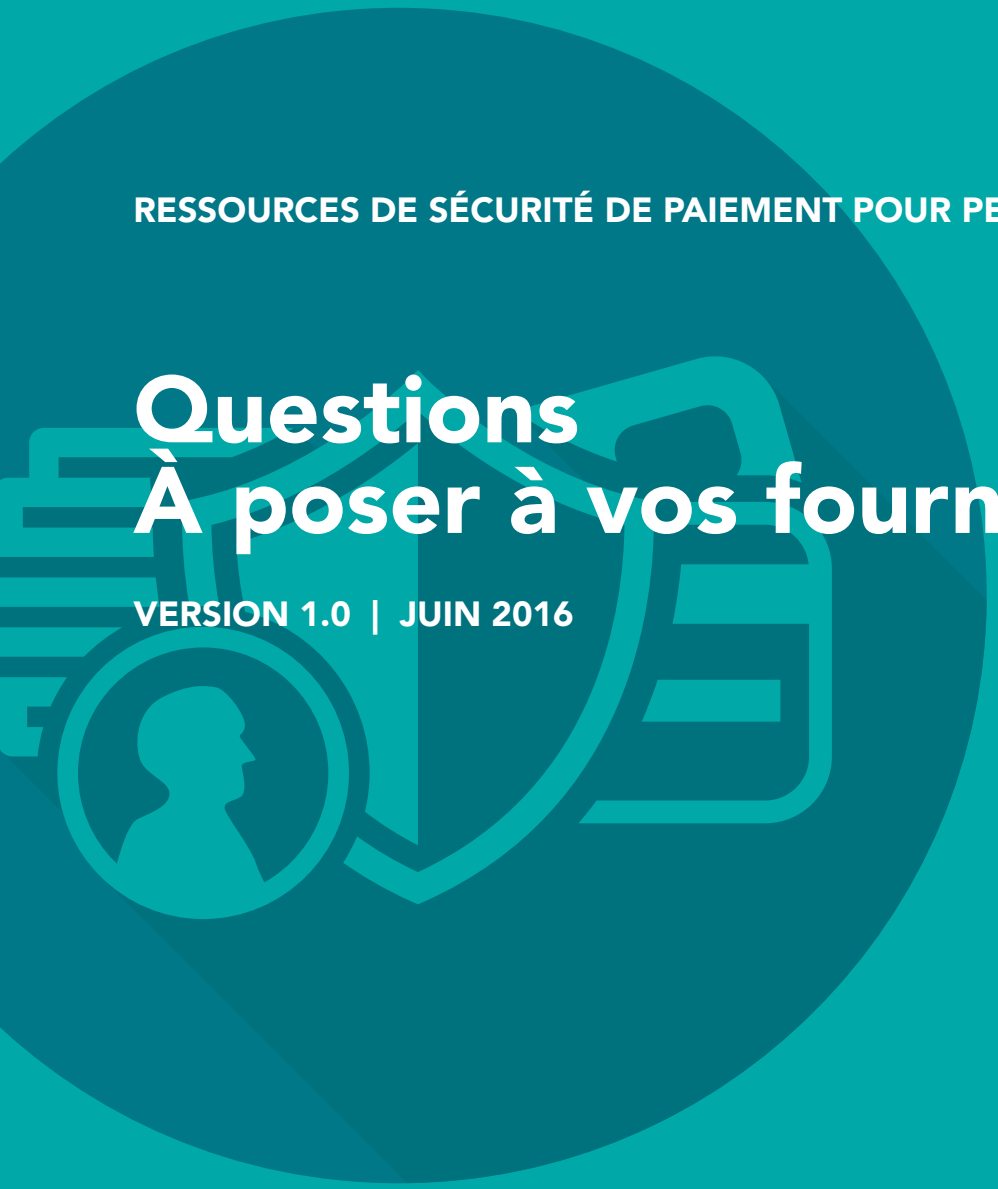
RESSOURCES DE SÉCURITÉ DE PAIEMENT POUR PETITS COMMERÇANTS

Questions À poser à vos fournisseurs

VERSION 1.0 | JUIN 2016



PCI Security Standards Council®

INTRODUCTION 1

FOURNISSEURS ET PRESTATAIRES DE SERVICES 2

QUESTIONS 3

Introduction

Ce document a été préparé afin de servir de guide pour les propriétaires et opérateurs des petits commerçants. En proposant des questions à poser à vos fournisseurs à prestataires de services, ce document est destiné à vous aider à comprendre comment ces entités soutiennent la protection des données de carte de vos clients.

