

Compliance Requirements

Avoiding risk and seeking compliance — your guide to understanding your responsibility under the Payment Card Industry Data Security Standards (PCI DSS).

PCI Frequently Asked Questions

Does PCI DSS apply to me?

Yes. It applies to all entities that store, transmit or process cardholder data regardless of whether payment is received online, by mail/ telephone orders or face-to-face. It also applies to any network component, server or application included in, or connected to, your cardholder environment.

Why must I go through the compliance process?

There are several reasons for compliance. Below are just a few:

- Avoiding loss of your customers' trust and loyalty.
- Identifying and addressing your vulnerabilities.
- Protecting your customers' sensitive data.
- Fines from the payment brands can cost up to \$50,000 per month and/or egregious fines of up to \$500,000.

What is required become PCI DSS compliant?

The Chase Paymentech Payment Brand Data Security information web page at www.chasepaymentech.ca, under "Merchant Support"; "PCI Data Security Standards" is your first stop in learning about requirements.

How do I know if my payment application is compliant?

Go to the Chase Paymentech PCI Data Security Standards page (listed above), click on the "Chase Paymentech Data Security" link, and then click on "Securing Your Customer's Cardholder Data." Alternatively, go to: www.pcisecuritystandards.org, click on "Security Standards" and choose "PA-DSS". View the listing of Validated Payment Applications and other supporting documents.

Is Chase Paymentech compliant?

Yes, and we will continue to be compliant with the PCI DSS. In 2007, we were named an inaugural member of the PCI Security Standard Council (PCI SSC) Board of Advisors.

How can I find out if I am at risk?

You can go to our free Risk Profiler at <http://chasecanada.riskprofiler.net> and answer a brief questionnaire to determine your risk of having customer credit card data stolen from your computers. There is no charge for Chase Paymentech merchant clients to go through the Risk Profiler. Simply visit <http://chasecanada.riskprofiler.net> and enter CHASECANADA08TKR in the enrollment code field under "Are you at risk?" to get started.

How can I validate compliance?

Chase Paymentech has arranged preferential pricing with Trustwave (www.trustwave.com). Trustwave's compliance solution is a simple, cost-effective method for validating compliance with the PCI DSS, for all the major payment brands' security programs. Simply go to <http://chasecanada.riskprofiler.net> and enter CHASECANADA08TKR in the enrollment code field under "Are you at risk?" and then click on "Start Risk Profiler".

Once I become compliant, how long am I considered compliant and what are the compliance deadlines?

All merchants are required to maintain compliance at all times. Please refer to the table in our Alert for current requirements by Merchant level. You may view the full Alert and the accompanying chart at: www.chasepaymentech.ca, under "Merchant Support"; "PCI Data Security Standards" and click on "Chase Paymentech Alert."

Your Responsibility, Security and Accountability

Providing customers a secure way to pay is more than just good business — it's a requirement. Fulfilling appropriate requirements helps merchants avoid security compromises for which they could be held liable. The fact is, non-compliance fines and related liability could cost you thousands of dollars.

To help, the major payment brands established the Payment Card Industry Data Security Standards (PCI DSS) aligning Visa Canada's AIS, MasterCard's SDP and other payment brands' cardholder data security program requirements. Chase Paymentech has created this guide to help you understand your responsibilities.

For more detailed information, please see our Alert at: www.chasepaymentech.ca, under "Merchant Support"; "PCI Data Security Standards" and click on "Chase Paymentech Alert."

For more information about how you can ensure your PCI compliance, please contact your Relationship Manager or contact Chase Paymentech Merchant Support at 1.800.265.5158.

Exigences relatives à la conformité

Éviter le risque et atteindre la conformité – votre guide de la compréhension de vos responsabilités dans le cadre des Payment Card Industry Data Security Standards (Normes de sécurité des données du secteur des cartes de paiement ou norme PCI DSS).

Foire aux questions relatives à PCI

La norme PCI DSS s'applique-t-elle à moi?

Oui. Elle s'applique à toutes les entités qui stockent, transmettent ou traitent les données de titulaires de cartes, que le paiement soit reçu en ligne, par commande postale ou téléphonique ou en personne. Elle s'applique aux composants de réseau, aux serveurs et aux applications faisant partie de votre environnement applicables aux titulaires de cartes ou qui y sont reliés.

Pourquoi dois-je suivre la procédure de conformité?

