hyperlien. Le Client dispose, après installation d'un hyperlien, d'un délai de quinze (15) jours pour adresser toute observation à la Banque Populaire. A défaut, le Client est réputé avoir validé le ou les hyperliens réalisés.
Le Client s'engage à vérifier la permanence et le maintien de la connexion au Service et reste seul responsable de la capacité de son serveur à traiter le trafic électronique, en termes d'accès simultané et de temps de réponse, qui sera généré à partir de la connexion au Service.

8 Disponibilité du service Cyberplus paiement

Le Service Cyberplus Paiement est accessible tous les jours (7 jours/7), 24 heures sur 24, sous réserve des indisponibilités occasionnelles énoncées ci-dessous.
Le Service Cyberplus Paiement peut être momentanément inaccessible afin de réaliser des opérations d'actualisation, de sauvegarde ou de maintenance. Dans ces hypothèses, la Banque Populaire s'efforcera d'en informer le Client par courrier électronique avant toute intervention.
D'une manière générale, le Client reconnaît que la disponibilité du Service Cyberplus Paiement ne saurait s'entendre de manière absolue, et qu'un certain nombre de défaillances, de retards ou de défauts de performance peuvent intervenir indépendamment de la volonté de la Banque Populaire, compte tenu de la structure du réseau internet ou GSM et des spécificités liées au Service Cyberplus Paiement.

9 Modification et évolution du service Cyberplus paiement

Il est expressément convenu entre les parties que la Banque Populaire se réserve le droit de modifier à tout moment, pour des raisons notamment techniques et/ou de sécurité, les conditions du Service Cyberplus Paiement.
Il est entendu entre les parties que toute nouvelle condition du Service Cyberplus Paiement entrera en vigueur à la date précisée par la Banque Populaire dans le courrier de notification adressé au Client par tous moyens. Seront joints à ce courrier les éléments d'information nécessaires pour l'exécution des mises à niveau.
Le Client disposera du délai stipulé dans le courrier de notification pour accepter ou résilier le Service Cyberplus Paiement dont les conditions auront été modifiées.
Si le Client n'effectue pas les dites mises à niveau dans les délais impartis, la responsabilité de la Banque Populaire ne saurait être recherchée en cas de dysfonctionnement du Service Cyberplus Paiement

10 Assistance clients lors de l'exploitation du service Cyberplus paiement

Le Client pourra faire appel à l'Assistance Clients en cas de problèmes survenus lors de l'exploitation du Service Cyberplus Paiement.
L'Assistance Clients est assurée par l'équipe Cyberplus Paiement du lundi au vendredi de **9h00 à 18h00.**
Tél. : 0811.363.364 (numéro Azur – coût d'un appel local depuis un poste fixe) **E-mail :** cyberplus.paiement@natixis.fr

L'Assistance Clients Cyberplus Paiement concerne toutes les demandes liées à la gestion courante des services (paramétrage du site/boutique et suivi des opérations de paiement) et au fonctionnement ou utilisation des outils de la Solution Cyberplus Paiement.
Le Client pourra contacter l'Assistance Clients par messagerie électronique ou par téléphone ou pendant les heures d'ouverture du service, telles que ci-avant précisées.
Avant chaque appel téléphonique, il appartient au Client :

- de se reporter à la Documentation visée à l'article 6 des présentes Conditions Générales et de décrire de façon précise et exhaustive, les symptômes du problème rencontré aux fins d'en faciliter le diagnostic ;
- d'adresser à la Banque Populaire la totalité des éléments demandés ;
- de rendre disponible le cas échéant son mandataire désigné sous le terme « d'Interlocuteur technique » dans le Formulaire d'Inscription Client, dont le Client garantit la compétence technique.

Le Client autorise la Banque Populaire à effectuer toutes les opérations de contrôle permettant de vérifier l'utilisation du Service Cyberplus Paiement conformément à la Documentation.
A partir des informations communiquées par le Client, la Banque Populaire procède au diagnostic et indique au Client, par téléphone ou par courrier électronique, la procédure à suivre pour pallier les problèmes rencontrés par ce dernier.

11. Respect de la législation en vigueur

Le Client s'engage à respecter la législation et les réglementations en vigueur, en particulier, à ne pas diffuser des informations contraires aux bonnes mœurs, à l'ordre public, aux droits et à la réputation de tiers, à la dignité humaine

Le Client reconnaît à ce titre qu'il a l'entière et pleine responsabilité de la licéité des contenus qu'il diffuse dans le cadre de l'utilisation de la Solution Cyberplus Paiement et du Service Cyberplus Paiement. Par conséquent, il garantit notamment que les contenus :

- ne portent pas atteinte à la vie privée de tiers
- ne pas portent pas atteinte aux droits de propriété intellectuelle de tiers
- n'incitent pas à la réalisation de crimes et délits
- ne font aucune discrimination
- ne provoquent pas la haine ou la violence en raison de la race, de l'ethnie ou de la nation,
- ne transmettent pas de fausses nouvelles,
- ne sont pas diffamatoires, injurieux, offensants et/ou outrageants - ne pas portent pas atteinte au droit à l'image des personnes.
- ne portent pas atteinte à l'image ni ne dénigrent les produits ou services offerts par des tiers
- ne contiennent pas d'informations fausses de nature à causer un préjudice à des tiers en influençant leur comportement
- ne sont pas obscènes, vulgaires, pornographiques ou indécents,
- ne constituent pas ou n'encouragent pas des comportements susceptibles de constituer un délit,

La Banque Populaire ne pourra être tenue responsable de toute infraction à la législation et réglementations précitées. Le Client garantit la Banque Populaire qu'il détient l'ensemble des droits d'auteur sur les contenus qu'il diffuse dans le cadre de l'utilisation du Service Cyberplus Paiement et de la Solution Cyberplus Paiement.

Le client garantit la Banque Populaire contre tous recours et/ou actions que pourraient former à un titre quelconque, les tiers sur tout ou partie des contenus diffusés par le Client.
Le Client s'engage, sous les mêmes conditions, à adhérer aux bons usages de la profession de la vente à distance et à les mettre en œuvre, à respecter les règles du commerce concernant la vente en général et de la vente à distance en particulier, ainsi que la législation notamment sur les devises, les taxes, les publications.
Dans le cas de vente en ligne à partir d'un site marchand, le Client déclare et garantit que ledit site, ainsi que les liens rattachés, ne présentent pas de caractère illicite, immoral ou illégal et qu'ils ne portent pas atteinte aux droits des tiers, notamment aux droits de la personnalité et aux droits de la propriété intellectuelle.
De même le Client garantit que les produits et services qu'il délivre via son site internet sont conformes à l'activité qu'il a initialement déclarée à la Banque Populaire lors de son adhésion au Service Cyberplus Paiement. A cet égard, le Client s'engage à informer sans délai la Banque Populaire de tout changement d'activité.
Le Client s'engage à ne pas mettre en œuvre une activité de galerie marchande virtuelle multi-sites ou de prestation de paiement centralisée sans l'accord écrit de la Banque Populaire.
Le Client garantit qu'il ne conservera, ni ne stockera, de manière informatique ou manuelle, les références bancaires des Acheteurs (numéro de la carte bancaire, numéro de compte bancaire,…) auxquelles il aurait eu accès, dans le cadre de l'utilisation du Service Cyberplus Paiement.
Toutefois, si le Client conserve les numéros de cartes bancaires des Acheteurs dans un fichier ayant pour finalité de lutter contre la fraude au paiement, celui-ci garantit la Banque Populaire qu'il a déclaré au préalable ce fichier ainsi que sa durée de conservation auprès de la CNIL et qu'il a informé clairement les Acheteurs de l'existence et de la finalité d'un tel traitement afin que ces derniers puissent s'y opposer et ce, conformément aux dispositions de la Loi Informatique et Libertés.
Le Client déclare détenir le droit d'usage et de diffusion des éléments (textes, éléments graphiques ...) qu'il utilise, et ne pas porter atteinte à un quelconque droit de propriété intellectuelle ou droit de la personnalité.

