CONDITIONS GENERALES D'ACCEPTATION EN PAIEMENT PAR CARTES DE PAIEMENT SUR AUTOMATE EN LIBRE-SERVICE

PARTIE 1 CONDITIONS GENERALES COMMUNES A TOUS LES SCHEMAS

ARTICLE 1 - DEFINITIONS

1) L'»Accepteur» peut être tout commerçant, tout prestataire de services, toute personne exerçant une profession libérale, et d'une manière générale, tout professionnel vendant ou louant des biens ou des prestations de services, ou toute entité dûment habilitée à recevoir des dons ou percevoir des cotisations, susceptible d'utiliser un Système d'Acceptation reconnu par le(s) Schéma(s) dûment convenu(s) avec l'Acquéreur.

2) Par «Marque», il faut entendre tout nom, terme, sigle, symbole (matériel ou numérique) ou la combinaison de ces éléments susceptible de désigner le Schéma.
Les Marques pouvant être acceptées entrant dans le champ d'application du présent Contrat sont visées en partie 2.

3) Par «Acquéreur» il faut entendre tout établissement de crédit ou de paiement habilité à organiser l'acceptation des Cartes portant la(les) Marque(s) du(des) Schéma(s) visé(s) en Partie 2 du présent Contrat].

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

5) Par « Equipement Electronique «, il faut entendre tout dispositif de paiement capable de lire la Carte équipée d'une puce au standard EMV ou d'une piste magnétique permettant l'authentification du titulaire de la Carte. L'Equipement Electronique est soit agréé soit approuvé par l'entité responsable de chacun des Schémas dont les Cartes sont acceptées sur cet équipement.
L'agrément ou l'approbation de l'Equipement Electronique est une attestation de conformité avec des spécifications techniques et fonctionnelles définies par chaque Schéma concerné, qui dispose de la liste des Equipements Electroniques agréés ou approuvés.

6) Par «Automate de paiement en libre-service», il faut entendre tout Equipement Electronique acceptant les Marques figurant sur les Carte acceptées par l'Accepteur pour la distribution automatique de biens et services ou la location de bien, acceptant le paiement par Carte en libre-service, impliquant la présence du Titulaire de la Carte au point d'acceptation et sans intervention directe de l'Accepteur.
Ces automates sont désignés ci-après par le terme générique «Automate».

7) Par « Règlement », il faut entendre le Règlement UE n°2015/751 du 29 avril 2015.

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

9) Par « Carte «, on entend un instrument de paiement qui permet au payeur d'initier une opération de paiement. Elle porte une ou plusieurs Marques.
Lorsque la Carte est émise dans l'Espace Economique Européen (ci-après l'»EEE» - Il comprend les Etats membres de l'Union Européenne, l'Islande, le Liechtenstein et la Norvège), elle porte au moins l'une des mentions suivantes :
- crédit ou carte de crédit
- débit,
- prépayé,
- commercial,

ou l'équivalent dans une langue étrangère.

10) Par « Instrument de paiement « sans contact », il faut entendre un instrument de paiement disposant de la technologie « sans contact » constitué d'un logiciel de paiement mobile en mode «sans contact » intégré pour partie dans l'élément sécurisé d'un téléphone mobile, pour partie dans le téléphone mobile lui-même, et permettant de réaliser des opérations de paiement quelle qu'en soit la Marque.

11) Par « Schéma «, il faut entendre un ensemble de règles régissant l'exécution d'opérations de paiement liées à une carte tel que défini à l'article 2 du Règlement.
Les Schémas Visa / MasterCard / CB reposent sur l'utilisation de Cartes Visa / MasterCard / CB auprès des Accepteurs acceptant les Marques desdits Schémas, et cela dans le cadre des seules dispositions et procédures définies ou homologuées par lesdits Schémas.

12) Par « Point d'acceptation », on entend le lieu physique où est initié l'ordre de paiement.

13) Par « Contrat « ou « Contrat d'acceptation en paiement de par cartes de paiement sur automate en libre-service », il faut entendre ensemble les Conditions Générales communes à tous les Schémas (partie 1), les dispositions spécifiques à chaque Schéma (partie 2) et les conditions particulières d'acceptation en paiement par cartes de paiement sur automate en libre-service (aussi appelées « Conditions Particulières »).

14) Par « Parties », il faut entendre l'Acquéreur et l'Accepteur.

ARTICLE 2 - OBLIGATIONS DE L'ACCEPTEUR

L'Accepteur s'engage à :

2.1 Afficher visiblement chaque Marque qu'il accepte notamment en apposant de façon apparente à l'extérieur et à l'intérieur de son Point d'acceptation des panonceaux, vitrophanies et enseignes qui lui sont fournis par l'Acquéreur ou le Schéma.
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 qu'en soit la Catégorie de carte.

2.2 Afficher visiblement chaque Catégorie de carte qu'il accepte ou refuse de façon apparente à l'extérieur et à l'intérieur de son Point d'acceptation.

2.3 Afficher visiblement le montant maximum au-delà duquel aucune opération de paiement ne peut être réalisée ainsi que le montant minimum éventuel à partir duquel la Carte ou la Catégorie de carte est acceptée afin que le titulaire de la Carte en soit préalablement informé. Ce montant minimum doit être raisonnable et ne pas être un frein à l'acceptation des Cartes.

2.4 Informer clairement les Titulaires de Cartes des procédures et conditions avec lesquelles ils peuvent utiliser leur Carte pour régler le prix soit de leurs achats de biens ou de prestations de services, soit de leur location de biens.

2.5 En cas de présence de plusieurs Marques sur la Carte, respecter la Marque choisie par le titulaire de la Carte pour donner l'ordre de paiement.

2.6 Respecter les obligations légales, réglementaires et fiscales applicables à son secteur et sa zone d'activité, les dispositions professionnelles ainsi que les bonnes pratiques applicables aux ventes et prestations réalisées sur automate (notamment la mise à disposition des conditions générales de vente à ses acheteurs par tout moyen adapté).

2.7 Afin que le titulaire de la Carte n'ait pas de difficulté à vérifier et identifier les opérations de paiement qu'il a effectuées, vérifier avec l'Acquéreur la conformité des informations transmises pour identifier son Point d'acceptation. Les informations doivent indiquer une dénomination commerciale connue du titulaire de la Carte dans ce Point d'acceptation.

