



Votre entreprise et la conformité aux normes du secteur des cartes de paiement

Votre entreprise et la conformité aux normes du secteur des cartes de paiement

Selon les Normes en matière de sécurité des données du secteur des cartes de paiement ou normes PCI-DSS, les commerçants qui acceptent les paiements par carte de crédit doivent protéger contre le vol d'identité les renseignements associés aux consommateurs utilisant ces cartes. Les entreprises du secteur des cartes de paiement, comme VISA, MasterCard et American Express, exigent dorénavant que les commerçants adhèrent à ces normes. Tout manquement à cet égard peut entraîner des amendes, des restrictions et même le retrait permanent du privilège d'accepter des cartes de crédit comme mode de paiement. Si le sort de votre entreprise dépend de l'utilisation des cartes de crédit par ses clients, vous n'avez pas le choix : vous devez vous conformer aux normes du secteur des cartes de paiement.

Dernièrement, Fusepoint a atteint le plus haut niveau de conformité aux normes du secteur des cartes de paiement s'adressant aux fournisseurs de services d'infogérance des commerçants de première catégorie. Nous sommes l'un des rares fournisseurs au Canada à avoir obtenu cette homologation. L'infrastructure et les normes de sécurité de Fusepoint répondent à une grande partie des exigences que les entreprises doivent respecter pour être jugées conformes aux normes du secteur des cartes de paiement. Les entreprises ont ainsi une mise de fonds moins importante à faire au départ et se libèrent d'une partie des lourdes tâches à accomplir pour pouvoir être jugées conformes. De plus, une fois qu'un client a pu démontrer sa conformité aux normes du secteur des cartes de paiement, les experts hautement compétents de Fusepoint lui fournissent les services nécessaires, comme la surveillance 24 heures sur 24, pour maintenir cette conformité.

FAQ sur la conformité aux normes du secteur des cartes de paiement – Les 10 questions les plus courantes

- 1. Qui a créé les Normes en matière de sécurité du secteur des cartes de paiement?**
- 2. Quelles sont les exigences rattachées aux Normes en matière de sécurité des données du secteur des cartes de paiement?**
- 3. Comment sont définis les niveaux des commerçants?**
- 4. Quels avantages y a-t-il à avoir recours à un fournisseur de services qui respecte les Normes en matière de sécurité des données du secteur des cartes de paiement?**
- 5. Qui doit se conformer aux Normes en matière de sécurité des données du secteur des cartes de paiement?**
- 6. Que dois-je faire pour me conformer aux Normes en matière de sécurité des données du secteur des cartes de paiement?**
- 7. À quelles vérifications dois-je me soumettre?**
- 8. De quoi est responsable mon fournisseur de services d'infogérance?**
- 9. Combien coûte l'attestation de conformité aux normes du secteur des cartes de paiement?**
- 10. Où se situent le plus souvent les problèmes de non-conformité aux normes du secteur des cartes de paiement?**

¹PCI-DSS est l'abréviation de « *Payment Card Industry Data Security Standard* », dont la traduction française officielle est « Normes en matière de sécurité des données du secteur des cartes de paiement ». On a employé le pluriel « normes » en français.

1. Qui a créé les Normes en matière de sécurité du secteur des cartes de paiement?

Les Normes en matière de sécurité du secteur des cartes de paiement ont été élaborées conjointement par de grandes sociétés émettrices de cartes de crédit, parmi lesquelles se trouvent Visa, MasterCard, Discover et American Express. Ces normes visent à établir des politiques et des règles de sécurité minimale pour protéger l'information sur les comptes de titulaire carte de crédit ainsi que sur les transactions.

2. Quelles sont les exigences rattachées aux Normes en matière de sécurité des données du secteur des cartes de paiement?

Les Normes en matière de sécurité des données du secteur des cartes de paiement constituent un ensemble uniforme de normes de sécurité que doivent appliquer les commerçants et les administrateurs de paiements par carte de crédit qui stockent, traitent ou transmettent des données sur les titulaires de carte dans le but d'effectuer des opérations de paiement. Le cadre constitué par ces normes prévoit des mécanismes de sécurité rigoureux définis sous la forme de 12 exigences principales visant le contrôle administratif et la sécurité physique et technique.

