

A decorative graphic consisting of two overlapping, curved shapes. The top shape is orange and the bottom shape is blue, both pointing towards the right. They are positioned to the right of the main title.

# Sécurité de l'information concernant les comptes

Guide du marchand



Chez Visa, la protection des titulaires de carte est au cœur même de toutes nos activités. La confiance envers notre marque s'explique entre autres choses par le fait que nous améliorons la sécurité des achats et des ventes. Nous reconnaissons aussi que la protection des renseignements des titulaires de carte est essentielle au succès des marchands partout dans le monde. C'est pourquoi la sécurité du système de paiement est une priorité constante chez Visa. Notre objectif est de restreindre le crime en le rendant plus difficile à commettre.

## ENGAGEMENT DE VISA ENVERS LA PROTECTION DES TITULAIRES DE CARTE

La croissance de l'utilisation des cartes se traduit par le traitement et le stockage d'une plus grande quantité de renseignements sur les comptes par les marchands et les fournisseurs de service. Afin de protéger l'intégrité des données des titulaires de carte, toutes ces entités doivent demeurer vigilantes lorsqu'il s'agit de sauvegarder des données de nature délicate. Visa s'est engagée à soutenir les institutions financières, les marchands et leurs mandataires en s'assurant que nous travaillons tous ensemble pour conserver un système de paiement sécuritaire et fiable.

Visa s'est engagée à protéger de façon soutenue l'intégrité de l'information concernant les transactions et les comptes Visa®. Le programme Sécurité de l'information concernant les comptes, lancé en 2000, est conçu pour protéger l'information concernant les transactions et les comptes Visa et préserver à la fois l'intégrité des transactions et l'achalandage des titulaires de carte.

Les marchands et les fournisseurs de service qui mettent en oeuvre les mesures de contrôle de ce programme peuvent en bénéficier de nombreuses façons. Si elles sont appliquées de manière adéquate et uniforme, elles peuvent aider les marchands à :

- **SE DOTER** d'un avantage concurrentiel;
- **ACCROÎTRE** leurs revenus et améliorer leurs résultats;
- **CONSERVER** une image favorable;
- **SUSCITER** la confiance des consommateurs.

## AVANTAGES POUR LES MARCHANDS

Visa aide à instaurer la confiance des consommateurs et à augmenter les revenus en fournissant aux marchands des outils pour les aider à prévenir la fraude et, notamment, à :

- protéger l'intégrité de leur marque et instaurer la confiance des consommateurs en respectant de hauts niveaux de conformité aux normes de l'industrie;
- réduire le nombre de différends avec les titulaires de carte et ainsi augmenter le nombre de ventes ayant des répercussions favorables sur les résultats;

- améliorer la sensibilisation et les connaissances en matière de sécurité des données et aider les marchands à renforcer les mesures de sécurité afin de réduire au minimum la possibilité de bris de sécurité des données;
- réduire au minimum le risque de compromission et de perte de données en cas de bris de sécurité;
- accéder à l'information portant sur les pratiques exemplaires de l'industrie et les services de *Visa*, tels les bulletins sur la sécurité.

## IL EST RENTABLE D'ASSURER LA SÉCURITÉ DES DONNÉES

Le renforcement de la sécurité est à l'avantage de tous. La protection des données est un bon investissement. Il peut être difficile d'évaluer le rendement du capital investi en matière de sécurité, étant donné qu'il n'a aucun effet direct sur les résultats. Cependant, le fait de *ne pas* assurer la sécurité des données peut se traduire en un coût beaucoup plus élevé. Un marchand qui a subi un bris de sécurité des données en connaît les lourdes conséquences :

- pertes financières;
- réputation entachée;
- risques juridiques;
- perte d'occasions d'affaires imputable à un manque de confiance;
- temps d'arrêt découlant d'un bris de sécurité des données;
- possibilité d'amendes, de pénalités, de frais ou d'une annulation de service;
- coût de l'examen judiciaire.

*Visa* s'est mise à l'écoute des besoins des marchands pour élaborer un programme pratique et complet qui aide à protéger l'information de nature délicate concernant les transactions *Visa* — le programme SIC.

## QU'EST-CE QUE LE PROGRAMME SIC?

Le programme Sécurité de l'information concernant les comptes est un programme de validation de la conformité, conçu pour aider quiconque conserve, transmet ou traite les données concernant les comptes *Visa* — institutions financières, marchands, acquéreurs et sociétés de traitement — à évaluer si les données des titulaires de carte sont protégées au sein de leur organisation. Il repose sur des normes, méthodologie éprouvée qui permet aux organisations d'améliorer leur niveau de sécurité afin de respecter ou d'excéder les normes de l'industrie.