12. Droit de propriété intellectuelle

La Banque Populaire conserve, en tant que titulaire des droits, la propriété intellectuelle des documents techniques et plus généralement de tous les éléments remis au Client, ainsi que toutes les prérogatives s'y rattachant. Le Client n'acquiert par le Contrat Cyberplus Paiement aucun droit de propriété intellectuelle mais un simple droit d'utilisation personnel, non transférable et non exclusif pour la durée des présentes.
Le Client s'engage à ne pas modifier ou faire modifier les documents techniques ou les éléments remis, à ne pas les utiliser pour un autre usage que celui prévu par le Contrat Cyberplus Paiement, à respecter la documentation de service fournie par la Banque Populaire et à informer immédiatement cette-dernière en cas de dysfonctionnement.
Il s'oblige aussi à ne pas dupliquer ou faire dupliquer la documentation technique ou les éléments reçus pour une autre raison que celle des tests d'évaluation et dans ce cas, à détruire les copies dupliquées et à retourner l'ensemble de la documentation Cyberplus Paiement dès la fin des tests.
La Banque Populaire demeure propriétaire des procédés, moyens, méthodes et savoir-faire qu'elle met en œuvre pour exécuter ses prestations.

13. Confidentialité – secret bancaire

13.1 Le Client s'engage à garder le secret le plus absolu notamment sur les méthodes utilisées par la Banque Populaire et dont il pourrait avoir connaissance dans le cadre de l'exécution de la présente Convention Cyberplus Paiement. A ce titre, il s'engage notamment à ne transférer ou mettre à la disposition ou à la connaissance d'aucun tiers autre qu'un sous-traitant et dans la stricte limite nécessaire à la transmission des ordres de paiement vers le Service Cyberplus Paiement, et sous aucun prétexte, la Documentation technique visée à l'article 6 ci-avant, manuels utilisateurs, matériels ou droits dont il pourrait bénéficier ou avoir l'usage.
En cas de sous-traitance, le Client s'engage à imposer à ses sous-traitants le respect de la confidentialité des méthodes et Documentation technique précitées de la Banque Populaire relative à la présente Convention.
Il s'oblige en outre à informer sans délai la Banque Populaire de toute potentialité de divulgation du secret.

13.2 Les documents ou renseignements fournis par le Client, ainsi que les états, études et documents provenant de leur traitement sont couverts par le secret bancaire. En particulier, aucune communication n'en pourra être effectuée à des tiers, sauf dispositions légales l'y autorisant ou autorisation expresse du Client. La Banque Populaire s'oblige à respecter de façon absolue cette obligation au secret et à la faire respecter de la meilleure façon par son personnel, ses sous-traitants, ou prestataires de services. Pour l'application de cette disposition, il est précisé que conformément aux dispositions de l'article L.511-33,6° du Code monétaire et financier, des informations confidentielles pourront être communiquées à toute personne devant intervenir ou accéder aux fichiers et en particulier les conseils ou sous-traitants de la Banque Populaire.

13.3 L'obligation de confidentialité continuera à lier les parties et leurs ayants droit, pendant toute la durée de la Convention de service et pendant cinq (5) ans après sa résiliation ou son expiration. Le présent article survivra à la résiliation ou à l'expiration de la Convention pour quelque cause que ce soit.

14. Conditions financières - facturation et règlement

14.1 Les conditions financières du Service Cyberplus Paiement sont indiquées dans le Formulaire d'Inscription Commerçant spécifique à chaque Solution Cyberplus Paiement.
Sauf dispositions contraires, figurant dans le Formulaire d'Inscription Commerçant spécifique à la Solution Cyberplus Paiement, les factures de la Banque Populaire sont payables sans escompte dès réception.

14.2 Dans le cas où une facture ne serait pas réglée dans les trente (30) jours de son envoi par la Banque Populaire au Client, la Banque Populaire aura la faculté de suspendre l'exécution des prestations prévues par la présente Convention de service, jusqu'au règlement de la facture en souffrance, et sans que cette suspension puisse être considérée comme une inexécution de ses obligations contractuelles, ou comme une résiliation de Contrat Cyberplus Paiement du fait de la Banque Populaire, ou n'ouvre un quelconque droit à indemnisation pour le Client.
Tout mois commencé sera entièrement dû.

14.3 En outre, à compter du trente et unième jour, la somme due portera intérêt au taux de trois (3) fois le taux d'intérêt légal sans qu'une mise en demeure préalable soit nécessaire, même par simple lettre, l'intérêt étant dû et exigible par le seul fait de l'échéance du terme contractuel.

15. Responsabilité de la banque populaire

La Banque Populaire garantit ses prestations dans les conditions ci-dessous précisées :

15.1 Le Service est conforme aux spécifications de la documentation technique, à l'exclusion de toute adéquation à des besoins implicites envisagés par le Client. La Banque Populaire ne saurait toutefois être tenue pour responsable des dysfonctionnements du Service Cyberplus Paiement ayant pour origine l'intervention du Client ou de tiers, tels que notamment le fournisseur d'accès Internet (FAI) ou l'opérateur Télécom (par exemple, accès momentanément indisponible, lenteur ou retard dans l'affichage des pages HTML).

15.2 La Banque Populaire ne répond ni des dommages indirects tels que notamment manque à gagner, perte financière, perte de clientèle, perte de bénéfices ou d'économies escomptées, trouvant leur origine ou étant la conséquence de la Convention de service, ni des dommages causés à des personnes ou des biens distincts de l'objet de la présente convention de service.

15.3 Au cas où la responsabilité de la Banque Populaire serait retenue, et ce pour quelque raison que ce soit, les parties conviennent expressément que, quel que soit le préjudice subi, la Banque Populaire ne sera pas tenu de payer un montant supérieur aux redevances versées par le Client au titre des douze (12) derniers mois de facturation de la présente Convention de service.

15.4 La responsabilité de la Banque Populaire ne pourra également être engagée en cas d'usage impropre du Service Cyberplus Paiement, par l'Acheteur, le Client ou tout tiers non autorisé.

15.5 De même, la responsabilité de la Banque Populaire ne pourra être engagée en raison des conséquences susceptibles de découler d'un usage frauduleux ou abusif de l'identifiant et du mot de passe.

15.6 La Banque Populaire ne saurait être tenue pour responsable des difficultés liées à une mauvaise utilisation du Service Cyberplus paiement et de la Documentation visée à l'article 6 des présentes Conditions Générales.

15.7 La Banque Populaire ne saurait être tenue pour responsable des difficultés d'accès au site internet du Client ou au Service Cyberplus Paiement en raison de la saturation et de la complexité du réseau internet.

16. Divers

16.1 En cas de difficulté d'interprétation ou de contradiction entre les titres des articles et le texte de leur contenu, le contenu des articles primera sur leur titre.

16.2 Les dispositions de la présente Convention prévalent sur toute proposition ou accord antérieur, ainsi que sur toute autre communication antérieure entre les parties ayant trait au Service Cyberplus Paiement.

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

16.4 Aucune des deux parties ne sera tenue pour responsable vis-à-vis de l'autre de l'inexécution ou des retards dans l'exécution de la présente Convention du fait de la survenance d'un cas de force majeure ou d'évènements tels que l'intervention des autorités civiles ou militaires, l'interruption totale ou partielle des réseaux de communications, le refus de licence d'importation, les incendies, les grèves, les conflits sociaux, les dysfonctionnements de matériels ou toute autre cause qui serait raisonnablement hors de son contrôle.

17. Modification des conditions

La Banque Populaire peut modifier à tout moment la présente Convention, pour des raisons techniques ou relatives à la sécurité du Service Cyberplus Paiement. Elle en informera alors le Client par écrit.
A défaut d'accord sur les modifications, le Client a la possibilité de résilier la présente Convention sans indemnité de part ni d'autre et sans autre formalité que l'envoi d'une lettre recommandée avec demande d'avis de réception.
Sauf exercice de la faculté de résiliation par le Client, les nouvelles conditions entreront en vigueur dans le délai d'un (1) mois à compter de l'envoi de la lettre ou d'un courriel d'information.

18. Durée - suspension et résiliation du contrat

18.1 Durée de la Convention :

La présente Convention est conclue pour une durée indéterminée.

18.2 La suspension de la Convention :

La Banque Populaire pourra suspendre l'exécution de la présente Convention sans que cette suspension soit constitutive d'une résiliation ou d'un manquement à l'une de ses propres obligations, dans les cas suivants :

- dans le cas où le Client ne remplirait pas les obligations mises à sa charge (fourniture de données, accès aux renseignements, etc...) nécessaires à la bonne exécution de la présente Convention, Cette suspension pourra ainsi intervenir en cas de retard de paiement tel que prévu à l'article 14.2 de la présente Convention
- dans le cas où le contrat d'acceptation en paiement à distance sécurisé, le contrat d'acceptation en paiement à distance à sécurité optionnelle et progressive et/ou le contrat d'acceptation en paiement à distance « classique » par cartes « CB » ou agréées « CB » signés par acte séparé feraient l'objet d'une suspension.