2.8 Accepter les paiements (à l'exclusion de toute délivrance d'espèces ou de tout titre convertible en espèces pour leur valeur faciale) effectués avec les Cartes portant la(les) Marque(s) et Catégorie(s) de carte qu'il a choisi d'accepter ou qu'il doit accepter dont les règles de fonctionnement sont définies en Partie 2 du présent contrat.

2.9 Ne recevoir des paiements qu'en contrepartie d'actes de vente ou de prestations de services offerts à sa clientèle et qu'il fournit ou réalise lui-même.

2.10 Transmettre les enregistrements des opérations de paiement à l'Acquéreur, dans les délais prévus dans les Conditions Particulières convenues avec lui.

La Banque Postale - S.A. à Directoire et Conseil de Surveillance - Capital Social 6 585 350 218 € - 115 rue de Sèvres 75275 Paris Cedex 06 - RCS Paris 421 100 645
- IDU EMP FR231771_01UJPN - ORIAS n° 07 023 424.

2.11 Régler, selon les Conditions Particulières convenues avec l'Acquéreur, les commissions, frais et d'une manière générale toute somme due au titre de l'acceptation des Cartes.

2.12 Utiliser obligatoirement l'Automate tel que défini à l'article 1 ci-dessus et ne pas modifier les paramètres de son fonctionnement.

2.13 Prendre toutes les mesures propres à assurer la garde de son Automate et être vigilant quant à l'utilisation qui en est faite.

2.14 Prévoir, dans ses relations contractuelles avec les tiers, tels que les prestataires de services techniques ou sous-traitants intervenant dans le traitement et le stockage des données liées à l'utilisation des Cartes, que ces derniers s'engagent à respecter le Référentiel Sécuritaire Accepteur (Annexe 1) et le Référentiel Sécuritaire PCI/DSS et acceptent que les audits visés à l'article 2.14 soient réalisés dans leurs locaux et que les rapports puissent être communiqués comme précisé dans cet article.

2.15 Permettre à l'Acquéreur de faire procéder aux frais de l'Accepteur dans les locaux de l'Accepteur ou ceux des tiers visés à l'article 2.13, à la vérification par un tiers indépendant du respect tant des clauses du présent Contrat que des exigences du Référentiel Sécuritaire Accepteur annexé au présent Contrat et/ou de celles du Référentiel Sécuritaire PCI/DSS. Cette vérification, appelée «procédure d'audit» peut intervenir à tout moment dès la conclusion du présent Contrat et/ou pendant sa durée.
L'Accepteur autorise la communication du rapport à l'Acquéreur et aux Schémas concernés.
Au cas où le rapport remis aux Parties par le tiers indépendant à l'issue de la procédure d'audit révélerait un ou plusieurs manquements à ces clauses ou exigences, l'Acquéreur peut procéder, le cas échéant, à la demande du (des) schéma(s) concerné(s), à une suspension de l'acceptation par l'Accepteur des Cartes portant la (les) Marque(s) du(des) Schéma(s) voire à une résiliation du présent contrat, dans les conditions prévues à l'article 11 du présent contrat.

2.16 L'Accepteur doit respecter les exigences du Référentiel Sécuritaire Accepteur annexé au présent Contrat et celles du Référentiel Sécuritaire PCI/DSS dont il peut prendre connaissance à l'adresse suivante: http// fr.pcisecuritystandards.org/minisite/en/ ou qui lui sera communiqué par l'Acquéreur à première demande.

2.17 Faire son affaire personnelle des litiges liés à la relation sous-jacente qui existe entre lui et le titulaire de la Carte, et de leurs conséquences financières.

2.18 Dans le cas où l'Acquéreur serait condamné, par un Réseau national ou international Carte, à payer des pénalités qui résulteraient du non-respect par l'Accepteur de ses obligations en matière de sécurité et/ou de fraude, l'Acquéreur se réserve la possibilité de demander à l'Accepteur le remboursement de son préjudice correspondant à ces pénalités.

ARTICLE 3 - OBLIGATIONS DE L'ACQUEREUR

L'Acquéreur s'engage à :

3.1 Fournir à l'Accepteur les informations le concernant directement sur le fonctionnement du (des) Schéma(s) visé(s) dans la partie 2 du présent Contrat et son/leur évolution, les Catégories de carte et les Marques dont il assure l'acceptation ainsi que les frais applicables à chacune des Catégories de carte et Marques acceptées par lui, y compris les commissions d'interchange et les frais versés au(x) Schéma(s).

3.2 Respecter le choix de la Marque utilisée pour donner l'ordre de paiement effectué au Point d'acceptation conformément au choix de l'Accepteur ou du titulaire de la Carte.

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

3.4 Créditer le compte de l'Accepteur des sommes qui lui sont dues selon les Conditions Particulières convenues avec lui.

3.5 Ne pas débiter, au-delà du délai maximum de 15 (quinze) mois à partir de la date du crédit initial porté au compte de l'Accepteur, les opérations non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.

3.6 Selon les modalités convenues avec l'Accepteur, communiquer au moins une fois par mois les informations suivantes:
- la référence lui permettant d'identifier l'opération de paiement,
- le montant de l'opération de paiement exprimé dans la devise dans laquelle son compte est crédité,
- le montant de tous les frais appliqués à l'opération de paiement et le montant de la commission de service acquittée par l'Accepteur et de la commission d'interchange.

L'Accepteur peut demander à ce que ces informations soient regroupées par Marque, application de paiement, Catégorie de carte et par taux de commission d'interchange applicable à l'opération.
Il est précisé que le taux de commission restitué dans la facture correspond à un taux moyen pondéré fourni à titre indicatif. Le taux réellement appliqué à chaque nature d'opération figure dans les reportings détaillés mis à disposition de l'Accepteur.

3.7 Indiquer et facturer à l'Accepteur les commissions de services à acquitter séparément pour chaque Catégorie de carte et chaque Marque selon les différents niveaux de commission d'interchange.
L'Accepteur peut demander à ce que les commissions de services soient regroupées par Marque, application de paiement, Catégorie de carte et par taux de commission d'interchange applicable à l'opération.

ARTICLE 4 - GARANTIE DU PAIEMENT

4.1 Les opérations de paiement sont garanties sous réserve du respect de l'ensemble des mesures de sécurité visées tant à l'article 5, 6 et 7 de la présente partie 1 qu'en partie 2 du présent Contrat, ainsi qu'aux Conditions Particulières.

4.2 Toutes les mesures de sécurité sont indépendantes les unes des autres.
Ainsi, l'autorisation donnée par le serveur d'autorisation ne vaut garantie que sous réserve du respect des autres mesures de sécurité, et notamment le contrôle du code confidentiel.