Voici les principes et les exigences rattachés aux normes du secteur des cartes de paiement ainsi que les services et les méthodes déployés par Fusepoint pour s'y conformer.

Exigences du secteur des cartes de paiement	Services et méthodes de Fusepoint
<p>Établir et gérer un réseau sécurisé</p> <ol style="list-style-type: none"> 1. Installer et gérer un coupe-feu pour protéger les données des titulaires de carte. 2. Ne pas utiliser les mots de passe et les autres paramètres de sécurité de système définis par les fabricants. 	<ul style="list-style-type: none"> • Établissement de normes adéquates pour les coupe-feux. • Modèle de sécurité à liste blanche, qui autorise uniquement le passage des données dument autorisées, sur les connexions entrantes et sortantes. • Paramétrage sécurisé de tous les composants réseau. • Procédure établie de gestion des changements. • Documentation comprenant des diagrammes. • Utilisation des logiciels Opware pour surveiller les changements, le matériel et les logiciels, pour repérer les vulnérabilités et pour synchroniser les fichiers de paramétrage. • Séparation des tâches. • Vérifications internes du dispositif de sécurité. • Masquage d'adresses IP. • Coupe-feu personnel intégré. • Paramétrage sécurisé prédéfini et éprouvé de tous les composants de système. • Utilisation des logiciels Opware pour automatiser les services et vérifier périodiquement la conformité. • Réseau dédié et isolé de gestion de tous les composants de réseau
<p>Protéger les données des titulaires de carte</p> <ol style="list-style-type: none"> 3. Protéger les données stockées des titulaires de carte. 4. Crypter les données des titulaires de carte transmises par les réseaux publics ouverts. 	<ul style="list-style-type: none"> • Cryptage des données sauvegardées. • Cryptage des données sur disque. • Réseau privé virtuel de site à site et de client à site.
<p>Mettre en œuvre un programme de gestion de la vulnérabilité</p> <ol style="list-style-type: none"> 5. Utiliser et mettre à jour régulièrement un logiciel antivirus. 6. Développer et gérer des applications et des systèmes sécurisés 	<ul style="list-style-type: none"> • Programme établi de gestion des logiciels. • Utilisation des logiciels Opware pour produire des rapports de conformité et installer les rustines. • Procédure établie de gestion des changements. • Réduction au minimum de la quantité de services activés dans les systèmes.

Exigences du secteur des cartes de paiement	Services et méthodes de Fusepoint
<p>Appliquer des mesures de contrôle d'accès efficaces</p> <p>7. Limiter l'accès aux données des titulaires de carte aux cas de nécessité professionnelle absolue.</p> <p>8. Attribuer un identifiant particulier à chaque utilisateur d'un système informatique.</p> <p>9. Limiter l'accès physique aux données des titulaires de carte</p>	<ul style="list-style-type: none"> Séparation des tâches. Authentification à deux facteurs. Politique stricte de gestion des mots de passe. Centres informatiques de première classe Politique stricte concernant les visiteurs. Télévision en circuit fermé. Services d'entreposage externe de concert avec la société Iron Mountain Vérifications régulières des stocks de supports de données. Politique établie d'élimination des supports de données.
<p>Surveiller et tester régulièrement les réseaux</p> <p>10. Surveiller tous les accès aux ressources du réseau et aux données des titulaires de carte.</p> <p>11. Tester régulièrement les systèmes et les mécanismes de sécurité.</p>	<ul style="list-style-type: none"> Surveillance en temps réel 24 heures sur 24, par le personnel, de tous les événements système. Politiques de conservation des journaux (7 ans). Vérifications internes régulières. Évaluation de la vulnérabilité de l'infrastructure. Tests de pénétration de l'infrastructure. Surveillance de l'ensemble des données circulant sur les segments publics de réseau. Surveillance de l'ensemble des données circulant sur les segments privés de réseau. Vérifications de l'intégrité des fichiers.
<p>Établir une politique de sécurité de l'information</p> <p>12. Établir une politique régissant la sécurité de l'information</p>	<ul style="list-style-type: none"> Politique de sécurité établie. Programme de sensibilisation. Vérification des antécédents de tout le personnel technique.

3. Comment sont définis les niveaux des commerçants?

Les commerçants sont classés par niveau selon principalement le nombre de transactions effectuées sur une période de 12 mois.