Que les données se trouvent sur un serveur autonome ou sur le site Web d'un marchand, le programme SIC protège les données à tous les points du système de paiement.

Le programme SIC aide les marchands à évaluer et à améliorer leurs contrôles organisationnels, physiques et logiques en matière de sécurité des données et est obligatoire pour tous les marchands acceptant la carte *Visa*. Les normes du programme SIC portent entre autres sur les opérations cryptographiques, les contrôles d'accès logique, la protection des données physiques et la sécurité du réseau.

Tous les marchands qui ont accès à l'information concernant les données des comptes ou qui la conservent doivent le faire de façon sécuritaire, conformément à la *Norme de sécurité des données du secteur des cartes de paiement* (SCP). De plus, en participant à ce programme, les marchands ont accès en temps opportun à l'information et aux pratiques exemplaires en matière de sécurité des données.

## COMMENT LE PROGRAMME SIC ET SCP FONCTIONNENT-ILS ENSEMBLE?

Pour se conformer au programme SIC, les marchands et les fournisseurs de service doivent adhérer à la *Norme de sécurité des données du SCP*. Cette norme est le fruit d'une collaboration entre Visa et MasterCard et est conçue pour créer des exigences sectorielles communes en matière de sécurité. Le programme SIC exige que les marchands et les autres entités qui sont en contact avec les données de nature délicate des titulaires de carte se conforment à la *Norme de sécurité des données du SCP* et valident cette conformité selon le cadre de mise en œuvre du programme SIC.

La *Norme de sécurité des données du SCP* est constituée de 12 exigences de base. Pour obtenir de l'information plus détaillée sur ces exigences ou télécharger une version PDF de cette norme, visitez [www.visa.ca/sic](http://www.visa.ca/sic).



### **Établir et maintenir un réseau sécuritaire**

1. Installer et maintenir une configuration de pare-feu pour protéger les données.
2. Ne pas utiliser les paramètres par défaut du fournisseur dans le cas des mots de passe du système et des autres paramètres de sécurité.

### **Protéger les données des titulaires de carte**

3. Protéger les données stockées.
4. Chiffrer la transmission des données des titulaires de carte et des informations confidentielles par le biais des réseaux publics.

### **Maintenir un programme de gestion de la vulnérabilité**

5. Utiliser et mettre régulièrement à jour un logiciel antivirus.
6. Développer et maintenir des systèmes et des applications sécuritaires.

### **Mettre en place de solides mesures de contrôle de l'accès**

7. Restreindre l'accès aux données confidentielles des titulaires de carte aux personnes qui ont besoin de les connaître.
8. Attribuer un code d'utilisateur exclusif à chaque personne ayant accès à l'ordinateur.
9. Restreindre l'accès physique aux données des titulaires de carte.

## Surveiller et tester régulièrement les réseaux

10. Assurer un suivi et une surveillance de tout accès aux ressources du réseau et aux données des titulaires de carte.
11. Tester régulièrement les systèmes et les processus de sécurité.

## Maintenir une politique de sécurité de l'information

12. Maintenir une politique en matière de sécurité de l'information.

## LE PROGRAMME SIC ME CONCERNE-T-IL?

Tous les marchands qui participent au processus de paiement *Visa* doivent se conformer à la *Norme de sécurité des données du SCP*. Cette norme est le fondement du programme SIC.

Les exigences en matière de validation de la conformité du programme SIC reposent sur le volume de transactions traitées par un marchand et, par conséquent, sur le risque de compromission qu'il représente pour le système *Visa*.

Les acquéreurs sont responsables de déterminer le niveau des exigences en matière de validation de la conformité de leurs marchands. Chaque marchand se situe à l'un des quatre niveaux, selon son volume annuel de transactions *Visa*. Visitez [www.visa.ca/sic](http://www.visa.ca/sic) pour obtenir plus d'information sur les définitions des niveaux de marchands.

*Visa* et votre acquéreur peuvent vous aider à trouver le moyen le plus efficace et le plus rentable d'être conforme au programme SIC. Un évaluateur indépendant qualifié autorisé par *Visa* peut vous guider à travers ce processus, diminuer les conjectures et réduire le temps requis pour assurer la conformité. Il peut gérer le processus de conformité directement avec le marchand au nom de l'acquéreur, et assurer la confidentialité. Communiquez avec votre acquéreur ou visitez [www.visa.ca/sic](http://www.visa.ca/sic) pour obtenir plus d'information sur les évaluateurs indépendants qualifiés autorisés par *Visa*.