La suspension sera notifiée au Client par lettre recommandée avec accusé de réception indiquant les motifs de la suspension. L'exécution reprendra une fois que les motifs à l'origine de cette suspension auront disparus, compte tenu des modifications de prix et de délais encourues de ce fait.

18.3 La résiliation de la Convention pour manquement :

En cas de manquement par l'une quelconque des parties, aux obligations dont elle a la charge au titre des présentes, et auquel il n'aurait pas été remédié dans un délai de huit (8) jours à compter de l'envoi d'une lettre recommandée avec demande d'avis de réception, l'autre partie pourra, prononcer de plein droit la résiliation de la présente Convention.
En pareil cas, la Banque Populaire, lorsqu'elle prononce la résiliation, aura droit au paiement des prestations exécutées et non facturées, et pourra demander en sus une indemnité de résiliation égale au triple de la facturation du mois précédent.

18.4 La résiliation de la Convention de plein droit

La Convention sera résiliée de plein droit en cas de résiliation du

contrat d'acceptation en paiement à distance sécurisé, du contrat d'acceptation en paiement à distance à sécurité optionnelle et progressive et/ou du contrat d'acceptation en paiement à distance « classique » par cartes « CB » ou agréées « CB » signé(s) par acte(s) séparé(s).

Par ailleurs, la résiliation de la Convention entraîne automatiquement la résiliation de tous les contrats d'acceptation conclus entre la Banque Populaire et le Client pour l'exécution de la présente Convention.

18.5 La résiliation de la Convention sans motif

Chacune des parties peut résilier à tout moment la présente convention. La résiliation deviendra effective au terme d'un délai de trois (3) mois à compter de l'envoi d'une lettre recommandée avec demande d'avis de réception.

19. Entrée en vigueur - élection de domicile - droit applicable - Règlement des litiges

La présente Convention entre en vigueur dès signature par les parties et souscription, par acte(s) séparé(s), du contrat d'acceptation en paiement à distance sécurisé, ou du contrat d'acceptation en paiement à distance à sécurité optionnelle et progressive et/ou du contrat d'acceptation en paiement à distance « classique » par cartes « CB » ou agréées « CB ».

La présente Convention est soumise au droit français.

Pour l'exécution de la présente Convention, il est fait élection de domicile, par la Banque Populaire et par le Client en leur siège social mentionné aux Conditions Particulières.

Pour le règlement de toute contestation ou de tout litige relatif à la présente Convention ou découlant de son exécution, il est fait expressément attribution de compétence au tribunal dans le ressort duquel est situé le siège social de la Banque Populaire.

BANQUE POPULAIRE
BOURGOGNE
FRANCHE-COMTÉ
www.bpbfc.banquepopulaire.fr

PAIEMENTEXPRESS

CONVENTION DE SERVICE PAIEMENT EXPRESS

CONDITIONS GENERALES

1 Définitions

Toutes les définitions insérées dans les Conditions Générales du contrat d'acceptation en paiement à distance sécurisé VADS sont applicables à la présente Convention.
Les définitions supplémentaires suivantes auront la signification qui suit :

Acheteur :
Désigne tout consommateur réalisant une opération de paiement par carte à distance auprès du Client, Accepteur

Service Paiement Express :
Désigne l'ensemble des traitements et fonctionnalités liés à l'encaissement des paiements en vente à distance et intégrés dans la Solution Paiement Express

Formulaire d'Inscription Client :
Désigne le document d'enregistrement et de paramétrage des conditions du Service Paiement Express souscrites par le Client auprès de la Banque Populaire. Il fait partie des Conditions Particulières de la présente convention.

Client :
Personne physique ou morale ayant souscrit au Service Paiement Express

Solution Paiement Express :
Désigne l'offre commerciale du Service Paiement Express

2 Objet de la convention de services

La Banque Populaire propose à ses clients associations et autres organismes sans but lucratif, entreprises (artisans, commerçants, entreprises exploitées sous forme libérale), Accepteurs, recevant des paiements à distance, une solution d'encaissement des ordres de paiement par carte donnés à distance à leur profit, ainsi qu'un ensemble de traitements et fonctionnalités associés, désignés sous le nom de "Service Paiement Express".

Les présentes Conditions Générales ont pour objet de définir les modalités techniques et juridiques selon lesquelles la Banque Populaire permet au Client de bénéficier de la Solution Paiement Express.

L'adhésion à la Solution Paiement Express est effectuée par la signature du Formulaire d'Inscription Client.
Par cette signature, le Client accepte les présentes Conditions Générales, souscrit à la Solution Paiement Express et, le cas échéant, aux services additionnels mentionnés dans son Formulaire d'Inscription Client, et s'engage à respecter les instructions du Kit documentaire visé à l'article 6 ci-après.

Le Formulaire d'Inscription Client et les présentes Conditions Générales constituent la présente convention, ci-après dénommée la "Convention".
Elle annule et remplace toute autre convention qui aurait pu être signée entre les Parties, relative à la Solution Paiement Express.

3 Présentation de la solution paiement express

La Solution Paiement Express requiert la signature d'un contrat d'acceptation en paiement à distance sécurisé VADS avec la Banque Populaire.

La Solution Paiement Express comprend :

- Le service d'envoi de Mail avec lien pour paiement
- La page de paiement
  - affichage des cours de change en devises (contre-valeur)
  - affichage des pages de paiement en multi-langues (9 langues) (1),
  - affichage dynamique pour les mobiles et les tablettes,
  - personnalisation du logo du Client,
  - prise en charge du protocole 3D-Secure.
- L'acceptation des moyens de paiement suivants
  - cartes bancaires CB, VISA, VISA Electron, MASTERCARD et MAESTRO,
  - cartes virtuelle e-Carte Bleue,
- L'outil de gestion de caisse
  - consultation des opérations de paiement,
  - suivi du fichier des remises bancaires,
  - possibilité de valider, consulter, annuler, modifier, rembourser une opération de paiement,
  - capacité d'exporter les transactions sous format XLS, XML ou CSV.
- Les typologies de paiement
  - paiement unitaire, immédiat ou différé.
- La sécurité de la Solution Paiement Express :
  - certification PCI-DSS,
  - accès sécurisé à l'outil de gestion de caisse par identifiant et mot de passe, renouvellement des mots de passe tous les trois (3) mois,
  - envoi des identifiants et mots de passe par email (avec saisie du code de première connexion obligatoire),
  - garantie des paiements dans les conditions du protocole 3D-Secure
    - affichage en temps réel de l'existence ou non de la garantie à partir de l'outil gestion de caisse,
    - restitution en différé de l'existence ou non de la garantie dans les journaux de transactions.

(1) Allemand, anglais, chinois, espagnol, italien, japonais, portugais et russe

Les services additionnels

Ces services sont optionnels et comprennent :

- **le formulaire hébergé :** site internet dédié à l'encaissement de paiement en ligne, développé, hébergé et administré par la Banque Populaire, et que le Client peut personnaliser.
- **le suivi client,**
- **l'acceptation des cartes privatives** [(2)] **:** American Express, Cofinoga, Cetelem, JCB,

[(2)] Liste non exhaustive, consultez votre conseiller Banque Populaire

4 Conditions des fonctions de la solution paiement express

4.1 Mail avec lien pour paiement

Le service Mail avec lien pour paiement permet au Client de transmettre à ses Acheteurs, sous sa seule responsabilité, des courriers électroniques ponctuels intégrant dans le corps des messages un lien URL pointant vers la page de paiement1 de Paiement Express, ou en cas d'option du service additionnel « formulaire hébergé », un lien URL pointant vers ledit formulaire.

Le Client transmet des messages électroniques afférents à un produit, un service, une cotisation, un règlement de facture ou une proposition contractuelle, quelle qu'en soit la nature, et permet à ses Acheteurs, destinataires de ce courrier électronique, de procéder éventuellement à un paiement par carte.

Le Client est seul responsable du respect des lois et règlements applicables aux ventes et prestations réalisées à distance, ainsi que celles applicables au commerce électronique. Il reconnaît qu'il doit se conformer à ces dispositions ou à celles qui pourront intervenir et, le cas échéant, se soumettre aux dispositions relatives aux dons et règlement de cotisations qui lui sont applicables.

4.1.1 Gestion du contenu de l'e-mail et envoi aux Acheteurs

Via l'OUTIL DE GESTION DE CAISSE, le Client peut paramétrer sous sa seule responsabilité les caractéristiques de l'ordre de paiement associé au lien URL inséré dans l'e-mail (durée, montant et devise), et modifier le texte par défaut proposé par le service Mail avec lien pour paiement.

Une fois ces étapes de paramétrages terminées, le Client peut procéder à l'envoi depuis le Service Paiement Express des e-mails de façon unitaire dans la limite de 100 adresses saisies depuis l'OUTIL DE GESTION DE CAISSE.