Niveau du commerçant*	Description
1	Commerçant réalisant plus de 6 000 000 de transactions par année ou dont le système informatique a subi une atteinte à la sécurité ayant compromis des données de titulaire de carte.**
2	Commerçant réalisant de 1 000 000 à 6 000 000 de transactions par année.
3	Commerçant réalisant de 20 000 à 1 000 000 de transactions électroniques par année.
4	Commerçant réalisant moins de 20 000 transactions électroniques par année ou réalisant moins de 1 000 000 de transactions au total par année.

* Nouvelles définitions des niveaux des commerçants en vigueur depuis le 18 juillet 2006.

** Tout commerçant dont le système informatique a subi un piratage ayant compromis des données de titulaire de carte est susceptible d'être classé à un niveau supérieur.

4. Quels avantages y a-t-il à avoir recours à un fournisseur de services qui respecte les Normes en matière de sécurité des données du secteur des cartes de paiement?

En ayant recours à un fournisseur de services qui respecte les Normes en matière de sécurité des données du secteur des cartes de paiement, vous vous assurez que les données des titulaires de carte qui sont traitées par vos systèmes informatiques seront protégées. Ces normes sont conçues pour protéger les titulaires de carte et réduire au minimum les risques pour votre entreprise. Voici les principaux avantages, pour votre entreprise, de la mise en œuvre de ces normes et du recours à un fournisseur de services d'infogérance homologué :

- Protection des données personnelles des clients.
- Amélioration de la confiance des clients envers une entreprise lorsqu'ils constatent sa volonté de protéger les données personnelles.
- Protection de l'entreprise contre les sanctions financières.
- Mise à profit de l'investissement déjà fait par un fournisseur de services d'infogérance pour se conformer aux Normes en matière de sécurité des données du secteur des cartes de paiement. Ainsi, votre infrastructure informatique est hébergée dans un centre informatique ayant déjà réussi les épreuves de conformité.
- Économies potentielles de 100 000 \$ ou plus en dépenses d'immobilisation lorsqu'on externalise les systèmes de traitement des paiements par carte de crédit pour les confier à un fournisseur de services homologué par le secteur des cartes de paiement.

5. Qui doit se conformer aux Normes en matière de sécurité des données du secteur des cartes de paiement??

Tout commerçant ou administrateur de paiements par carte de crédit qui stocke, traite ou transmet des données sur les titulaires de carte de crédit doit se conformer aux Normes en matière de sécurité des données du secteur des cartes de paiement, quel que soit son volume de transactions. Cette obligation s'applique à toute personne physique ou morale, quelle que soit la taille de l'entreprise. Selon les experts, le piratage informatique vise de plus en plus les petits sites Web commerciaux « parce que les pirates s'aperçoivent que ces sites ne sont pas aussi bien protégés que ceux des grandes entreprises ». La conformité aux Normes en matière de sécurité des données du secteur des cartes de paiement est une affaire sérieuse. Tout manquement à cet égard pourrait entraîner des amendes et d'autres sanctions sévères et pourrait ternir la réputation de l'entreprise, ce qui nuirait à la fidélité de la clientèle.

6. Que dois-je faire pour me conformer aux Normes en matière de sécurité des données du secteur des cartes de paiement?

L'attestation de conformité aux normes du secteur des cartes de paiement s'obtient en remplissant deux conditions suivantes:

1. Prouver chaque trimestre sa conformité en se soumettant à un contrôle à distance de la vulnérabilité effectué par un contrôleur indépendant désigné officiellement par Visa et MasterCard. Chaque connexion Internet doit être contrôlée, qu'elle relie à l'Internet un réseau d'entreprise, qu'elle permette de relier un appareil distant à un réseau d'entreprise (par ligne téléphonique traditionnelle, ligne d'abonné numérique, câble ou liaison sans fil) ou qu'elle relie en permanence à l'Internet des serveurs comme un serveur Web ou un serveur de courriel.
2. Obtenir un résultat satisfaisant dans une autoévaluation de la sécurité effectuée en répondant à un questionnaire précis sur les pratiques internes qui assurent la sécurité des sites Web et des bureaux.

7. À quelles vérifications dois-je me prêter?