Le document « Questions à poser à vos fournisseurs » a été développé comme complément au *Guide de paiement sécurisé*, faisant partie du document Ressources de sécurité de paiement pour petits commerçants. Veuillez vous reporter au *Guide de paiement sécurisé* et aux autres Ressources de sécurité de paiement pour petits commerçants, aux endroits suivants :

RESSOURCE	URL
Guide de paiement sécurisé	https://fr.pcisecuritystandards.org/pdfs/Small_Merchant_Guide_to_Safe_Payments.pdf
Systèmes de paiement courants	https://fr.pcisecuritystandards.org/pdfs/Small_Merchant_Common_Payment_Systems.pdf
Glossaire des termes de paiement et de sécurité des informations	https://fr.pcisecuritystandards.org/pdfs/Small_Merchant_Glossary_of_Payment_and_Information_Security_Terms.pdf

Fournisseurs et prestataires de services : comment ils fonctionnent ?

Les petites entreprises/petits commerçants peuvent entrer en contact avec un grand nombre de fournisseurs ou de prestataires de services de paiement. Il est important pour les commerçants de comprendre le type de fournisseur avec lequel ils travaillent et de s'assurer que le fournisseur a pris les mesures appropriées pour protéger les données de carte.

Le tableau en page 2 décrit les types les plus courants de fournisseurs et prestataires de services de paiement et ce que les commerçants doivent rechercher avec chaque fournisseur.

Le tableau commençant en page 3 propose aux commerçants des questions qu'ils peuvent poser à leurs fournisseurs ou prestataires de services, afin de les aider à comprendre le rôle du fournisseur ou du prestataire de services dans la protection des données de carte.

Fournisseurs et prestataires de services

Le tableau ci-dessous décrit le type le plus courant de fournisseurs et prestataires de services de paiement et ce que les commerçants doivent rechercher avec chaque fournisseur.

TYPE DE FOURNISSEUR/ PRESTATAIRE DE SERVICES	FONCTION	NORME OU PROGRAMME PCI	RECHERCHER :
Fournisseur de l'application de paiement	Vendre des applications de stockage, traitement et/ou transfert des données du titulaire et proposer une assistance pour ces applications.	PA-DSS (Norme de sécurité des données des applications de paiement)	L'application apparaît sur la List of PCI PA-DSS of Validated Payment Applications (Liste des applications de paiement conformes à la norme PCI PA-DSS).
Fournisseur du terminal de paiement	Vendre des dispositifs utilisés pour accepter des paiements par carte (par ex. terminal de paiement) et proposer une assistance pour ces dispositifs.	Sécurité de transaction par code PIN (PTS)	Le terminal de paiement apparaît sur la PCI Council's Approved PTS Devices (Dispositifs PTS approuvés par le conseil de PCI).
Services de traitement de paiement, services de traitement/fournisseurs d'hébergement de commerce en ligne	Stocker, traiter ou transmettre les données du titulaire en votre nom. Ils peuvent également héberger et gérer votre serveur/site Internet de commerce en ligne et/ou développer votre site Internet et proposer l'assistance pour celui-ci.	Norme de sécurité des données PCI (PCI DSS)	Réclamer leur Attestation de conformité à la norme PCI DSS et demander si leur évaluation intégrait le service que vous utilisez. Le prestataire de services apparaît sur l'une de ces listes : MasterCard's List of Compliant Service Providers (Liste des prestataires de services conformes de MasterCard) Visa's Global Registry of Service Providers (Registre mondial des prestataires de services de Visa) Visa Europe's Registered Member Agents (Agents membres enregistrés de Visa Europe)
Fournisseurs de logiciels en tant que service (SaaS)	Développer, héberger et/ou gérer votre application de paiement ou votre application Web basée sur le cloud (par ex. application d'émission de tickets de caisse en ligne ou de réservation).	PCI DSS	Réclamer leur Attestation de conformité à la norme PCI DSS et demander si leur évaluation intégrait le service que vous utilisez. Le prestataire de services apparaît sur l'une de ces listes : MasterCard's List of Compliant Service Providers (Liste des prestataires de services conformes de MasterCard) Visa's Global Registry of Service Providers (Registre mondial des prestataires de services de Visa) Visa Europe's Registered Member Agents (Agents membres enregistrés de Visa Europe)
Intégrateurs/revendeurs	Installer en votre nom des applications de paiement conformes à la norme PA-DSS.	Revendeurs et intégrateurs qualifiés (QIR)	Demander si le fournisseur est un revendeur ou intégrateur qualifié (QIR) de PCI. Le fournisseur apparaît sur la List of PCI QIRs (Liste des QIR de PCI.)
Prestataires de services satisfaisant les exigences de la norme PCI DSS	Gérer/exploiter les systèmes ou services en votre nom (par ex. gestion du pare-feu, services de correctifs/ AV).	PCI DSS	Réclamer leur Attestation de conformité à la norme PCI DSS et demander si leur évaluation intégrait le service que vous utilisez. Le prestataire de services apparaît sur l'une de ces listes : MasterCard's List of Compliant Service Providers (Liste des prestataires de services conformes de MasterCard) Visa's Global Registry of Service Providers (Registre mondial des prestataires de services de Visa) Visa Europe's Registered Member Agents (Agents membres enregistrés de Visa Europe)