La Banque Populaire s'engage à insérer dans le courrier électronique rédigé par le Client, un lien URL pointant vers la page de paiement de Paiement Express, ou en cas d'option du service additionnel « formulaire hébergé », un lien URL pointant vers ledit formulaire, afin de permettre à tout Acheteur destinataire d'un message de donner éventuellement un ordre de paiement.

4.1.2 Licéité du contenu du message

Le Client est seul responsable des informations contenues dans ses messages adressés à ses Acheteurs.

En tant que diffuseur et non éditeur des messages, la Banque Populaire n'assurera aucun contrôle sur la licéité du contenu des messages du Client.

Le Client s'engage à ce que les messages émis respectent la réglementation en vigueur (respect des bonnes mœurs, de l'ordre public, interdiction de toute forme de manifestation discriminatoire).

Le Client s'engage également à respecter les droits de la personnalité et le droit de la propriété intellectuelle. Il déclare notamment posséder les droits de reproduction et de représentation de l'image des personnes et des œuvres intellectuelles, textes, éléments graphiques, artistiques, sonores présents dans les messages.
Par ailleurs, le Client s'engage aussi à respecter la législation propre au commerce, à la vente à distance, à la consommation et à la protection des données nominatives et à ne pas se recommander de la Banque Populaire auprès de ses Acheteurs.

4.1.3 Licéité de l'émission du message

Le Client est seul responsable des adresses électroniques utilisées dans le cadre du service Mail avec lien pour paiement.
À cet égard, il s'assure notamment que la personne à laquelle il adresse ce message, l'a expressément et préalablement autorisé à recevoir des courriers électroniques de cette nature et qu'elle a été dûment informée de ses droits.

Le Client s'engage à respecter l'ensemble de la réglementation relative à la prospection par courrier électronique et au Code des postes et télécommunications et plus particulièrement les dispositions de l'article L34-5 dudit code.

La Banque Populaire ne saurait être tenue pour responsable de toute communication ou de tout envoi d'un courrier électronique sans le consentement préalable et exprès du destinataire, des conséquences résultant d'un problème ou défaut d'acheminement des messages adressés par le Client à ses propres Acheteurs, dont la liste des adresses électroniques a été communiquée à la Banque Populaire dans le cadre du service Paiement par e-mail.

La Banque Populaire garantit au Client qu'elle ne fera aucun usage commercial des données et notamment des adresses électroniques transmises par le Client dans le cadre du service Mail avec lien pour paiement.

4.1.4 Responsabilités

Le Client s'engage à informer la Banque Populaire, par lettre recommandée avec accusé de réception de toute plainte, action en justice, réclamation exercée par tout tiers, directement ou indirectement, liées à la diffusion des messages du service Mail avec lien pour paiement.

Le Client s'engage à assurer à ses frais, la défense de la Banque Populaire dans le cas où cette dernière ferait objet d'une action en revendication relative aux données contenues dans les messages, et à prendre à sa charge l'indemnité due en réparation du préjudice éventuellement subi.

4.2 Paiement différé

Le Client a la possibilité de choisir le délai de rétention des paiements effectués via le Service Paiement Express avant remise en banque.

Le Client définit librement ce délai dans l'outil de gestion de caisse. Par défaut, le délai de remise en banque est paramétré au jour de l'opération de paiement.

4.3 Validation manuelle des paiements

Par défaut, l'envoi en remise des paiements dont la sécurisation est assurée par le Service Paiement Express est automatique.
Le Client a la possibilité de confirmer cet envoi en remise de façon manuelle.

Le Client signifie librement son choix (validation automatique ou manuelle) dans l'outil de gestion de caisse.

Dans le cas où le Client sélectionne "validation manuelle", chaque demande de paiement sécurisé en ligne effectuée par ses Acheteurs doit être validée à l'aide de la fonction "valider" présente dans l'outil de gestion de caisse.

La Banque Populaire ne pourra donc être tenue responsable par le Client ou par tout tiers, de la non réalisation d'un règlement consécutif à un défaut de validation en mode manuel ainsi que des conséquences qui pourraient en découler.

4.4 Affichage multi-devises

Ce service permet au Client de proposer à ses propres clients un paiement dans une devise autre que l'euro.
Le Client est informé que les paiements par carte dont la sécurisation est assurée par le Service Paiement Express s'effectuent selon les modalités prévues dans les accords conclus entre la Banque Populaire et les réseaux internationaux (ex : Visa, MasterCard …).

Aux termes de ces accords, la compensation des paiements réalisés dans une devise étrangère acceptée par lui via le service Mail avec lien pour paiement, se fera en euros, en application du taux de change en vigueur à la date de traitement de l'opération de paiement et appliqué par le réseau international dont la marque figure sur la carte utilisée pour le paiement.

Le produit de ce paiement sera imputé sur un compte dont la devise de tenue de compte est l'euro.

5 Conditions des services additionnels

5.1 Conditions relatives au service de formulaire hébergé

5.1.1 Accès au service

En préalable à la mise en ligne du formulaire hébergé, le Client devra :

- paramétrer son formulaire :
  - via l'outil de gestion de caisse :
    - texte introductif de présentation du client ou de son activité.
    - coordonnées (adresse, mail de contact, téléphone),
      - les champs à remplir par l'acheteur.
- puis demander à la Banque Populaire la mise en ligne du formulaire via l'outil de gestion de caisse

La Banque Populaire se réserve la possibilité de suspendre, sans délai et sans que sa responsabilité ne puisse être engagée de ce fait, l'accès au service de formulaire hébergé en cas de non-respect des obligations à la charge du Client, et notamment dans l'hypothèse où le Client intégrerait dans son formulaire des éléments de quelque nature que ce soit qui seraient contraires aux bonnes mœurs, à l'ordre public ou à la réglementation en vigueur.

5.1.2 Évolutions du service

Evolutions du fait du Client
Toute demande d'adaptation graphique du formulaire pour répondre aux exigences du Client, fera l'objet d'un devis spécifique de la part de la Banque Populaire, dès lors que cette demande est réalisable.

Evolutions du fait de la Banque Populaire
Dans le cadre de l'évolution du Service Formulaire Hébergé, le Client est informé que la Banque Populaire ou ses partenaires, se réservent le droit de modifier, à tout moment, les spécifications techniques et caractéristiques du Service Formulaire Hébergé ainsi que les Conditions générales, dans les conditions prévues à l'article 9 des présentes.

5.2 Suivi client

L'option « suivi client » permet d'apporter d'avantage de personnalisation du service de paiement vis-à-vis des Acheteurs. Pour chaque paiement validé, un e-mail de confirmation personnalisé au logo de la Banque Populaire est adressé en temps réel à l'acheteur pour l'informer du détail du paiement.

5.3 Acceptation des cartes privatives

Ce Service permet au Client de proposer aux acheteurs de payer par carte privative (telles que American Express, Aurore, Cofinoga,….) (3)

Pour cela, le Client doit avoir souscrit un contrat d'acceptation de carte privative avec chacun des émetteurs de cartes privatives de son choix.

6 Documentation du service paiement express

Dès réception du Formulaire d'Inscription Client composant les Conditions Particulières, la Banque Populaire adresse au Client un Kit documentaire.

Ce Kit documentaire est constitué des éléments suivants :

- Un manuel utilisateur "Ordre de paiement par email"
- Un manuel utilisateur de l'outil de gestion de caisse,
- Un descriptif des journaux de reporting,
- Un manuel utilisateur du formulaire de paiement hébergé (service additionnel).

Le Client s'engage à respecter les présentes Conditions Générales ainsi que les spécifications d'utilisation du Service Paiement Express telles que décrites dans la Documentation.

Le Client reconnaît disposer de la compétence nécessaire pour procéder aux vérifications et tests nécessaires tant lors de l'installation qu'au cours de l'utilisation du Service Paiement Express.

Pendant l'exécution du contrat, le Client reste gardien et seul responsable de ses matériels, logiciels, fichiers, programmes, informations ou bases de données.

(3) Liste non exhaustive consultez votre conseiller Banque Populaire

Le Client reconnaît que la Banque Populaire a satisfait à ses obligations de conseil et d'information concernant les caractéristiques essentielles et les modalités de fonctionnement de la Solution Paiement Express et/ou des services additionnels, eu égard aux besoins qu'il a exprimés.