Les commerçants de niveau 1 doivent se soumettre à une vérification de la sécurité sur place une fois l'an et à un contrôle de la vulnérabilité du réseau chaque trimestre. Les commerçants de niveau 2, 3 ou 4 doivent répondre à un questionnaire d'autoévaluation une fois l'an et se soumettre à un contrôle de la vulnérabilité du réseau chaque trimestre.

8. De quoi est responsable mon fournisseur de services d'infogérance?

Les fournisseurs de services d'infogérance homologués par le secteur des cartes de paiement relativement aux Normes en matière de sécurité des données sont responsables de protéger chaque système hébergé, notamment en s'assurant que les gens ont accès uniquement aux données de leurs propres clients, en consignait adéquatement les pistes de vérification dans des journaux et en prévoyant les moyens qui permettront d'enquêter dans les meilleurs délais si l'intégrité d'un système est compromise. L'expertise relative au secteur des cartes de crédit doit être un facteur déterminant lorsque vient le temps de choisir un fournisseur de services d'infogérance.

9. Combien coûte l'attestation de conformité aux normes du secteur des cartes de paiement?

Trois types de dépenses doivent entrer en ligne de compte dans toute analyse des coûts en vue de se conformer aux normes du secteur des cartes de paiement.

1. Dépenses initiales pour atteindre la conformité : Ces dépenses varient selon divers facteurs, notamment le type d'entreprise, le nombre de transactions que l'entreprise effectue chaque année, les caractéristiques de ses systèmes informatiques et ses pratiques courantes en matière de stockage. Le tableau ci-dessous indique les dépenses initiales telles qu'estimées par le groupe Gartner.

Niveau du commerçant	Dépenses d'évaluation de l'étendue des travaux à réaliser	Dépenses pour atteindre la conformité
Niveau 1	125 000 \$	568 000 \$
Niveau 2	105 000 \$	267 000 \$
Niveau 3	44 000 \$	81 000 \$
Niveau 4	Dépenses variant beaucoup selon le type d'entreprise.	

2. Dépenses de maintien de la conformité : achat et maintenance d'équipement et de logiciels; achat de licences; ressources humaines hautement spécialisées pour la gestion technique et la surveillance en tout temps, conformément aux exigences.
3. Dépenses de non-conformité : Des sanctions financières de 10 k\$ à 100 k\$ par mois sont prévues depuis le 1er octobre 2006 contre tout commerçant fautif. En cas d'atteinte à la sécurité d'un système, des restrictions peuvent être imposées au commerçant, et ces restrictions peuvent aller jusqu'à une interdiction totale de prendre part aux programmes des sociétés émettrices de carte de crédit. Compte tenu de la violation de la confidentialité découlant d'une pareille atteinte, celle-ci entraîne une perte de confiance de la part des consommateurs à l'égard du commerçant, qui voit ainsi son nom et ses marques de commerce ternies à un degré tel que le préjudice risque d'être irréparable.

Lorsque vous confiez votre infrastructure technique à un fournisseur de services d'infogérance qui a déjà fait les investissements pour se conformer aux Normes en matière de sécurité des données du secteur des cartes de paiement, vos systèmes se trouvent d'ores et déjà à être hébergés dans des centres informatiques ayant reçu les attestations nécessaires, ce qui garantit la protection de l'information traitée par vos systèmes sur les comptes de titulaire de carte de crédit et vous permet de réduire de beaucoup vos dépenses en immobilisations.

10. Où se situent le plus souvent les problèmes de non-conformité aux normes du secteur des cartes de paiement?

Selon Forrester Research, les 3 principales causes de non-conformité sont les suivantes:

1. Gestion de l'accès inadéquate (ce qui signifie que des faiblesses existent dans le contrôle de l'accès électronique, a gestion des identifiants ou la sécurité physique);
2. Surveillance et mise à l'épreuve insuffisantes (ce qui signifie que des faiblesses existent dans les systèmes et les méthodes de surveillance et de mise à l'épreuve);
3. gestion de l'infrastructure inadéquate (ce qui signifie que des faiblesses existent dans les antivirus, les coupe-feux ou le paramétrage des systèmes).

Pour en savoir davantage, consultez notre site Web à
www.fusepoint.com/francais ou composez le 1.888.664.9001