4.3 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.

ARTICLE 5 - MESURES DE SECURITE

5.1 L'Automate doit être clairement identifié par un numéro d'identification spécifique fourni par l'Acquéreur lui permettant l'accès au Système de paiement.

5.2 L'Accepteur doit informer immédiatement l'Acquéreur en cas de fonctionnement anormal de l'Automate, et pour toutes autres anomalies.

5.3 L'Accepteur doit procéder à une inspection visuelle externe approfondie des Automates afin de détecter l'éventuelle présence de matériels de capture de données placés à l'extérieur de ceux-ci. En cas de présence anormale d'un matériel, l'Accepteur doit le signaler immédiatement à l'Acquéreur.

5.4 Lors du paiement L'Accepteur s'engage à :

5.4.1 Utiliser l'Automate, respecter ou faire respecter les indications affichées sur son écran.

5.5 Après le paiement L'Accepteur s'engage à :

5.5.1 Transmettre à l'Acquéreur dans les délais et selon les modalités prévues dans les Conditions Particulières convenues avec l'Acquéreur, les enregistrements électroniques des opérations, et s'assurer que les opérations de paiement ont bien été portées au crédit du compte dans les délais et selon les modalités prévues dans les Conditions Particulières convenues avec l'Acquéreur. Toute opération ayant fait l'objet d'une autorisation transmise par l'Acquéreur doit être obligatoirement remise à ce dernier.

5.5.2 Archiver et conserver, à titre de justificatif, pendant 24 (vingt-quatre) mois après la date de l'opération, l'enregistrement électronique représentatif de chaque opération comprenant les données du ticket fourni par l'Automate (ci- après le « Ticket »).

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

ARTICLE 6 - MESURES DE SECURITE A LA CHARGE DE L'ACCEPTEUR ET ASSUREES DIRECTEMENT PAR L'AUTOMATE

L'Automate doit notamment, après lecture de la Carte, assurer automatiquement les opérations suivantes :

6.1 Interdire une opération de plus de 1500 (mille cinq cents euros) euros.

6.2 Afficher le montant réel de l'opération dès que l'Automate peut le définir ou l'estimer et, au plus tard, à la délivrance complète du bien ou du service.

6.3 Contrôler la validité de la Carte.

6.4 Lorsque la Carte le demande, mettre en oeuvre le contrôle du code confidentiel de la Carte. La preuve de ce contrôle est apportée par le certificat qui doit être enregistré par l'Automate et imprimé sur le Ticket.

6.5 En cas d'opération en mode « sans contact » permise par l'Automate, l'opération de paiement est garantie même si le code confidentiel n'a pas à être vérifié, sous réserve du respect de l'ensemble des autres mesures de sécurité à la charge de l'Accepteur.

6.6 Obtenir une autorisation au moment de l'opération et pour le montant de l'opération :
- lorsque le montant de l'opération en cause, ou le montant cumulé des opérations réglées au moyen de la même Carte, dans la même journée pour le même Point d'acceptation et pour le même type de paiement (Automate),

La Banque Postale - S.A. à Directoire et Conseil de Surveillance - Capital Social 6 585 350 218 € - 115 rue de Sèvres 75275 Paris Cedex 06 - RCS Paris 421 100 645
- IDU EMP FR231771_01UJPN - ORIAS n° 07 023 424.

dépasse celui du seuil de demande d'autorisation fixé dans les Conditions Particulières convenues avec l'Acquéreur, et ceci, quelle que soit la méthode d'acquisition des informations,
- lorsque l'Automate ou la Carte à puce déclenche une demande d'autorisation, indépendamment du seuil de demande d'autorisation de l'Automate fixé dans les Conditions Particulières convenues avec l'Acquéreur.

A défaut, l'opération ne sera pas garantie.
Une opération interdite, refusée ou interrompue par le serveur d'autorisation doit être abandonnée par l'Automate.

6.7 Proposer au client l'émission d'un Ticket. Si l'Automate ne peut pas délivrer temporairement de Ticket, il doit en informer le client avant l'opération et lui proposer d'arrêter l'opération.

6.8 Stocker les enregistrements des opérations, effectuées au Point d'acceptation en vue de leur remise à l'Acquéreur.

ARTICLE 7 - PAIEMENT AVEC PREAUTORISATION

Cet article s'applique si l'Accepteur utilise un Automate disposant de la fonctionnalité de « préautorisation » dont les modalités de paiement par Carte présentent la particularité que le montant exact du paiement n'est pas connu lorsque le titulaire de la Carte donne son consentement.
Sauf disposition contraire prévue dans le présent article, l'ensemble des dispositions du présent Contrat sont applicables.

7.1 Au moment du consentement, l'Automate doit :

7.1.1 Recueillir l'acceptation du titulaire de la carte d'être débité du montant final de l'opération dont le montant maximal estimé lui est précisé.

7.1.2 Ne pas faire usage de la Carte pour s'octroyer une caution ou un dépôt de garantie.

7.1.3 Attribuer à l'occasion de l'initialisation de l'opération de paiement un numéro de dossier indépendant du numéro de Carte.

7.1.4 Obtenir systématiquement une autorisation d'un montant identique à celui connu et accepté par le titulaire de la Carte.
A défaut, l'opération ne sera pas garantie, même pour la fraction autorisée ou correspondant au montant du seuil de demande d'autorisation.
Lorsque la puce n'est pas présente sur une Carte, l'autorisation doit être demandée en transmettant les données de la piste.
Une opération pour laquelle l'autorisation a été refusée par le serveur d'autorisation n'est jamais garantie.

7.1.5 Fournir au titulaire de la Carte l'exemplaire du Ticket qui lui est destiné sur lequel doit figurer notamment :
- le montant maximal estimé de l'opération,
- le numéro de dossier,
- la mention de : «ticket provisoire» [ou Option : «pré-autorisation»].

7.2 A la clôture du dossier l'Accepteur transmet l'opération de paiement à l'Acquéreur pour le montant final qui ne doit pas excéder le montant maximal autorisé par le titulaire de la Carte.