7 Obligations du client relatives au service paiement express

7.1 Mise en garde et conditions d'adhésion

Il appartient au Client de s'assurer notamment de l'adéquation de la Solution Paiement Express à ses propres besoins et de la possibilité, ainsi que de l'opportunité pour lui d'utiliser ce service.
Le Client reconnaît avoir été informé des risques inhérents à l'utilisation des réseaux internet et particulièrement, en termes de :

- Défaut de sécurité et de confidentialité dans la transmission, dans la réception des instructions et/ou des informations sur les demandes de paiement sécurisé ;
- Performance dans la transmission des messages, d'informations sur la demande de paiement sécurisé et d'exécution d'instructions ;
- Mise à jour différée de l'ensemble des informations sur les demandes de paiement sécurisé effectuées.

Le Client est informé que pour bénéficier du Service Paiement Express, il doit :

- être titulaire d'un compte bancaire ouvert auprès de la Banque Populaire,
- avoir souscrit un contrat d'acceptation en paiement à distance par cartes bancaires CB ou agréées CB en cours de validité avec la Banque Populaire,
- le cas échéant, avoir souscrit auprès du réseau privatif concerné le contrat d'acceptation en paiement par carte nécessaire pour permettre à ses clients de payer avec une telle carte (ex : American Express …). La Banque Populaire décline toute responsabilité en cas de défaut de fourniture par le réseau privatif des identifiant et mot de passe correspondant au contrat souscrit, et en cas d'anomalie ou dysfonctionnement dans le traitement des ordres de paiement reçus dans le cadre dudit réseau privatif.

7.2 Sécurité

Le Client s'engage à mettre en œuvre et à faire mettre en œuvre les dispositifs (matériel, procédures...) permettant d'assurer la confidentialité et la sécurité des documents de spécifications techniques, les fichiers, les données, les éléments sécuritaires remis par la Banque Populaire dans le cadre de la présente Convention.

7.2.1 Confidentialité des identifiants du Client

La Banque Populaire propose au Client un accès sécurisé à l'outil de gestion de caisse.

Le Client s'engage à respecter et à faire respecter l'ensemble des obligations de sécurité, qui sont mises à sa charge, et notamment à conserver sous son contrôle exclusif et dans le respect des obligations de confidentialité à sa charge, les identifiant et mot de passe. Il s'engage également à modifier régulièrement son mot de passe.

Le Client est entièrement responsable de l'usage et de la conservation de son identifiant et de son mot de passe, ainsi que des conséquences d'une divulgation, même involontaire, à quiconque ou d'une usurpation. Toute utilisation des codes d'accès et mots de passe du Client sera réputée effectuée par ce dernier. L'identification et l'authentification du Client au moyen de l'utilisation de l'identifiant et mot de passe valent imputabilité des opérations effectuées au Client.

En cas de perte ou d'oubli, le Client peut demander l'attribution d'un nouvel identifiant et d'un nouveau mot de passe

7.2.2 Protection des fichiers et documents

Le Client se prémunira impérativement contre tous risques concernant les fichiers, programmes et autres documents confiés à la Banque Populaire en constituant un double de ceux-ci. Le Client se déclare à cet égard pleinement informé que les supports informatisés présentent une fragilité nécessitant, d'une part de vérifier la qualité et l'exhaustivité de ses sauvegardes, d'autre part de réaliser des sauvegardes multiples.
Le Client est informé qu'il fait son affaire de la conservation et de l'archivage des documents concernant sa clientèle et/ou son activité pendant la durée légale et/ou règlementaire fixée par les textes.

8 Disponibilité du service paiement express

Le Service Paiement Express est accessible tous les jours (7 jours/7), 24 heures sur 24, sous réserve des indisponibilités occasionnelles énoncées ci-dessous.

Le Service Paiement Express peut être momentanément inaccessible afin de réaliser des opérations d'actualisation, de sauvegarde ou de maintenance. Dans ces hypothèses, la Banque Populaire s'efforcera d'en informer le Client, dans un délai raisonnable, par courrier électronique avant toute intervention.

D'une manière générale, le Client reconnaît que la disponibilité du Service Paiement Express ne saurait s'entendre de manière absolue, et qu'un certain nombre de défaillances, de retards ou de défauts de performance peuvent intervenir indépendamment de la volonté de la Banque Populaire, compte tenu de la structure du réseau internet ou GSM et des spécificités liées au Service Paiement Express.

9 Modification et évolution du service paiement express

Il est expressément convenu entre les parties que la Banque Populaire se réserve le droit de modifier à tout moment, pour des raisons notamment techniques et/ou de sécurité, les présentes conditions générales relatives au Service Paiement Express. Elle en informera le Client par tous moyens.

Il est entendu entre les parties que toute modification des présentes conditions générales entrera en vigueur à la date précisée par la Banque Populaire dans le courrier de notification adressé au Client par tous moyens.

Seront joints à ce courrier les éléments d'information nécessaires pour l'exécution des mises à niveau.

Le Client disposera du délai stipulé dans le courrier de notification pour accepter ou résilier le Service Paiement Express dont les conditions auront été modifiées.

Si le Client n'effectue pas les dites mises à niveau dans les délais impartis, la responsabilité de la Banque Populaire ne saurait être recherchée en cas de dysfonctionnement du Service Paiement Express.

10 Assistance clients lors de l'exploitation du service paiement express

Le Client pourra faire appel à l'Assistance Clients en cas de problèmes survenus lors de l'exploitation du Service Paiement Express.

L'Assistance Clients est assurée par l'équipe Paiement Express du lundi au vendredi de 9h00 à 18h00.

Tél. : 0811.363.364 (numéro Azur – coût d'un appel local depuis un poste fixe)
E-mail : cyberplus.paiement@natixis.fr

L'Assistance Clients Paiement Express concerne toutes les demandes liées à la gestion courante des services et au fonctionnement ou utilisation des outils de la Solution Paiement Express.

Le Client pourra contacter l'Assistance Clients par messagerie électronique ou par téléphone pendant les heures d'ouverture du service, telles que ci-avant précisées.

Avant chaque appel téléphonique, il appartient au Client :
- de se reporter à la Documentation visée à l'article 6 des présentes Conditions Générales et de décrire de façon précise et exhaustive, les manifestations du problème rencontré aux fins d'en faciliter le diagnostic,
- d'adresser à la Banque Populaire la totalité des éléments demandés.

Le Client autorise la Banque Populaire à effectuer toutes les opérations de contrôle permettant de vérifier l'utilisation du Service Paiement Express conformément à la Documentation.

A partir des informations communiquées par le Client, la Banque Populaire procède au diagnostic et indique au Client, par téléphone ou par courrier électronique, la procédure à suivre pour pallier les problèmes rencontrés par ce dernier.

11 Respect de la législation en vigueur

Le Client s'engage à respecter la législation et les réglementations en vigueur, en particulier, à ne pas diffuser des informations contraires aux bonnes mœurs, à l'ordre public, aux droits et à la réputation de tiers, à la dignité humaine

Le Client reconnaît à ce titre qu'il a l'entière et pleine responsabilité de la licéité des contenus qu'il diffuse dans le cadre de l'utilisation de la Solution Paiement Express et du Service Paiement Express. Par conséquent, il garantit notamment que les contenus :
- ne portent pas atteinte à la vie privée de tiers
- ne pas portent pas atteinte aux droits de propriété intellectuelle de tiers
- n'incitent pas à la réalisation de crimes et délits
- ne font aucune discrimination
- ne provoquent pas la haine ou la violence en raison de la race, de l'ethnie ou de la nation,
- ne transmettent pas de fausses informations
- ne sont pas diffamatoires, injurieux, offensants et/ou outrageants
- ne pas portent pas atteinte au droit à l'image des personnes
- ne portent pas atteinte à l'image ni ne dénigrent les produits ou services offerts par des tiers
- ne contiennent pas d'informations fausses de nature à causer un préjudice à des tiers en influençant leur comportement
- ne sont pas obscènes, vulgaires, pornographiques ou indécents,
- ne constituent pas ou n'encouragent pas des comportements susceptibles de constituer un délit,

La Banque Populaire ne pourra être tenue responsable de toute infraction à la législation et réglementations précitées. Le Client garantit la Banque Populaire qu'il détient l'ensemble des droits d'auteur sur les contenus qu'il diffuse dans le cadre de l'utilisation du Service Paiement Express et de la Solution Paiement Express.

Le client garantit la Banque Populaire contre tous recours et/ou actions que pourraient former à un titre quelconque, des tiers sur tout ou partie des contenus diffusés par le Client.

Le Client s'engage, sous les mêmes conditions, à adhérer aux bons usages de la profession de la vente à distance et à les mettre en œuvre, à respecter les règles du commerce concernant la vente en général et de la vente à distance en particulier, ainsi que la législation notamment sur les devises, les taxes, les publications.