## COMMENT PUIS-JE M'INSCRIRE?

La conformité au programme SIC peut inclure une partie ou la totalité des éléments suivants, selon le volume de transactions du marchand.

1. Inscription en ligne
2. Questionnaire d'auto-évaluation à remplir en ligne
3. Évaluation à distance de la vulnérabilité des systèmes du marchand par un évaluateur indépendant qualifié en matière de sécurité
4. Un examen sur place
5. Rapport final de conformité en ligne de l'évaluateur indépendant qualifié en matière de sécurité
6. Plan de mesures correctives

Les marchands de tous les niveaux — qu'ils exercent leurs activités dans un endroit physique, par commerce électronique ou par commande téléphonique ou commande postale (CTCP) — doivent s'inscrire auprès d'un évaluateur indépendant qualifié en matière de sécurité, remplir un questionnaire d'auto-évaluation annuel et effectuer un scan trimestriel de leur réseau, lequel doit être validé par un évaluateur indépendant qualifié en matière de sécurité. Pour respecter les exigences du programme SIC de Visa, certains marchands doivent aussi effectuer une évaluation sur place de la sécurité des données de l'industrie des cartes de paiement, laquelle doit démontrer qu'ils respectent les normes sectorielles dans le cadre de la conformité au programme SIC.

Pour obtenir plus d'information sur les exigences de conformité et le processus de validation, visitez [www.visa.ca/sic](http://www.visa.ca/sic).

La confiance du consommateur est longue à acquérir et peut se perdre du jour au lendemain.

### « EXONÉRATION » : PROTECTION DE LA CONFORMITÉ

Si Visa juge un marchand conforme au programme SIC, il sera « exonéré » de toute amende, de tous frais ou de toute pénalité de la part de Visa Canada s'il est victime de piratage ou de compromission. Ceci s'applique à tout marchand qui a validé sa conformité au programme SIC selon le cadre de mise en œuvre du programme et qui

a été jugé conforme, après une enquête judiciaire par un évaluateur indépendant qualifié autorisé par Visa, au moment du bris de sécurité des données.

## NIVEAUX DE PROTECTION

### TRAVAILLONS ENSEMBLE : LA SÉCURITÉ EST LA RESPONSABILITÉ DE TOUS

Visa et les institutions financières émettrices de la carte *Visa* reconnaissent que la dépendance des entreprises envers la technologie ne cesse d'augmenter à un rythme croissant et que le risque de bris de sécurité augmente de jour en jour. Visa s'est engagée à travailler avec les marchands pour assurer la sécurité de tout le système de paiement *Visa*.

Grâce à des investissements importants en technologie et aux efforts concertés de Visa et de ses partenaires, tels les marchands, l'incidence de la fraude contre le système *Visa* est demeurée peu élevée, même si le volume des transactions par carte *Visa* a énormément augmenté. La technologie et l'expérience de *Visa* permettent à tous les participants au système de paiement *Visa* de conserver une longueur d'avance sur les criminels et assurent une « sécurité sans discontinuité » — en d'autres termes, chaque transaction est protégée de bout en bout, de sorte que peu importe où l'on se trouve dans le processus de transaction, il existe des mesures de sécurité pour protéger les cartes et les comptes *Visa*.

## À PROPOS DE VISA CANADA

Visa exploite le plus vaste réseau de paiements électroniques au détail du monde et est l'une des marques mondiales de services financiers les plus reconnues. Visa facilite le commerce mondial par le transfert de valeur et d'information entre les institutions financières, les marchands, les consommateurs, les entreprises et les organismes gouvernementaux. Nous offrons un éventail de plateformes de produits de paiement, que les institutions financières faisant affaire avec nous utilisent pour élaborer des programmes de crédit, de paiement, de charge reportée, de prépaiement et d'accès à des fonds, et pour les offrir aux titulaires de carte. La plateforme des cartes *Visa* fournit aux consommateurs, aux entreprises, aux marchands et aux organismes gouvernementaux une mode de paiement sécuritaire, pratique et fiable dans plus de 170 pays et territoires.



®/MC Marques déposées / marques de commerce de Visa International;  
Visa Canada est un usager licencié.