ARTICLE 8 - PAIEMENT «SANS CONTACT»

Cet article s'applique si l'Accepteur utilise un Automate disposant de la technologie « sans contact ».
Sauf disposition contraire prévue dans le présent article, l'ensemble des dispositions du présent Contrat sont applicables aux opérations de paiement réalisées avec une Carte équipée de la technologie « sans contact » ou un Instrument de paiement « sans contact ».
Dans ce cas, ledit Automate permet le paiement rapide grâce à une lecture à distance de la Carte équipée de la technologie « sans contact » ou de l'instrument de paiement « sans contact ».
L'Accepteur s'engage à signaler au public l'acceptation du paiement «sans contact» par l'apposition sur l'Automate, au niveau du lecteur « sans contact », de façon apparente, d'un pictogramme permettant d'identifier le paiement « sans contact ».
Le montant unitaire maximum de chaque opération de paiement en mode « sans contact » est limité :
- sans frappe du code confidentiel à 50 euros lorsque l'opération de paiement est réalisée par une Carte équipée de la technologie « sans contact ». Au-delà de ce montant unitaire maximum, les conditions de l'opération de paiement telles que prévues dans la présente partie 1 restent inchangées.

Lorsqu'un certain nombre d'opérations de paiement successives en mode « sans contact » est atteint, l'Automate peut être amené à passer en mode contact même pour une opération d'un montant inférieur au montant unitaire maximum d'une opération en mode « sans contact ».
- à 300 (trois cents) euros dans les autres cas, lorsque l'opération de paiement est réalisée par un Instrument de paiement « sans contact ». Au-delà de ce montant unitaire maximum, l'opération de paiement « sans contact » ne peut être effectuée.

Lorsque l'opération de paiement est réalisée à l'aide d'un Instrument de paiement « sans contact », les articles 9.3, et 9.4 de la présente partie 1 ne sont pas applicables.

ARTICLE 9 - MODALITES ANNEXES DE FONCTIONNEMENT

9.1 Réclamation
Toute réclamation doit être formulée par écrit à l'Acquéreur, dans un délai maximum de 6 (six) mois à compter de la date de l'opération contestée, sous peine de forclusion.
Ce délai est réduit à une durée de 15 (quinze) jours calendaires à compter de la date de débit en compte d'une opération non garantie.

9.2 Convention de preuve

De convention expresse entre les Parties, les enregistrements électroniques constituent la preuve des opérations de paiement remises à l'Acquéreur. En cas de conflit, les enregistrements électroniques produits par l'Acquéreur ou le Schéma dont les règles s'appliquent à l'opération de paiement concernée prévaudront sur ceux produits par l'Accepteur, à moins que ce dernier ne démontre l'absence de fiabilité ou d'authenticité des enregistrements produits par l'Acquéreur ou le Schéma.

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

En cas de retrait à son titulaire d'une Carte faisant l'objet d'un blocage ou en opposition (le retrait ayant eu lieu sur instruction du serveur d'autorisation), l'Accepteur utilise la procédure de gestion et de renvoi des Cartes capturées (disponible sur demande auprès de l'Acquéreur).
Pour toute capture de Carte, une prime pourra être versée à l'Accepteur ou à toute personne indiquée par lui et exerçant une activité au sein de son Point d'acceptation.

9.4 Oubli d'une Carte par son Titulaire

En cas d'oubli de sa Carte par le titulaire, l'Accepteur peut la lui restituer dans un délai maximum de deux (2) jours ouvrables après la date d'oubli de la Carte, sur justification de son identité et après obtention d'un accord demandé selon la procédure communiquée par l'Acquéreur. Au-delà de ce délai, l'Accepteur utilise la procédure de gestion et de restitution des Cartes oubliées (disponible sur demande auprès de l'Acquéreur).

9.5 Dysfonctionnement

L'Acquéreur et l'Accepteur ne peuvent être tenus pour responsable de l'impossibilité d'effectuer le paiement en cas de dysfonctionnement de la Carte et/ou de l'instrument de paiement « sans contact ».

ARTICLE 10 - MODIFICATIONS

10.1 L'Acquéreur peut modifier à tout moment les présentes Conditions Générales ainsi que les Conditions Particulières.

10.2 L'Acquéreur peut notamment apporter :

- des modifications techniques telles que l'acceptation de nouvelles Cartes, les modifications de logiciel, le changement de certains paramètres, la remise en état de l'Automate suite à un dysfonctionnement, etc.
- des modifications sécuritaires telles que :
- la modification du seuil de demande d'autorisation,
- la suppression de l'acceptabilité de certaines Cartes,
- la suspension

10.3 Les nouvelles conditions entrent généralement en vigueur au terme d'un délai minimum fixé à 1 (un) mois à compter de la notification sur support papier ou sur tout autre support informatique durable.
D'un commun accord, précisé dans les Conditions Particulières, les Parties peuvent déroger à ce délai en cas de modifications importantes.

10.4 Ce délai est exceptionnellement réduit à cinq (5) jours calendaires lorsque l'Acquéreur ou le Schéma concerné constate, dans le Point d'acceptation, une utilisation anormale de Cartes/d'Instruments de paiement « sans contact » perdu(s), volé(e)s ou contrefait(e)s.

10.5 Passés les délais visés au présent article, les modifications sont réputées acceptées par l'Accepteur s'il n'a pas résilié le présent Contrat. Elles lui sont dès lors opposables.

10.6 Le non-respect des nouvelles conditions techniques ou sécuritaires, dans les délais impartis, peut entraîner la résiliation du présent Contrat.

ARTICLE 11 - DUREE ET RESILIATION DU CONTRAT

11.1 Le présent Contrat est conclu pour une durée indéterminée, sauf dispositions contraires visées dans les Conditions Particulières.
L'Accepteur d'une part, l'Acquéreur d'autre part, peuvent, à tout moment, sans justificatif ni préavis (sauf dérogation particulière convenue entre les deux Parties), sous réserve du dénouement des opérations en cours, résilier le présent Contrat, sans qu'il soit nécessaire d'accomplir aucune autre formalité que l'envoi d'une lettre recommandée avec demande d'avis de réception. L'Accepteur garde alors la faculté de continuer à accepter les Cartes de tout Schéma avec tout autre acquéreur de son choix.
Lorsque cette résiliation fait suite à un désaccord sur les modifications prévues à l'article 10 ci-dessus, elle ne peut intervenir qu'au-delà du délai prévu dans

La Banque Postale - S.A. à Directoire et Conseil de Surveillance - Capital Social 6 585 350 218 € - 115 rue de Sèvres 75275 Paris Cedex 06 - RCS Paris 421 100 645
- IDU EMP FR231771_01UJPN - ORIAS n° 07 023 424.

cet article pour l'entrée en vigueur de ces modifications.