Questions

Le tableau ci-dessous contient une série de questions que les commerçants peuvent poser à leurs fournisseurs/prestataires de services, afin de déterminer si les mesures de contrôle appropriées sont en place pour protéger les données de carte.

QUESTION *Posée par le commerçant au fournisseur*	**RÉPONSE SOUHAITÉE DU FOURNISSEUR**	**ACTION RECOMMANDÉE** *Ajustée selon la réponse du fournisseur*
DE QUEL NIVEAU DE SÉCURITÉ VOTRE SOLUTION OU PRODUIT BÉNÉFICIE-T-IL ?		
1. Votre solution/produit assure-t-il une capture et un transfert sécurisés des données du titulaire ?	**Pour les transactions de paiement avec carte présente et en face à face :** **OUI** • Ici, vérifier si le terminal de paiement est un dispositif PTS approuvé par PCI : List of PCI Approved PTS Devices (Liste des dispositifs PTS approuvés de PCI) ET/OU • Ici, vérifier si l'application de paiement est une application conforme à la norme PCI PA-DSS : List of PCI PA-DSS of Validated Payment Applications (Liste des applications de paiement conformes à la norme PCI PA-DSS) OU • Ici, vérifier si la solution de cryptage est une solution P2PE conforme de PCI : List of PCI P2PE Validated Solutions (Liste des solutions P2PE conformes de PCI) **Pour les transactions de paiement avec carte absente (notamment commerce en ligne, commande par e-mail/téléphone) :** **OUI** • Ici, vérifier si l'application de paiement est une application conforme à la norme PCI PA-DSS : List of PCI PA-DSS of Validated Payment Applications (Liste des applications de paiement conformes à la norme PCI PA-DSS) OU • Ici, vérifier si le prestataire de services est un prestataire de services conforme à la norme PCI DSS : MasterCard's List of Compliant Service Providers (Liste des prestataires de services conformes de MasterCard) Visa's Global Registry of Service Providers (Registre mondial des prestataires de services de Visa) Visa Europe's Registered Member Agents (Agents membres enregistrés de Visa Europe)	Si la réponse est **NON**, posez la Question 2.