De même le Client garantit que les produits et services qu'il délivre sont conformes à l'activité qu'il a initialement déclarée à la Banque Populaire lors de son adhésion au Service Paiement Express. A cet égard, le Client s'engage à informer sans délai la Banque Populaire de tout changement d'activité.

Le Client s'engage à ne pas mettre en œuvre une activité de galerie marchande virtuelle multi-sites ou de prestation de paiement centralisée sans l'accord écrit de la Banque Populaire.
Le Client garantit qu'il ne conservera, ni ne stockera, de manière informatique ou manuelle, les références bancaires des Acheteurs (numéro de la carte bancaire, numéro de compte bancaire,…) auxquelles il aurait eu accès, dans le cadre de l'utilisation du Service Paiement Express.

Toutefois, si le Client conserve les numéros de cartes bancaires des Acheteurs dans un fichier ayant pour finalité de lutter contre la fraude au paiement, celui-ci garantit la Banque Populaire qu'il a déclaré au préalable ce fichier ainsi que sa durée de conservation auprès de la Commission nationale de l'informatique et des libertés et qu'il a informé clairement les Acheteurs de l'existence et de la finalité d'un tel traitement afin que ces derniers puissent s'y opposer et ce, conformément aux dispositions de la Loi Informatique et Libertés.

Le Client déclare détenir le droit d'usage et de diffusion des éléments (textes, éléments graphiques ...) qu'il utilise, et ne pas porter atteinte à un quelconque droit de propriété intellectuelle ou droit de la personnalité.

12 Droit de propriété intellectuelle

La Banque Populaire conserve, en tant que titulaire des droits, la propriété intellectuelle des documents techniques et plus généralement de tous les éléments remis au Client, ainsi que toutes les prérogatives s'y rattachant. Le Client n'acquiert par le Contrat Paiement Express aucun droit de propriété intellectuelle mais un simple droit d'utilisation personnel, non transférable et non exclusif pour la durée des présentes.

Le Client s'engage à ne pas modifier ou faire modifier les documents techniques ou les éléments remis, à ne pas les utiliser pour un autre usage que celui prévu par le Contrat Paiement Express, à respecter la documentation de service fournie par la Banque Populaire et à informer immédiatement cette-dernière en cas de dysfonctionnement.

Il s'oblige aussi à ne pas dupliquer ou faire dupliquer la documentation technique ou les éléments reçus pour une autre raison que celle des tests d'évaluation et dans ce cas, à détruire les copies dupliquées et à retourner l'ensemble de la documentation Paiement Express dès la fin des tests.

La Banque Populaire demeure propriétaire des procédés, moyens, méthodes et savoir-faire qu'elle met en œuvre pour exécuter ses prestations.

13 Confidentialité – secret bancaire

13.1 Le Client s'engage à garder le secret le plus absolu notamment sur les méthodes utilisées par la Banque Populaire et dont il pourrait avoir connaissance dans le cadre de l'exécution de la présente Convention Paiement Express. A ce titre, il s'engage notamment à ne transférer ou mettre à la disposition ou à la connaissance d'aucun tiers autre qu'un sous-traitant et dans la stricte limite nécessaire à la transmission des ordres de paiement vers le Service Paiement Express, et sous aucun prétexte, la Documentation technique visée à l'article 6 ci-avant, manuels utilisateurs, matériels ou droits dont il pourrait bénéficier ou avoir l'usage.

En cas de sous-traitance, le Client s'engage à imposer à ses sous-traitants le respect de la confidentialité des méthodes et Documentation technique précitées de la Banque Populaire relative à la présente Convention.

Il s'oblige en outre à informer sans délai la Banque Populaire de toute éventualité divulgation du secret.

13.2 Les documents ou renseignements fournis par le Client, ainsi que les états, études et documents provenant de leur traitement sont couverts par le secret bancaire. En particulier, aucune communication ne pourra être effectuée à des tiers, sauf dispositions légales l'y autorisant ou autorisation expresse du Client.

La Banque Populaire s'oblige à respecter de façon absolue cette obligation au secret et à la faire respecter de la meilleure façon par son personnel, ses sous-traitants, ou prestataires de services. Pour l'application de cette disposition, il est précisé que conformément aux dispositions de l'article L.511-33,6° du Code monétaire et financier, des informations confidentielles pourront être communiquées à toute personne devant intervenir ou accéder aux fichiers et en particulier les conseils ou sous-traitants de la Banque Populaire.

13.3 L'obligation de confidentialité continuera à lier les parties et leurs ayants droit, pendant toute la durée de la Convention de service et pendant cinq (5) ans après sa résiliation ou son expiration. Le présent article survivra à la résiliation ou à l'expiration de la Convention pour quelque cause que ce soit.

14 Conditions financières - facturation et règlement

14.1 Les conditions financières du Service Paiement Express sont indiquées dans le Formulaire d'Inscription Commerçant spécifique à la Solution Paiement Express.

Sauf dispositions contraires, figurant dans le Formulaire d'Inscription Commerçant spécifique à la Solution Paiement Express, les factures de la Banque Populaire sont payables sans escompte dès réception.

14.2 Dans le cas où une facture ne serait pas réglée dans les trente (30) jours de son envoi par la Banque Populaire au Client, la Banque Populaire aura la faculté de suspendre l'exécution des prestations prévues par la présente Convention de service, jusqu'au règlement de la facture en souffrance, et sans que cette suspension puisse être considérée comme une inexécution de ses obligations contractuelles, ou comme une résiliation de Contrat Paiement Express de son fait ou n'ouvre un quelconque droit à indemnisation pour le Client.

Tout mois commencé sera entièrement dû.

14.3 En outre, à compter du trente et unième jour, la somme due portera intérêt au taux de trois (3) fois le taux d'intérêt légal sans qu'une mise en demeure préalable soit nécessaire, même par simple lettre, l'intérêt étant dû et exigible par le seul fait de l'échéance du terme contractuel.

15 Responsabilité de la banque populaire

La Banque Populaire garantit ses prestations dans les conditions ci-dessous précisées :

15.1 Le Service est conforme aux spécifications de la documentation technique. La Banque Populaire ne saurait toutefois être tenue pour responsable des dysfonctionnements du Service Paiement Express ayant pour origine l'intervention du Client ou de tiers, tels que notamment le fournisseur d'accès Internet (FAI) ou l'opérateur Télécom (par exemple, accès momentanément indisponible, lenteur ou retard dans l'affichage des pages HTML).

15.2 La Banque Populaire ne répond ni des dommages indirects tels que notamment manque à gagner, perte financière, perte de clientèle, perte de bénéfices ou d'économies escomptées, trouvant leur origine ou étant la conséquence de la Convention de service, ni des dommages causés à des personnes ou des biens distincts de l'objet de la présente Convention de service.

15.3 La responsabilité de la Banque Populaire ne pourra également être engagée en cas d'usage impropre du Service Paiement Express, par l'Acheteur, le Client ou tout tiers non autorisé.

15.4 De même, la responsabilité de la Banque Populaire ne pourra être engagée en raison des conséquences susceptibles de découler d'un usage frauduleux ou abusif de l'identifiant et du mot de passe.

15.5 La Banque Populaire ne saurait être tenue pour responsable des difficultés liées à une mauvaise utilisation du Service Paiement Express et de la Documentation visée à l'article 6 des présentes Conditions Générales.

15.6 La Banque Populaire ne saurait être tenue pour responsable des difficultés d'accès au Service Paiement Express en raison de la saturation et de la complexité du réseau internet.

16 Divers

16.1 En cas de difficulté d'interprétation ou de contradiction entre les titres des articles et le texte de leur contenu, le contenu des articles primera sur leur titre.

16.2 Les dispositions de la présente Convention prévalent sur toute proposition ou accord antérieur, ainsi que sur toute autre communication antérieure entre les parties ayant trait au Service Paiement Express.

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

16.4 Aucune des deux parties ne sera tenue pour responsable vis-à-vis de l'autre de l'inexécution ou des retards dans l'exécution

de la présente Convention du fait de la survenance d'un cas de force majeure ou d'évènements tels que l'intervention des autorités civiles ou militaires, l'interruption totale ou partielle des réseaux de communications, le refus de licence d'importation, les incendies, les grèves, les conflits sociaux, les dysfonctionnements de matériels ou toute autre cause qui serait raisonnablement hors de son contrôle.

17. Durée - suspension et résiliation du contrat

17.1 Durée de la Convention

La présente Convention est conclue pour une durée indéterminée.