11.2 En outre, à la demande de tout Schéma, l'Acquéreur peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à la résiliation du présent Contrat. Elle peut être décidée notamment pour l'une des raisons visées à l'article 12.2 ci-dessous. Elle est notifiée par lettre recommandée avec demande d'avis de réception et doit être motivée. Son effet est immédiat.

11.3 Toute cessation d'activité de l'Accepteur, cession ou mutation du fonds de commerce, entraîne la résiliation immédiate de plein droit du présent Contrat, sous réserve du dénouement des opérations en cours.
Dans le cas où, après résiliation du présent Contrat, il se révélerait des impayés, ceux-ci seront à la charge de l'Accepteur ou pourront faire l'objet d'une déclaration de créances.
L'Accepteur s'engage à retirer immédiatement de son Point d'acceptation tout signe d'acceptation des Cartes ou Marques des Schémas concernés.

ARTICLE 12 - PENALITES DES SCHEMAS DE CARTES

Les schémas de cartes édictent des règles que l'Accepteur par l'intermédiaire de son Acquéreur doit respecter. Parmi ces règles édictées, il y a notamment le respect des obligations suivantes:
- celles applicables en matière de sécurité et/ou de fraude,
- suivre mensuellement la fraude et les impayés,
- se conformer à la réglementation locale et européenne en vigueur et mettre en œuvre son évolution,
- exercer son activité dans la zone géographique autorisée.

Dans le cas où l'Acquéreur serait condamné par un schéma de carte à payer des pénalités qui résulteraient du non respect de ces règles par l'Accepteur, l'Acquéreur se réserve la possibilité de demander à l'Accepteur le remboursement des pénalités.

ARTICLE 13 - SUSPENSION DE L'ACCEPTATION

13.1 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/Instrument de paiement sans contact portant certaines Marques par l'Accepteur.
Cette suspension de l'acceptation par l'Accepteur peut s'appliquer à la(les) marques du(des) schémas(s) de manière partielle (limitation en volume, montant des opérations, limitation à une zone géographie,...) ou totale.
La suspension est précédée, le cas échéant, d'un avertissement à l'Accepteur, voire d'une réduction de son seuil de demande d'autorisation. Elle est notifiée par tout moyen et doit être motivée. Son effet est immédiat.
Elle peut également intervenir à l'issue d'une procédure d'audit telle que visée à l'article 2.14 de la présente partie 1, au cas où le rapport révélerait un ou plusieurs manquements tant aux clauses du présent Contrat qu'aux exigences du Référentiel Sécuritaire Accepteur annexé au présent Contrat et/ou du Référentiel Sécuritaire PCI/DSS.

13.2 La suspension peut être décidée en raison notamment :

- 13.2.1 du non-respect répété des obligations du présent Contrat ou du refus d'y remédier, notamment d'une utilisation d'un Automate non agréé permettant à l'Accepteur d'accéder au Système d'Acceptation et d'un risque de dysfonctionnement important du Système d'Acceptation du Schéma,
- 13.2.2 d'une participation à des activités frauduleuses, notamment d'une utilisation anormale de Cartes/d'Instruments de paiement « sans contact » perdu(e)s, volé(e)s ou contrefait(e)s,
- 13.2.3 L'Accepteur s'engage alors à restituer à l'Acquéreur l'Equipement Electronique, les dispositifs techniques et sécuritaires 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 du Schéma concerné.
- 13.2.4 de plaintes répétées d'autres membres ou partenaires d'un Schéma et qui n'ont pu être résolues dans un délai raisonnable,
- 13.2.5 de retard volontaire ou non motivé de transmission des justificatifs,
- 13.2.6 d'un risque aggravé en raison des activités de l'Accepteur.

13.3 L'Accepteur s'engage alors à restituer à l'Acquéreur l'Equipement Electronique, les dispositifs techniques et sécuritaires 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 du Schéma concerné.

13.4 La période de suspension est au minimum de six (6) mois, éventuellement renouvelable. A l'expiration de ce délai, l'Accepteur peut demander la reprise du présent Contrat auprès de l'Acquéreur ou souscrire un nouveau contrat d'acceptation en paiement de proximité par cartes de paiement avec un autre acquéreur de son choix.

ARTICLE 14 - MESURES DE PREVENTION ET DE SANCTION PRISES PAR L'ACQUEREUR

14.1 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/d'instruments de paiement « sans contact » perdu(e)s, volé(e)s ou contrefait(e)s, l'Acquéreur peut prendre des mesures de sauvegarde et de sécurité consistant, en premier lieu, en un avertissement à l'Accepteur valant mise en demeure précisant les mesures à prendre pour remédier au manquement ou résorber le taux d'impayés anormalement élevé constaté.

14.2 Si, dans un délai de trente (30) jours, l'Accepteur n'a pas remédié au manquement ayant justifié l'avertissement ou n'a pas mis en oeuvre les mesures destinées à résorber le taux d'impayés constaté, l'Acquéreur peut soit procéder à une suspension de l'acceptation des Cartes/des Instruments de paiement « sans contact » dans les conditions précisées à l'article 10 ci-dessus, soit résilier de plein droit avec effet immédiat, sous réserve du dénouement des opérations en cours, le présent Contrat par l'envoi d'un courrier simple.

14.3 De même, si dans un délai de trois (3) mois à compter de l'avertissement, l'Accepteur est toujours confronté à un taux d'impayés anormalement élevé, l'Acquéreur peut décider la résiliation de plein droit avec effet immédiat, sous réserve des opérations en cours, du présent Contrat, notifiée par l'envoi d'un courrier simple.

14.4 Lutte contre la corruption

Les dispositions applicables à la lutte contre la corruption sont précisées à l'article « Lutte contre la corruption » des Conditions Générales de la Convention de Compte Courant Postal en vigueur (Professionnels et Associations de proximité ou Entreprises-Economie Sociale et Secteur Public Local).