Il y a plusieurs raisons de se conformer à la norme. En voici quelques-unes :

- Éviter de perdre la confiance et la loyauté de vos clients.
- Trouver vos vulnérabilités et y remédier.
- Protéger les données sensibles de vos clients.
- Les amendes imposées par les marques de cartes de paiement peuvent aller jusqu'à 50 000 \$ par mois ou atteindre le niveau énorme de 500 000 \$, ou les deux.

Que faut-il faire pour devenir conforme à la norme PCI DSS?

La page Web sur la sécurité des informations de Chase Paymentech, que vous trouverez à l'adresse www.chasepaymentech.ca, en cliquant sur « Soutien aux commerçants » puis sur « Normes sécurité des données du SCP » constitue votre première étape pour vous renseigner sur ces exigences.

Comment savoir si mon application de paiement respecte la norme?

Rendez-vous à la page de Normes de sécurité des données du SCP de Chase Paymentech (indiquée ci-dessus) et cliquez sur le lien « Chase Paymentech Sécurité des données », puis sur « La protection des données de titulaires de cartes de vos clients. » Alternativement, rendez à l'adresse : www.pcisecuritystandards.org, cliquez sur « Normes de sécurité » et choisissez « PA-DSS ». Consultez la liste des applications de paiement validées et les autres documents pertinents.

Chase Paymentech est-elle conforme à la norme?

Oui, et nous continuerons d'être conformes à la norme PCI DSS. En 2007, nous avons été nommés parmi les premiers membres du comité consultatif du Conseil des normes de sécurité du secteur des cartes de paiement (PCI SSC).

Comment savoir si je suis vulnérable?

Vous pouvez consulter notre Risk Profiler gratuit à l'adresse <http://chasecanada.riskprofiler.net> et répondre à un bref questionnaire afin de déterminer le risque que les données liées aux cartes de crédit de vos clients soient piratées à partir de vos ordinateurs. L'utilisation du Risk Profiler est gratuite pour les commerçants qui sont des clients de Chase Paymentech. Il suffit de vous rendre à l'adresse <http://chasecanada.riskprofiler.net> et de saisir

CHASECANADA08TKR dans le champ code d'inscription, dans la section « Avez-vous risque pour la sécurité? » pour commencer.

Comment puis-je valider ma conformité?

Chase Paymentech a prévu des tarifs privilégiés avec Trustwave (www.trustwave.com). La solution de conformité de Trustwave est une méthode simple et économique pour valider la conformité avec la norme PCI DSS des programmes de sécurité de toutes les marques de cartes de paiement majeures. Il suffit de vous rendre à l'adresse <http://chasecanada.riskprofiler.net> et de saisir CHASECANADA08TKR dans le champ code d'inscription, dans la section « Avez-vous risque pour la sécurité? » puis de cliquer sur « Commencer Risk Profiler ».

Une fois conforme, pendant combien de temps suis-je considéré comme étant conforme et quels sont les échéanciers relatifs à la conformité?

Tous les commerçants doivent respecter la norme en tout temps. Veuillez consulter le tableau dans notre Alerte pour obtenir les exigences actuelles selon le niveau de commerçant. Vous pouvez consulter l'Alerte complète et le tableau qui l'accompagne à l'adresse www.chasepaymentech.ca, en cliquant sur « Soutien aux commerçants » puis sur « Normes sécurité des données du SCP » puis « Alerte de Chase Paymentech. »

Votre responsabilité, sécurité et responsabilisation

Fournir à vos clients une façon sûre de payer n'est pas seulement bon pour vos affaires : c'est une nécessité. Répondre aux exigences appropriées aide les commerçants à éviter des compromissions de la sécurité dont ils pourraient être tenus responsables. Les amendes pour non-conformité et les obligations en découlant pourraient vous coûter des milliers de dollars.

Pour vous aider, les marques de carte de paiement majeures ont établi les Normes de sécurité des données du secteur des cartes de paiement (norme PCI DSS) qui font correspondre les exigences des programmes SIC de Visa Canada, SDP de MasterCard et les exigences des programmes de sécurité des données de titulaires de cartes des autres marques de cartes de paiement. Chase Paymentech a créé ce guide pour vous aider à comprendre vos responsabilités.

Pour en savoir plus, veuillez consulter notre Alerte à l'adresse www.chasepaymentech.ca, en cliquant sur « Soutien aux commerçants » puis sur « Normes sécurité des données du SCP », puis « Alerte de Chase Paymentech. »