17.2 La suspension de la Convention

La Banque Populaire pourra suspendre l'exécution de la présente Convention sans que cette suspension soit constitutive d'une résiliation ou d'un manquement à l'une de ses propres obligations, dans les cas suivants :

- dans le cas où le Client ne remplirait pas les obligations mises à sa charge (fourniture de données, accès aux renseignements, sécurité des modes d'accès etc...) nécessaires à la bonne exécution de la présente Convention, Cette suspension pourra ainsi intervenir en cas de retard de paiement tel que prévu à l'article 14.2 de la présente Convention
- dans le cas où le contrat d'acceptation en paiement à distance sécurisé, par cartes « CB » ou agréées « CB » signés par acte séparé ferait l'objet d'une suspension.

La suspension sera notifiée au Client par lettre recommandée avec accusé de réception indiquant les motifs de la suspension. L'exécution reprendra une fois que les motifs à l'origine de cette suspension auront disparu, compte tenu des modifications de prix et de délais encourus de ce fait.

17.3 La résiliation de la Convention pour manquement

En cas de manquement par l'une quelconque des parties, aux obligations dont elle a la charge au titre des présentes, et auquel il n'aurait pas été remédié dans un délai de huit (8) jours à compter de l'envoi d'une lettre recommandée avec demande d'avis de réception, l'autre partie pourra, prononcer de plein droit la résiliation de la présente Convention. En pareil cas, la Banque Populaire, lorsqu'elle prononce la résiliation, aura droit au paiement des prestations exécutées et non facturées,

17.4 La résiliation de la Convention de plein droit

La Convention sera résiliée de plein droit en cas de résiliation du contrat d'acceptation en paiement à distance sécurisé par cartes "CB" ou agréées "CB", signé(s) par acte(s) séparé(s).

17.5 La résiliation de la Convention sans motif

Chacune des parties peut résilier à tout moment la présente convention. La résiliation deviendra effective au terme d'un délai de trois (3) mois à compter de l'envoi d'une lettre recommandée avec demande d'avis de réception.

18 Entrée en vigueur - élection de domicile - droit applicable - règlement des litiges

La présente Convention entre en vigueur dès signature par les parties

La présente Convention est soumise au droit français.

Pour l'exécution de la présente Convention, il est fait élection de domicile, par la Banque Populaire et par le Client en leur siège social mentionné aux Conditions Particulières.

Pour le règlement de toute contestation ou de tout litige relatif à la présente Convention ou découlant de son exécution, il est fait expressément attribution de compétence au tribunal dans le ressort duquel est situé le siège social de la Banque Populaire.

ANNEXE 1

REFERENTIEL SECURITAIRE ACCEPTEUR

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

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

Pour assurer la sécurité des données des transactions et notamment, des données des Titulaires de Cartes, une organisation, des procédures et des responsabilités doivent être établies.
En particulier, un responsable de la sécurité du système commercial et de paiement doit être désigné. Il est chargé, entre autres, d'appliquer la législation sur la protection des données nominatives et des données bancaires dans le cadre de leur utilisation et de leur environnement.
Les détenteurs de droits d'usage des informations et du système doivent être identifiés et sont responsables de l'attribution des droits d'accès au système.
Le contrôle du respect des exigences de sécurité relatives au système commercial et de paiement doit être assuré.
Une organisation chargée du traitement des incidents de sécurité, de leur suivi et de leur historisation doit être établie.

Exigence 2 (E2) : Gérer l'activité humaine et interne

Les obligations et les responsabilités du Personnel 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.
Les personnels doivent être sensibilisés aux risques encourus, notamment sur la divulgation d'informations confidentielles, l'accès non autorisé aux informations, aux supports et aux documents.
Les personnels doivent être régulièrement sensibilisés aux risques particuliers liés à l'usage des moyens informatiques (postes de travail en réseau, serveurs, accès depuis ou vers Internet), et notamment à l'introduction de virus.

Il convient que les personnels reçoivent une formation appropriée sur l'utilisation correcte du système d'exploitation et du système applicatif commercial et de paiement.

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

Tout dispositif (équipement réseau, serveur, …) qui stocke ou qui traite des données relatives à une transaction, et notamment des données du porteur, doit être hébergé dans un local sécurisé et répondre aux exigences édictées par les 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 de paiement

Les règles de sécurité relatives aux accès et sorties depuis et vers le système commercial et de paiement doivent être établies et leur respect doit être contrôlé.
Le serveur de base de données client ainsi que le serveur hébergeant le système de paiement ne doivent être accessibles de l'extérieur que par le serveur commercial FrontOffice et seulement par l'intermédiaire d'un pare-feu.
Les accès internes des utilisateurs comme des administrateurs à ces mêmes serveurs doivent se faire par l'intermédiaire du pare-feu.
L'architecture réseau doit être organisée de manière à ce que les règles de sécurité définies soient mises en œuvre et contrôlées.
Le pare-feu doit être mis à jour systématiquement lorsque des vulnérabilités sont identifiées sur ses logiciels (logiciel pare-feu et logiciel d'exploitation) et corrigeables.
Le serveur supportant le pare-feu doit être doté d'un outil de contrôle de l'intégrité.
Le pare-feu doit assurer l'enregistrement des accès et des tentatives d'accès dans un journal d'audit. Celui-ci doit être analysé quotidiennement.

Exigence 5 (E5) : Contrôler l'accès au système commercial et de paiement

Le principe d'autorisation d'utilisation du système doit être défini et reposer sur la notion d'accès des classes d'utilisateurs aux classes de ressources : définition des profils d'utilisateurs et des droits accordés.
Les responsabilités et rôles quant à l'attribution, l'utilisation et le contrôle doivent être identifiés. Notamment, les profils, les droits et les privilèges associés doivent être validés par les propriétaires des informations et du système d'encaissement.
Les droits des utilisateurs et des administrateurs ainsi que leurs privilèges, doivent être gérés et mis à jour conformément à la politique de gestion des droits.

Exigence 6 (E6) : Gérer les accès autorisés au système commercial et de paiement

Aucune ouverture de droits ne peut se faire en dehors des procédures d'autorisation adéquates. Les autorisations données doivent être archivées et contrôlées régulièrement.
Outre les accès clients, tout accès au système commercial et de paiement doit se faire sur la base d'une identification et d'une authentification.
L'identification doit être nominative y compris pour les administrateurs et les personnels de maintenance. Les droits accordés à ceux-ci doivent être restreints aux opérations qui leur sont autorisées.
L'utilisation de codes d'identification attribués à des groupes ou des fonctions (process techniques comme l'alimentation automatique des signatures antivirales) n'est autorisée que si elle est appropriée au travail effectué.
Les changements de situation (changement de poste, départ, …) des personnels doivent systématiquement entraîner un contrôle des droits d'accès attribués.
La suppression des droits d'accès doit être immédiate en cas de départ d'une personne.
Le contrôle d'accès doit être assuré au niveau réseau par le pare-feu, au niveau système par les systèmes d'exploitation des machines accédées et au niveau applicatif par le logiciel applicatif et par le gestionnaire de base de données.
Les tentatives d'accès doivent être limitées en nombre.
Les mots de passe doivent être changés régulièrement.
Les mots de passe doivent comporter au minimum 8 caractères dont des caractères spéciaux.

Exigence 7 (E7) : Surveiller les accès au système commercial et de paiement

Les accès et tentatives d'accès au système doivent être enregistrés dans des journaux d'audit.
L'enregistrement doit comporter au minimum la date et l'heure de l'accès (ou tentative) et l'identification de l'acteur et de la machine.
Les opérations privilégiées comme la modification des configurations, la modification des règles de sécurité, l'utilisation d'un compte administrateur

doivent également être enregistrées.
Les systèmes assurant l'enregistrement doivent au minimum être le pare-feu, le système supportant la base de données Clients ainsi que celui supportant la base de données Paiements.
Les journaux d'audit doivent être protégés contre des risques de désactivation, modification ou suppression non autorisées.
Les responsabilités et rôles quant à l'audit des données enregistrées sont identifiés. Celui-ci doit être effectué quotidiennement.

Exigence 8 (E8) : Contrôler l'introduction de logiciels pernicieux

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

Exigence 9 (E9) : Appliquer les correctifs de sécurité (patches de sécurité) sur les logiciels d'exploitation

Les correctifs de sécurité doivent être systématiquement appliqués sur les équipements de sécurité et les serveurs applicatifs frontaux pour fixer le code lorsque des vulnérabilités pourraient permettre des accès non autorisés et non visibles.
Ces correctifs doivent être appliqués sur la base d'une procédure formelle et contrôlée.