ARTICLE 15 - PROTECTION DES DONNEES A CARACTERE PERSONNEL

Les données à caractère personnel recueillies font l'objet de traitements dont le responsable est La Banque Postale, conformément à la réglementation relative à la protection des données à caractère personnel.
Elles sont traitées pour la gestion de la relation bancaire, des comptes ou des produits et services souscrits, pour la gestion des clients et des prospects et en vertu de l'exécution du contrat ou du respect d'obligations légales ou règlementaires, telles que la lutte contre le blanchiment des capitaux et le financement du terrorisme. Les données de l'Accepteur seront conservées pendant la durée de la relation contractuelle.
Les données sont également utilisées dans l'intérêt légitime de la Banque notamment dans le cadre de la lutte contre la fraude et la cybercriminalité, ainsi qu'à des fins d'optimisation, de personnalisation et de ciblage des offres commerciales pour améliorer la relation commerciale, et conservées à ce titre pour une durée de 1 an.
Par ailleurs, elles peuvent être utilisées à des fins de prospection commerciale par voie postale ou par téléphone ou par voie électronique, dans l'intérêt légitime de la Banque et conservées à ce titre pour une durée de 3 ans à compter de la fin de la relation commerciale ou du dernier contact avec l'Accepteur.
L'ensemble de ces données pourra être conservé au-delà des durées précisées, dans le respect des délais de prescription légaux applicables.
Les données à caractère personnel collectées sont obligatoires pour la souscription aux produits et services de la Banque. A défaut, les demandes de souscription ne pourront pas être traitées et l'Accepteur s'expose à un refus ou à la résiliation des produits ou services concernés.
La Banque collecte auprès de ses filiales les données à caractère personnel de l'Accepteur et les informations relatives aux produits qu'il a souscrits auprès d'elles. La Banque peut également, dans le cadre de ses obligations légales et réglementaires, collecter des données à caractère personnel auprès d'administrations et autorités publiques (INSEE, Banque de France, Administration fiscale, ...).
Elles sont destinées à la Banque et pourront être communiquées aux sociétés du Groupe auquel elle appartient et à ses sous-traitants ou partenaires pour les traitements et finalités cités ci-avant. Elles pourront également être communiquées à toute autorité administrative ou judiciaire habilitée ou plus généralement à tout tiers autorisé, pour satisfaire à ses obligations légales ou réglementaires.
L'Accepteur dispose d'un droit d'accès, de rectification, d'effacement, d'opposition et de limitation du traitement. Il peut faire une demande de portabilité pour les données qu'il a fournies et qui sont nécessaires au contrat ou au traitement desquelles il a consenti. Il peut à tout moment retirer son consentement lorsque celui-ci a été préalablement donné. Il peut aussi donner des instructions relatives à la conservation, à l'effacement et à la communication de ses données après son décès.
Il peut exercer ces droits en précisant son nom, prénom, adresse postale et en joignant une copie recto-verso de sa pièce d'identité, en s'adressant par courrier au responsable de traitement, La Banque Postale - Service Relations Clients - 115, rue de Sèvres - 75275 Paris Cedex 06.
La Banque peut prendre des décisions automatisées, y compris par profilage, concernant l'Accepteur. Ces décisions sont prises après interrogation des

La Banque Postale - S.A. à Directoire et Conseil de Surveillance - Capital Social 6 585 350 218 € - 115 rue de Sèvres 75275 Paris Cedex 06 - RCS Paris 421 100 645
- IDU EMP FR231771_01UJPN - ORIAS n° 07 023 424.

fichiers réglementaires (FICOBA, FICP, FCC, ...), après analyse du profil de risque de l'Accepteur et des pièces justificatives fournies. Selon les cas ces décisions peuvent se traduire par le refus d'accès à un produit ou un service.
L'Accepteur peut s'adresser au Délégué à la Protection des Données de La Banque Postale - 115, rue de Sèvres - 75275 Paris Cedex 06.
En cas de difficulté en lien avec la gestion de ses données à caractère personnel, l'Accepteur a le droit d'introduire une réclamation auprès de la Commission Nationale de l'Informatique et des Libertés (CNIL).

ARTICLE 16 - SERVICE CLIENT – TRAITEMENT DES RECLAMATIONS

Les dispositions applicables au traitement des réclamations sont précisées à l'article « Traitement des réclamations » de la Convention de compte en vigueur (Professionnels et Associations de proximité ou Entreprises-Economie Sociale et Secteur Public Local).

ARTICLE 17 - 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 18 - DÉMARCHAGE – RÉTRACTATION

Le Client, dont le total de bilan ou le chiffre d'affaires ou le montant des recettes ou le montant des actifs gérés ne dépasse pas 5 millions d'euro ou dont les effectifs annuels moyens ne dépassent pas 50 personnes au jour de la souscription, qui a souscrit le Service par voie de démarchage dispose d'un délai de 14 jours calendaires révolus pour exercer son droit de rétractation, sans avoir à justifier de motif ni à supporter de pénalités. Ce délai commence à courir soit à compter du jour où le contrat est conclu soit à compter du jour où le Client a reçu les conditions contractuelles et les informations, si cette date est postérieure à la date à laquelle le contrat est conclu.

Pour faire valoir ce droit, le Client envoie sa demande de rétractation par courrier simple à son Service Clients en mentionnant les éléments suivants:
- Sa raison sociale et son adresse,
- Son numéro de CCP
- Le nom du Service : « Contrat d'acceptation en Paiement de Proximité par cartes de paiement »
- La date de signature de la souscription du Service,
- La signature du représentant légal.

Le Client est redevable du prix correspondant aux produits et/ou services fournis entre la date de conclusion du contrat et celle de la rétractation. Le Client a 30 jours pour restituer à la Banque toute somme ou tout bien qu'il aurait reçu en exécution du contrat.

ARTICLE 19 - LOI APPLICABLE

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.

ARTICLE 20 - LANGUE DU PRESENT CONTRAT

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

La Banque Postale - S.A. à Directoire et Conseil de Surveillance - Capital Social 6 585 350 218 € - 115 rue de Sèvres 75275 Paris Cedex 06 - RCS Paris 421 100 645 - IDU EMP FR231771_01UJPN - ORIAS n° 07 023 424.

PARTIE 2 DISPOSITIONS SPECIFIQUES A CHAQUE SCHEMA

DISPOSITIONS SPECIFIQUES AUX SCHEMAS VISA ET MASTERCARD

ARTICLE 1 - FONCTIONNEMENT DES SCHEMAS

Les entités responsables des Schémas sont :

• Visa Europe et VISA Inc,

• MasterCard Europe SA.

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

• Pour VISA Inc. et Visa Europe :

- Visa,
- V PAY,
- ELECTRON.

• Pour MasterCard Europe SA. :

- MasterCard,
- Maestro.

ARTICLE 2 - OBLIGATIONS DE L'ACQUEREUR

Par dérogation à l'article 3.6 de la partie 1 du Contrat, l'Acquéreur s'engage à ne pas débiter, au-delà du délai maximum de vingt-quatre (24) mois à partir de la date du crédit initial porté au compte de l'Accepteur, les opérations non garanties et qui n'ont pu être imputées au compte sur lequel fonctionne la Carte.