Questions

QUESTION *Posée par le commerçant au fournisseur*	RÉPONSE SOUHAITÉE DU FOURNISSEUR	ACTION RECOMMANDÉE *Ajustée selon la réponse du fournisseur*
DE QUEL NIVEAU DE SÉCURITÉ VOTRE SOLUTION OU PRODUIT BÉNÉFICIE-T-IL ? *suite*		
2. Notre accord avec vous (le fournisseur) inclut-il des clauses qui indiquent que vous maintiendrez la conformité à la norme PCI DSS pour votre produit/service (ou qu'il/elle deviendra conforme à la norme PCI DSS) ?	**OUI** Les fournisseurs avec des produits/solutions qui sont ou deviendront conformes à la norme PCI DSS doivent consentir à faire apparaître ce statut dans un accord écrit. Pour en savoir plus sur les preuves à rechercher concernant les produits/solutions conformes à la norme PCI DSS, reportez-vous à la Question 1 ci-dessus.	Si la réponse est **NON**, envisagez un autre fournisseur ou une autre solution.
3. Votre solution/produit stocke-t-il les données des cartes de paiement localement (sur le site de mon magasin/ma boutique) ?	**NON** Si oui, les commerçants peuvent envisager une solution de segmentation en unités ou de cryptage afin de mieux sécuriser les données de carte. Reportez-vous au *Guide de paiement sécurisé* pour en savoir plus sur le cryptage et la segmentation en unités.	Si la réponse est **OUI**, le commerçant doit vérifier avec le fournisseur que les données sont stockées conformément aux exigences de la norme PCI DSS. Si ce n'est pas le cas, envisagez un autre fournisseur.
4. Votre solution/produit protège-t-il les données des cartes de paiement avec un cryptage puissant ?	**OUI** Le cryptage est un moyen pour sécuriser les données, afin de limiter les risques de vol de données. Si vous le pouvez, choisissez une solution figurant sur la List of PCI P2PE Validated Solutions (Liste des solutions P2PE conformes de PCI). Ces solutions permettent de sécuriser les données de carte dès que vous les recevez et de les protéger lorsqu'elles circulent sur votre réseau.	Si la réponse est **NON**, envisagez un autre fournisseur ou une autre solution.

Questions

QUESTION *Posée par le commerçant au fournisseur*	RÉPONSE SOUHAITÉE DU FOURNISSEUR	ACTION RECOMMANDÉE *Ajustée selon la réponse du fournisseur*
DE QUEL NIVEAU DE SÉCURITÉ L'INSTALLATION DE MON PRODUIT BÉNÉFICIE-T-ELLE ?		
5. Si le fournisseur installe une application de paiement figurant sur la Liste des applications de paiement conformes du conseil de PCI, posez la question suivante : Êtes-vous un revendeur ou intégrateur qualifié (QIR) de PCI ?	**OUI** Un QIR est formé et qualifié par le conseil pour l'installation et l'intégration d'applications de paiement conformes à la norme PA-DSS. Leurs installations apportent la garantie que l'application de paiement conforme à la norme PA-DSS a été mise en place de manière à assurer votre conformité à la norme PCI DSS. Ici, vérifier si le fournisseur apparaît sur la liste : List of PCI QIRs (Liste des QIR de PCI).	Si la réponse est **NON**, posez les questions de suivi sur la gauche.
Questions de suivi si la réponse à la question ci-dessus est NON : Si l'application que le fournisseur installe n'est pas validée par PCI SSC, ou si le fournisseur n'est pas un QIR, posez la question suivante : • Proposez-vous une assistance pendant l'installation afin d'être sûrs que notre mise en place respecte les exigences de la norme PCI DSS ? • Fournissez-vous un guide de mise en place ? • Donnez-vous des conseils d'installation sur la façon de procéder pour s'assurer que les données de carte sont protégées où qu'elles soient stockées, traitées ou transférées ?	**OUI** Le fournisseur doit avoir des processus définis pour vous aider lors de l'installation de la solution, conformément aux exigences de la norme PCI DSS. Une installation inappropriée peut rendre la solution vulnérable aux incidents de sécurité des données. Vous réclamez une attestation auprès du fournisseur, expliquant comment il peut vous aider à vous assurer que les exigences de la norme PCI DSS sont ou peuvent être respectées pour le produit/la solution.	Si la réponse est **NON**, envisagez un autre fournisseur.

