















en contrepartie du règlement du montant de cotisations, à transmettre les enregistrements des opérations de paiement à la Banque 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 la Banque de faire procéder aux frais de l'Accepteur dans les locaux de l'Accepteur ou dans ceux des tiers visés à l'article 3.14 de la partie I du présent Contrat, 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 1.4 ci-après. Le Client autorise la communication du rapport à la Banque et au GIE CB.

#### 1.4 Suspension de l'adhésion et radiation du Schéma CB

1.4.1 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 au Client, 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.

1.4.2 Le Client s'engage alors à restituer à la Banque l'Equipement Electronique, les dispositifs techniques et sécuritaires et les documents en sa possession dont la Banque est propriétaire, et à retirer immédiatement de son Point d'acceptation tout signe d'acceptation des Cartes CB.

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

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

1.4.5 En cas de comportement frauduleux de la part du Client, il peut être immédiatement radié du Schéma CB ou la suspension être convertie en radiation.

détenteurs d'un seul compte bancaire professionnel au sein du Crédit Agricole ou de tout autre établissement bancaire et réalisant ou prévoyant de réaliser un chiffre d'affaires d'encaissement carte inférieur à 12 000 euros (douze mille) par année civile. La Caisse Régionale propose une offre spécifique consistant en l'application d'un forfait unique de 4€ par mois, quel que soit le nombre de transactions effectuées et quel que soit le montant des transactions.

1.2 REVISION DU PRIX : Les Parties conviennent que le forfait pourra être modifié, chaque début d'année civile, par application des nouvelles conditions générales de banque entrant en vigueur le 1er janvier de chaque année.

Si le Chiffre d'Affaires Monétique du Client dépasse 12 000 € par an durant l'exécution du Contrat, le forfait sera remplacé automatiquement par le taux de commission monétique prévu dans les conditions spécifiques de fonctionnement. Cette révision interviendra au cours du premier trimestre de chaque année civile après examen du Chiffre d'affaires monétique de l'année écoulée. La Caisse Régionale en informera le Client par courrier simple.

1.3 L'acquéreur se réserve le droit de demander à l'Accepteur tout document permettant à ce dernier de justifier de son Chiffre d'affaires d'encaissement cartes sur l'année précédente dont notamment son dernier Relevé Annuel de Frais d'Encaissements Cartes (RAFEC). »

## ADDENDUM FORFAIT « PETIT

### COMMERCANT »1.1 L'offre « Petit

Commerçant » est réservé aux accepteurs



## 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.

Version 2017

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 corrigables.

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.

### **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 ADMINISTRATEURS**

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

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

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

## ANNEXE 2 : REFERENTIEL SECURITAIRE PCI-DSS

Les exigences constituant le Référentiel Sécuritaire PCI-DSS sont organisées autour d'un ensemble de douze (12) familles d'exigences regroupant deux cent cinquante (250) règles réparties en six (6) grands domaines présentés ci-après :

### 1° Mettre en place et gérer un réseau sécurisé

1 <sup>ère</sup> exigence	Installer et gérer une configuration de pare-feu afin de protéger les données des Titulaires des Cartes
2 <sup>ème</sup> 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

3 <sup>ème</sup> exigence	Protéger les données des Titulaires de Cartes stockées
4 <sup>ème</sup> 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

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

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

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

### 5° Surveiller et tester régulièrement les réseaux

10 <sup>ème</sup> exigence	Suivre et surveiller tous les accès aux ressources du réseau et aux données des Titulaires de Cartes
11 <sup>ème</sup> exigence	Tester régulièrement les systèmes et procédures de sécurité

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

12 <sup>ème</sup> exigence	Disposer d'une politique régissant la sécurité de l'information
----------------------------	---

L'intégralité des exigences du Référentiel Sécuritaire PCI-DSS, ainsi que leurs mises à jour sont disponibles à l'adresse internet suivante : <http://fr.pcisecuritystandards.org/minisite/en/>

## ANNEXE 3 : CONDITIONS DE FONCTIONNEMENT DU SERVICE « DIFFERE SANTE »

### Préambule :

La présente annexe détaille les conditions de fonctionnement du service « Différé Santé », en complément des Conditions Générales et Conditions Particulières du présent Contrat. Ce service est destiné aux Clients (i) Professionnels de Santé listés ci-dessous, (ii) disposant d'un Equipement Electronique compatible avec l'accès au service « Différé Santé », et (iii) ayant choisi cette option aux Conditions Particulières du présent Contrat. Elle expose notamment les conditions dans lesquelles les Clients Professionnels de Santé peuvent bénéficier d'un délai prolongé de présentation en compensation des opérations leur permettant ainsi de proposer à leurs patients un délai supplémentaire avant que leur propre compte soit débité.

Les termes dotés d'une initiale majuscule non définis dans la présente annexe ont la signification qui leur est attribuée dans les Conditions Générales et/ou Particulières du Contrat.

### Article 1 : Conditions préalables

Le service « Différé Santé » est soumis aux conditions préalables et suspensives suivantes :

- Cartes : le service « Différé Santé » n'est disponible que pour les Cartes sur lesquelles figurent la Marque « CB ». En conséquence, le Client s'engage à systématiquement refuser sur son TPE le « Différé Santé » pour les autres cartes.
- Professionnels de Santé : le service « Différé Santé » n'est disponible que pour les Professionnels de Santé identifiés par les codes APE (NAF) suivants, déclarés à l'INSEE :

SECTEURS	APE (NAF) 2008	APE (NAF) 2003
Commerce de détail de produits Pharmaceutiques	4773Z	523A
Activités hospitalières	8610Z	851A
Pratique médicale	8621Z-8622A / 8622B-8622C	851C
Pratique dentaire	8623Z	851E
Activités des auxiliaires médicaux	8690D-8690E / 8710A-8710B 8710C-8720A / 8720B-8730A / 8730B	851G
Ambulances	8690A	851J
Laboratoires analyse médicale	8690B	851K
Commerce de détail d'optique et de photographie <sup>1</sup>	4778A <sup>1</sup>	524T <sup>1</sup>

Le Client est informé que (a) le service « Différé Santé » ne sera activé/disponible que postérieurement à la réception d'une confirmation de l'INSEE de son enregistrement sous l'un des code APE (NAF) listé ci-dessus, et (b) cette procédure peut prendre quelques jours.

Le service « Différé Santé » sera résilié de plein droit en cas de changement de numéro SIRET du Client, sauf accord préalable de la Banque.

- Choix lors de l'opération de paiement : lors de l'opération de paiement, le TPE proposera systématiquement au Client de choisir l'option « Différé Santé ». Le service « Différé Santé » ne sera effectif, pour chaque opération, qu'en cas d'acceptation de l'option par le Client.

### Article 2 : Obligation du Client

Le Client s'engage à informer systématiquement son patient de la possibilité de bénéficier du « Différé Santé » et du délai supplémentaire dont ce dernier bénéficiera en cas de choix de cette option.

### Article 3 : Délais du « Différé Santé »

Des délais spécifiques sont fixés dans les Conditions Particulières pour le crédit du compte du Client et la remise en compensation.

### Article 4 : Divers

Les stipulations des Conditions Générales et Conditions Particulières non modifiées par la présente annexe restent applicables.

<sup>1</sup> Activité d'optique uniquement, le Client doit fournir une déclaration sur l'honneur qu'il ne pratique que l'activité d'optique