ARTICLE 3 - GARANTIE DE PAIEMENT

Une opération de paiement réalisée en lecture puce EMV est garantie, même s'il n'y a pas eu frappe du code confidentiel par le titulaire de la Carte, à condition d'avoir obtenu une autorisation d'un montant identique à ladite opération.

DISPOSITIONS SPECIFIQUES AU SCHEMA CB

ARTICLE 1 - DEFINITION DU SCHEMA CB

Le Schéma CB repose sur l'utilisation de Cartes portant la Marque CB (ci-après les «Cartes CB») pour le paiement d'achats de biens et/ou de prestations de services ou pour le règlement de dons ou de cotisations auprès des Accepteurs adhérant au Schéma CB et cela dans le cadre des seules dispositions et procédures définies ou homologuées par le GIE CB.

Le GIE CB intervient notamment, pour des raisons sécuritaires, dans les modifications du seuil de demande d'autorisation, la suppression de l'acceptabilité de certaines Cartes CB ou solutions de paiement CB et la suspension de l'adhésion au Schéma CB. Il établit les conditions du contrat d'acceptation, l'Acquéreur définissant certaines conditions spécifiques de fonctionnement.

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

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

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

• les Cartes sur lesquelles figure la Marque CB,

• les solutions de paiement CB.

ARTICLE 2 BIS - DISPOSITIONS RELATIVES AUX CARTES PREPAYEES SANS PUCE

Les obligations prévues à l'article 2.1 de la partie 1 et à l'article 2 ci-dessus ne sont pas applicables aux cartes prépayées sans puce ne portant pas la Marque CB qui peuvent être acceptées dans le Schéma CB par l'Accepteur ayant signé un contrat spécial pour ce faire avec l'émetteur de ces cartes.

ARTICLE 3 - DISPOSITIONS SUR L'ACCEPTATION DE CARTES CB

En complément des dispositions des articles 2.7, 2.8 et 2.14 de la Partie 1 du présent Contrat, l'Accepteur s'engage:

- à accepter les Cartes telles que définies à l'article 2 ci-dessus pour le paiement d'achats de biens ou de prestations de services offerts à sa clientèle et réellement effectués (à l'exclusion de toute délivrance d'espèces ou de tout titre convertible en espèces pour leur valeur faciale), même lorsqu'il s'agit d'articles vendus à titre de promotion ou de soldes, pour le paiement de dons ou en contrepartie du règlement du montant de cotisations,

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

- En cas de demande d'audit par le GIE CB, à permettre à l'Acquéreur de faire procéder aux frais de l'Accepteur dans ses locaux ou ceux de ses prestataires, à la vérification par un tiers indépendant du respect tant des clauses du présent Contrat que des exigences du Référentiel Sécuritaire Accepteur et/ou du Référentiel Sécuritaire PCI/DSS. Cette vérification, appelée «procédure d'audit», peut intervenir à tout moment dès la conclusion du présent Contrat et/ou pendant sa durée.

- Au cas où le rapport remis aux Parties par le tiers indépendant à l'issue de la procédure d'audit révélerait un ou plusieurs manquements à ces clauses ou exigences, le GIE CB peut procéder à une suspension de l'adhésion, voire à une radiation du Schéma CB telle que prévue à l'article 4 ci-après. L'Accepteur autorise la communication du rapport à l'Acquéreur et au GIE CB.

ARTICLE 4 - SUSPENSION DE L'ADHESION ET RADIATION DU SCHEMA CB

4.1 Le GIE CB peut procéder, pour des raisons de sécurité, sans préavis et sous réserve du dénouement des opérations en cours, à une suspension de l'adhésion au 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 tout moyen. Son effet est immédiat.

Elle peut être décidée en raison notamment :

- d'une utilisation anormale de Cartes/d'Instruments de paiement « sans contact » perdu(e)s, volé(e)s ou contrefait(e)s,

- d'une utilisation d'un Equipement Electronique non agréé,

- d'un risque de dysfonctionnement important du Schéma CB.

4.2 L'Accepteur s'engage alors à restituer à l'Acquéreur l'Equipement Electronique, les dispositifs techniques et sécuritaires 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.

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

4.4 A l'expiration de ce délai, l'Accepteur peut, sous réserve de l'accord préalable du GIE CB, demander la reprise d'effet du présent Contrat auprès de l'Acquéreur, ou souscrire un nouveau contrat d'adhésion 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 - PROTECTION DES DONNÉES A CARACTERE PERSONNEL

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

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

la lutte contre la fraude et la gestion des éventuels recours en justice, conformément aux missions définies dans les statuts du GIE CB ;

de répondre aux obligations réglementaires ou légales notamment en matière pénale ou administrative liées à l'utilisation de la Carte.

La Banque Postale - S.A. à Directoire et Conseil de Surveillance - Capital Social 6 585 350 218 € - 115 rue de Sèvres 75275 Paris Cedex 06 - RCS Paris 421 100 645
- IDU EMP FR231771_01UJPN - ORIAS n° 07 023 424.

L'Accepteur (personne physique ou personne physique le représentant sur laquelle portent les données à caractère personnel) peut exercer les droits prévus au chapitre III du Règlement (UE) 2016/679 du 27 avril 2016 et détaillés à l'article 15 de la Partie 1 des présentes Conditions Générales par courriel à protegezvosdonnees@cartes-bancaires.com.

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

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

Juillet 2025

ANNEXE 1 : REFERENTIEL SECURITAIRE ACCEPTEUR

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

EXIGENCE 1 (E1) : GERER LA SECURITE DU SYSTEME COMMERCIAL ET D'ACCEPTATION AU SEIN DE L'ENTREPRISE

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

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

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

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

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

EXIGENCE 2 (E2) : GERER L'ACTIVITE HUMAINE ET INTERNE

Les obligations et les responsabilités du Personnel quant à l'utilisation des données bancaires et confidentielles, à leur stockage et à leur circulation en interne ou à l'extérieur doivent être établies. Il en est de même pour l'utilisation des postes de travail et du réseau interne comme du réseau Internet.

Les obligations et les responsabilités du Personnel quant à la protection des données bancaires et confidentielles doivent être établies. L'ensemble de ces règles doit s'appliquer à tous les personnels impliqués : salariés de l'entreprise et tiers.

Le Personnel doit être sensibilisé aux risques encourus, notamment sur la divulgation d'informations confidentielles, l'accès non autorisé aux informations, aux supports et aux documents.