Questions

QUESTION *Posée par le commerçant au fournisseur*	RÉPONSE SOUHAITÉE DU FOURNISSEUR	ACTION RECOMMANDÉE *Ajustée selon la réponse du fournisseur*
METTEZ-VOUS À MA DISPOSITION UNE ASSISTANCE ET UNE MAINTENANCE CONTINUES POUR VOTRE PRODUIT/ SOLUTION ? SI OUI, COMMENT ?		
6. Votre solution/produit est-il installé sur mon réseau ou mes systèmes ?	**OUI** Le fournisseur doit proposer une maintenance et une assistance continues pour les mises à jour des logiciels et les correctifs de sécurité. De surcroît, il doit fournir et offrir une assistance pour les futures versions. Il est dans votre meilleur intérêt de demander aux fournisseurs de fournir une assistance complète pour leurs produits et de vous aider avec les installations/ correctifs, afin de s'assurer que tous les changements sur le système respectent les exigences de PCI.	Si la réponse est **OUI**, reportez-vous aux questions de suivi sur la gauche. Si la réponse est **NON**, passez à la Question 7.
Questions de suivi si la réponse à la question ci-dessus est OUI : • Installez-vous des correctifs et mises à jour sur le système/la solution ? • Faites-vous cela conformément aux exigences de la norme PCI DSS ? • Comment m'informez-vous ? Comment les correctifs sont-ils mis à disposition ? Et quelle assistance proposez-vous ?	**OUI** Si la solution n'est jamais mise à jour, elle peut devenir vulnérable aux futurs incidents de sécurité.	Si la réponse est **NON**, envisagez un autre fournisseur.
7. La solution est-elle installée sur des systèmes détenus et entretenus (hébergés) par le prestataire de services ?	**OUI** Ceci est considéré comme un service géré. Si le prestataire de services héberge la solution, réclamez leur Attestation de conformité à la norme PCI DSS et demandez si leur évaluation intégrait le service que vous utilisez.	Si la réponse est **OUI**, posez la question de suivi sur la gauche. Si la réponse est **NON** (c'est-à-dire que le service géré n'est pas conforme à la norme PCI DSS), envisagez une autre solution.
Question de suivi si la réponse à la question ci-dessus est **OUI** : L'environnement du prestataire de services est-il conforme à la norme PCI DSS ?	Vérifiez que le prestataire de services apparaît sur l'une de ces listes : MasterCard's List of Compliant Service Providers (Liste des prestataires de services conformes de MasterCard) Visa's Global Registry of Service Providers (Registre mondial des prestataires de services de Visa) Visa Europe's Registered Member Agents (Agents membres enregistrés de Visa Europe)	

Questions

QUESTION *Posée par le commerçant au fournisseur*	RÉPONSE SOUHAITÉE DU FOURNISSEUR	ACTION RECOMMANDÉE *Ajustée selon la réponse du fournisseur*
METTEZ-VOUS À MA DISPOSITION UNE ASSISTANCE ET UNE MAINTENANCE CONTINUES POUR VOTRE PRODUIT/ SOLUTION ? *suite*		
8. Avez-vous besoin d'un accès à distance à ma solution/mon système de paiement pour fournir l'assistance ?	**NON** L'accès à distance est souvent exploité dans les violations de données de paiement. La fonctionnalité d'accès à distance doit être limitée à une brève utilisation périodique et être désactivée le reste du temps.	Si la réponse est **NON**, passez à la Question 9. Si la réponse est **OUI**, posez les questions de suivi sur la gauche.
Questions de suivi si la réponse à la question ci-dessus est OUI : • Avez-vous besoin que l'accès à distance soit toujours actif ?	**NON** La fonctionnalité d'accès à distance doit être limitée à une brève utilisation périodique et être désactivée le reste du temps.	Si la réponse est **OUI** (c'est-à-dire si l'accès à distance doit toujours être actif), envisagez un autre fournisseur ou une autre solution.
• Quelles mesures prenez-vous pour sécuriser les connexions d'accès à distance ?	**Votre fournisseur doit utiliser une authentification à plusieurs facteurs ET une combinaison nom d'utilisateur/mot de passe différente pour chaque client auquel il accède.** Les connexions d'accès à distance peuvent être sécurisées via l'utilisation d'identifiants utilisateur et de mots de passe uniques pour chaque personne qui utilise le système. De plus, plusieurs méthodes de vérification de l'identité de la personne qui accède au système (authentification à plusieurs facteurs) doivent être utilisées. Les fournisseurs qui utilisent des noms d'utilisateur/mots de passe uniques pour chacun de leurs clients évitent qu'un incident de sécurité chez l'un de ses clients ne crée un incident de sécurité chez beaucoup ou tous ses autres clients lié à l'utilisation d'un nom d'utilisateur et d'un mot de passe communs.	Si le produit/la solution n'offre pas d'authentification à plusieurs facteurs pour l'accès à distance, envisagez une autre solution.
9. La solution/le produit doit-il être intégré à mes autres systèmes (par exemple, terminaux de paiement, créances ou autres systèmes contenant des données du titulaire) ?	**NON** Un terminal de paiement autonomes est plus facile à sécuriser qu'un système de paiement plus complexe qui peut avoir de nombreux systèmes connectés. Si la solution n'a pas besoin d'être intégrée aux autres systèmes, cela simplifie-t-il votre environnement de traitement et/ou comment cela apportera-t-il de la valeur à votre entreprise ? Vous devez vraiment avoir un grand intérêt commercial à effectuer une intégration, car utiliser une solution intégrée augmentera le champ d'application de la norme PCI DSS puisque cela agrandit et complexifie votre environnement de données du titulaire. MasterCard's List of Compliant Service Providers (Liste des prestataires de services conformes de MasterCard)	Si la réponse est **OUI**, envisagez un autre fournisseur ou produit, à moins que vous ayez vraiment un grand intérêt commercial à disposer d'une solution plus sophistiquée avec des connexions vers les autres systèmes.