Exigence 10 (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 de paiement

Il convient d'établir les responsabilités et les procédures concernant les modifications opérationnelles touchant aux applications.
Les modifications apportées aux logiciels applicatifs doivent faire l'objet d'une définition précise.

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

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

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

Exigence 13 (E13) : Maintenir l'intégrité des informations relatives au système commercial et de paiement

La protection et l'intégrité des éléments de la transaction doivent être assurées lors de leur stockage et lors de leur routage sur les réseaux (internes ou externes). Il en est de même pour les éléments secrets servant à chiffrer ces éléments.
Le dossier de sécurité propre au système commercial et de paiement doit décrire les moyens mis en place pour répondre à cette exigence.

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

Les données du porteur ne peuvent être utilisées que pour exécuter l'ordre de paiement et les réclamations. Le cryptogramme visuel d'un porteur ne doit en aucun cas être stocké par le commerçant.
Les données bancaires et nominatives relatives à une transaction, et notamment les données du porteur doivent être protégées lors de leur stockage et lors de leur routage sur les réseaux internes et externes au site d'hébergement conformément aux recommandations de la CNIL. Il en est de même pour l'authentifiant du commerçant et les éléments secrets servant à chiffrer.
Le dossier de sécurité propre au système commercial et de paiement doit décrire les moyens mis en place pour répondre à cette exigence.

Exigence 15 (E15) : Protéger la confidentialité des identifiants – authentifiants des utilisateurs et des administrateurs

La confidentialité des identifiants - authentifiants doit être préservée lors de leur stockage et de leur circulation.
Il convient de s'assurer que les données d'authentification des administrateurs ne puissent être réutilisées. Dans le cadre d'une intervention extérieure pour maintenance, les mots de passe utilisés doivent être systématiquement changés à la suite de l'intervention.

ANNEXE 2

PRESENTATION GENERALE DES REGLES PCI-DSS

Les exigences constituant le Référentiel Sécuritaire PCI-DSS sont organisées autour d'un ensemble de 12 familles d'exigences regroupant 250 règles réparties en six grands domaines présentés ci-après :

Article 1 - Mettre en place et gérer un réseau sécurisé

1ère exigence : Installer et gérer une configuration de pare-feu afin de protéger les données des titulaires des Cartes.

2e exigence : Ne pas utiliser les paramètres par défaut du fournisseur pour les mots de passe et les autres paramètres de sécurité du système.

Article 2 - Protéger les données des titulaires de Cartes

3e exigence : Protéger les données des titulaires de Cartes stockées.

4e exigence : Crypter la transmission des données des titulaires de Cartes sur les réseaux publics ouverts.

Article 3 - Disposer d'un programme de gestion de la vulnérabilité

5e exigence : Utiliser et mettre à jour régulièrement un logiciel antivirus.

6e exigence : Développer et gérer des applications et systèmes sécurisés.

Article 4 - Mettre en œuvre des mesures de contrôle d'accès efficaces

7e exigence : Limiter l'accès aux données des titulaires de Cartes aux cas de nécessité professionnelle absolue.

8e exigence : Attribuer une identité d'utilisateur unique à chaque personne disposant d'un accès informatique.

9e exigence : Limiter l'accès physique aux données des titulaires de Cartes.

Article 5 - Surveiller et tester régulièrement les réseaux

10e exigence : Suivre et surveiller tous les accès aux ressources du réseau et aux données des titulaires de Cartes.

11e exigence : Tester régulièrement les systèmes et procédures de sécurité.

Article 6 - Disposer d'une politique en matière de sécurité de l'information

12e exigence : Disposer d'une politique régissant la sécurité de l'information

BANQUE POPULAIRE
BOURGOGNE
FRANCHE-COMTÉ
www.bpbfc.banquepopulaire.fr

ANNEXE 3

TABLEAU DES INTERCHANGES ET SCHEME FEES

Canal d'acquisition	Schéma de paiement de la transaction	Marque de la transaction	Catégorie de carte ayant réalisé la transaction	Interchange depuis le 08 Déc. 2016	Scheme Fee moyen du schéma de paiement de la transaction
Paiement de proximité	CB	CB	Carte de débit/universelle	0,20%	0,00122 €
			Carte de crédit	0,30%	0,00122 €
			Carte commerciale	0,90%	0,00122 €
			Cartes hors UE *		
	VISA	VISA	Carte de débit UE	0,20%	0,0100%
			Carte de crédit UE	0,30%	0,0140%
			Carte commerciale UE / Business DD	1,30%	0,0140%
			Carte commerciale UE / Corporate DD	1,35%	0,0140%
			Carte non régulée UE		
			Cartes de débit hors UE * particulier	1,60%	0,4600%
			Cartes de crédit hors UE * particulier	1,60%	0,4640%
			Cartes de débit hors UE * commerciale	2,00%	0,4600%
			Cartes de crédit hors UE * commerciale	2,00%	0,4640%
		VISA ELECTRON	Carte de débit UE	0,20%	0,0100%
			Carte de crédit UE	0,30%	0,0140%
			Carte commerciale UE	1,35%	0,0140%
			Carte non régulée UE		
			Cartes de débit hors UE * particulier	1,60%	0,4600%
			Cartes de crédit hors UE * particulier	1,60%	0,4640%
			Cartes de débit hors UE * commerciale	2,00%	0,4600%
			Cartes de crédit hors UE * commerciale	2,00%	0,4640%
		VPAY	Carte de débit UE	0,15 €	0,0100%
			Carte non régulée UE		
	MASTERCARD	MASTERCARD	Carte de débit UE	0,20%	0,0164%
			Carte de crédit UE	0,30%	0,0164%
			Carte commerciale UE / Business	1,65%	0,0164%
			Carte commerciale UE / Corporate	1,90%	0,0164%
			Carte non régulée UE		
			Cartes hors UE * particulier	1,60%	0,2627%
			Cartes hors UE * commerciale	2,00%	0,2627%
		MAESTRO	Carte de débit	0,20%	0,0164%
			Carte non régulée UE		

			Cartes hors UE * particulier	1,60%	0,2627%
			Cartes hors UE * commerciale	2,00%	0,2627%
	DFS	DFS	Carte de débit UE (Diners' Club)	0,20%	0,15%
			Carte de crédit UE (Diners'Club)	0,30%	0,15%
			Carte Commerciale	1,75%	0,15%
			Carte hors UE *	1,50%	0,15%
	UP	UP	Carte de débit UE		
			Carte de crédit UE		
			Carte hors UE *	1,20%	
E-commerce	CB	CB	Carte de débit/universelle	0,20%	0,00122 €
			Carte de crédit	0,30%	0,00122 €
			Carte commerciale	0,90%	0,00122 €
			Carte non régulée		
			Cartes hors UE *		
	VISA	VISA	Carte de débit UE	0,20%	0,020%
			Carte de crédit UE	0,30%	0,024%
			Carte commerciale UE / Business DD	1,30%	0,024%
			Carte commerciale UE / Corporate DD	1,35%	0,024%
			Carte non régulée UE		
			Cartes de débit hors UE * particulier	1,60%	0,5600%
			Cartes de crédit hors UE * particulier	1,60%	0,5640%
			Cartes de débit hors UE * commerciale	2,00%	0,5600%
			Cartes de crédit hors UE * commerciale	2,00%	0,5640%
		VISA ELECTRON	Carte de débit	0,20%	0,020%
			Carte de crédit UE	0,30%	0,024%
			Carte commerciale	1,35%	0,024%
			Carte non régulée UE		
			Cartes de débit hors UE * particulier	1,60%	0,5600%
			Cartes de crédit hors UE * particulier	1,60%	0,5640%
			Cartes de débit hors UE * commerciale	2,00%	0,5600%
			Cartes de crédit hors UE * commerciale	2,00%	0,5640%
		VPAY	Carte de débit UE	0,15 €	0,020%
			Carte non régulée UE		
	MASTERCARD	MASTERCARD	Carte de débit	0,20%	0,0164%
			Carte de crédit UE	0,30%	0,0164%
			Carte commerciale UE / Business	1,65%	0,0164%
			Carte commerciale UE/ Corporate	1,90%	0,0164%
			Carte non régulée UE		
			Cartes hors UE * particulier	1,60%	0,2627%

			Cartes hors UE * commerciale	2,00%	0,2627%
		MAESTRO	Carte de débit	0,20%	0,0164%
			Carte non régulée UE		
			Cartes hors UE * particulier	1,60%	0,2627%
			Cartes hors UE * commerciale	2,00%	0,2627%

* Hors UE, les interchanges restent inchangés (non impactés par le Règlement) ; les taux indiqués ici sont des taux moyens constatés