Le Personnel doit être régulièrement sensibilisé aux risques particuliers liés à l'usage des moyens informatiques (postes de travail en réseau, serveurs, accès depuis ou vers Internet) et notamment, à l'introduction de virus.

Il convient que le Personnel reçoive une formation appropriée sur l'utilisation correcte du système d'exploitation et du système applicatif commercial et d'acceptation.

EXIGENCE 3 (E3) : GERER LES ACCES AUX LOCAUX ET AUX INFORMATIONS

Tout dispositif (équipement réseau, serveur, ...) qui stocke ou qui traite des données relatives à une opération de paiement et notamment, des données du titulaire de la Carte doit être hébergé dans un local sécurisé et répondre aux exigences édictées par les règles et recommandations de la CNIL.

Les petits matériels ou supports informatiques sensibles doivent être rendus inaccessibles à des tiers en période de non utilisation. Notamment, les cartouches de sauvegarde doivent être stockées dans un coffre.

Dans le cas où ces petits matériels ou supports informatiques sensibles ne sont plus opérationnels, ils doivent être obligatoirement détruits et la preuve de leur destruction doit être établie.

La politique d'accès aux locaux sensibles doit être formalisée et les procédures doivent être établies et contrôlées.

EXIGENCE 4 (E4) : ASSURER LA PROTECTION LOGIQUE DU SYSTEME COMMERCIAL ET D'ACCEPTATION

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

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

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

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

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

Le pare-feu doit être mis à jour systématiquement lorsque des vulnérabilités sont identifiées sur ses logiciels (logiciel pare-feu et logiciel d'exploitation) et 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) : CONTROLER L'ACCES AU SYSTEME COMMERCIAL ET D'ACCEPTATION

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

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

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

EXIGENCE 6 (E6) : GERER LES ACCES AUTORISES AU SYSTEME COMMERCIAL ET D'ACCEPTATION

Aucune ouverture de droits ne peut se faire en dehors des procédures d'autorisation adéquates.

Les autorisations données doivent être archivées et contrôlées régulièrement.

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

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

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

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

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

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

Les tentatives d'accès doivent être limitées en nombre.

Les mots de passe doivent être changés régulièrement.

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

EXIGENCE 7 (E7) : SURVEILLER LES ACCES AU SYSTEME COMMERCIAL ET D'ACCEPTATION

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

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

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

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

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

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

La Banque Postale - S.A. à Directoire et Conseil de Surveillance - Capital Social 6 585 350 218 € - 115 rue de Sèvres 75275 Paris Cedex 06 - RCS Paris 421 100 645
- IDU EMP FR231771_01UJPN - ORIAS n° 07 023 424.

EXIGENCE 8 (E8) : CONTROLER L'INTRODUCTION DE LOGICIELS PERNICIEUX

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

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

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

EXIGENCE 9 (E9) : APPLIQUER LES CORRECTIFS DE SECURITE (PATCHES DE SECURITE) 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) : GERER 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'INTEGRITE DES LOGICIELS APPLICATIFS RELATIFS AU SYSTEME COMMERCIAL ET D'ACCEPTATION

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

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

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

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

EXIGENCE 12 (E12) : ASSURER LA TRAÇABILITE DES OPERATIONS 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'INTEGRITE DES INFORMATIONS RELATIVES AU SYSTEME COMMERCIAL ET D'ACCEPTATION

La protection et l'intégrité des éléments de l'opération de paiement doivent être assurées ainsi lors de leur stockage et lors de leur routage sur les réseaux (internes ou externes). Il en est de même pour les éléments secrets servant à chiffrer ces éléments.

Le dossier de sécurité propre au système commercial et d'acceptation doit décrire les moyens mis en place pour répondre à cette exigence.

EXIGENCE 14 (E14) : PROTEGER LA CONFIDENTIALITE DES DONNEES BANCAIRES

Les données du titulaire de la Carte ne peuvent être utilisées que pour exécuter l'ordre de paiement et pour traiter les réclamations. Le cryptogramme visuel d'un titulaire de Carte ne doit en aucun cas être stocké par l'Accepteur.

Les données bancaires et à caractère personnel relatives à une opération de paiement, et notamment les données du titulaire de la Carte doivent être protégées lors de leur stockage et lors de leur routage sur les réseaux internes et externes au site d'hébergement conformément aux dispositions de la loi Informatique et Libertés et aux recommandations de la CNIL. Il en est de même pour l'authentifiant de l'Accepteur et les éléments secrets servant à chiffrer.

Le dossier de sécurité propre au système commercial et d'acceptation doit décrire les moyens mis en place pour répondre à cette exigence.

EXIGENCE 15 (E15) : PROTEGER LA CONFIDENTIALITE DES IDENTIFIANTS – AUTHENTIFIANTS DES UTILISATEURS ET ADMINISTRATEUR

La confidentialité des identifiants-authentifiants doit être protégée lors de leur stockage et de leur circulation.

Il convient de s'assurer que les données d'authentification des administrateurs ne puissent être réutilisées.

Dans le cadre d'une intervention extérieure pour maintenance, les mots de passe utilisés doivent être systématiquement changés à la suite de l'intervention.

La Banque Postale - S.A. à Directoire et Conseil de Surveillance - Capital Social 6 585 350 218 € - 115 rue de Sèvres 75275 Paris Cedex 06 - RCS Paris 421 100 645 - IDU EMP FR231771_01UJPN - ORIAS n° 07 023 424.

ANNEXE 2 : REFERENTIEL SECURITAIRE 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 :

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

2° Protéger les données des titulaires de Cartes

3ème exigence	Protéger les données des titulaires de Cartes stockées
4ème exigence	Crypter la transmission des données des titulaires de Cartes sur les réseaux publics ouverts

3° Disposer d'un programme de gestion de la vulnérabilité

5ème exigence	Utiliser et mettre à jour régulièrement un logiciel antivirus
6ème exigence	Développer et gérer des applications et systèmes sécurisés

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

7ème exigence	Limiter l'accès aux données des titulaires de Cartes aux cas de nécessité professionnelle absolue
8ème exigence	Attribuer une identité d'utilisateur unique à chaque personne disposant d'un accès informatique
9ème exigence	Limiter l'accès physique aux données des titulaires de Cartes

5° Surveiller et tester régulièrement les réseaux

10ème exigence	Suivre et surveiller tous les accès aux ressources du réseau et aux données des titulaires de Cartes
11ème exigence	Tester régulièrement les systèmes et procédures de sécurité

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

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

Juillet 2025