Questions

QUESTION *Posée par le commerçant au fournisseur*	RÉPONSE SOUHAITÉE DU FOURNISSEUR	ACTION RECOMMANDÉE *Ajustée selon la réponse du fournisseur*
QUE SE PASSE-T-IL EN CAS DE VIOLATION DE DONNÉES ?		
10. En cas de violation des données et si votre solution/produit est impliqué : • Si je suis affecté, offrez-vous une assistance et une protection ? • Comment et quand m'informez-vous s'il y a une violation ? • Quel contrôle des violations de données et des activités suspicieuses proposez-vous ?	**OUI** Le fournisseur/prestataire de services doit proposer une assistance en cas de violation des données du titulaire. Le fournisseur/prestataire de services doit accepter de coopérer avec un investigateur en informatique légale, en cas de questions relatives à la solution ou au service géré qu'il propose. Le fournisseur/prestataire de services doit indemniser le commerçant s'il a reçu des amendes dans le cadre d'une violation et qu'il a été déterminé que la solution du fournisseur était la cause initiale du problème.	Si la réponse est **NON**, envisagez un autre fournisseur ou une autre solution.
11. Le fournisseur/prestataire de services propose-t-il une assurance pour couvrir les violations de données relatives à son produit/sa solution ?	**OUI** Avoir une assurance démontre que le fournisseur/prestataire de services a bien réfléchi à sa responsabilité et son imputabilité en cas de violations de données de carte. Si la réponse est **OUI**, demandez le champ d'application de la couverture et si votre mise en place sera couverte.	Si la réponse est **NON** (c'est-à-dire si le fournisseur ne propose pas d'assurance ou n'est pas d'accord de s'auto-assurer), envisagez de souscrire à votre propre assurance ou d'utiliser un autre fournisseur.
12. Le fournisseur/prestataire de services m'aide-t-il à informer mes clients en cas de violation de données et lorsque votre produit/solution est la cause initiale du problème ?	**OUI** Les fournisseurs/prestataires de services doivent être prêts à aider les commerçants à notifier une violation de données lorsque leur système de paiement est la cause initiale de la violation.	Si la réponse est **OUI**, posez les questions de suivi sur la gauche. Si la réponse est **NON** (c'est-à-dire si le fournisseur n'apporte pas son aide dans le processus de notification), vous devez développer un plan de notification et/ou envisager un autre fournisseur.
Si la réponse est **OUI**, à quel degré m'aiderez-vous dans le processus de notification ? • En couvrez-vous les coûts ? • Vous chargez-vous d'envoyer les notifications ? • Proposez-vous un contrôle des risques pour les clients impactés ?		