

À compter d'avril 2005, si le marchand fournit le code CVV2 aux fins d'authentification et que l'émetteur ne participe pas à cette validation, le marchand sera protégé contre toute transaction frauduleuse éventuelle.

Pour obtenir plus d'information sur l'utilisation du code CVV2 dans votre entreprise, communiquez avec votre acquéreur Visa.

Comment protéger votre entreprise contre la fraude sans présence de la carte

- Inscrivez-vous au programme *Vérfifié par Visa*. Visitez www.visa.ca/verifie pour obtenir plus d'information.
- Lorsque vous prenez une commande par téléphone ou par Internet, demandez au client de vous fournir la date d'expiration de sa carte et incluez-la dans votre demande d'autorisation. Une date d'expiration non valide ou manquante peut indiquer que le client n'est pas en possession de la carte.
- Utilisez des outils de détection de la fraude, tels que le code CVV2, dans le cadre du processus d'autorisation.
- Méfiez-vous des achats effectués au moyen de multiples cartes et provenant d'une seule adresse Internet ou des commandes effectuées au moyen de multiples cartes, mais à livrer à une seule adresse – cela peut indiquer une activité frauduleuse.
- Méfiez-vous des transactions qui présentent plusieurs des caractéristiques suivantes : nouvel acheteur, commandes supérieures à la normale, commandes d'une grande quantité d'un même article, commandes d'articles d'un montant élevé, commandes à livrer « en urgence » ou « en 24 heures » et commandes à livrer à une adresse internationale.

PIRATAGE

De nos jours, les criminels s'y connaissent de plus en plus en technologie et trouvent des moyens de pirater le système informatique d'une entreprise pour avoir accès aux renseignements confidentiels des clients. En piratant votre système, les criminels peuvent non seulement avoir accès à cette information, mais aussi obtenir des renseignements de nature délicate sur votre entreprise.

Que fait Visa pour vous aider à protéger votre système?

Programme Sécurité de l'information concernant les comptes (SIC)

Il s'agit d'un programme mondial qui exige que les marchands rendent leurs environnements physique et virtuel plus sécuritaires afin de se protéger contre le piratage. Il fournit aux marchands des outils faciles à utiliser qui présentent des normes mondiales, un guide des pratiques exemplaires et un questionnaire d'auto-évaluation fournissant des renseignements clés et des exigences visant tout particulièrement la protection des comptes des titulaires et des données des transactions.

Récemment, Visa a aligné son programme SIC au programme de protection de MasterCard afin de procurer une série de normes sectorielles en matière de sécurité des données. Ces normes ont été conçues pour assurer le traitement sécuritaire des renseignements des cartes et accroître la confiance des titulaires. Les marchands et les fournisseurs de services peuvent maintenant évaluer leur niveau de sécurité en utilisant une seule série d'exigences en matière de sécurité.

Que faire pour protéger votre entreprise contre le piratage?

- Assurez-vous que votre entreprise respecte les normes du programme SIC de Visa. Pour en savoir davantage sur ce programme, visitez www.visa.ca/sic.
- Limitez l'accès aux données des comptes aux employés qui en ont besoin.
- Élaborez des programmes internes de détection de la fraude, tels que des lignes directrices à l'intention du personnel sur la manière de repérer et de signaler les transactions douteuses.
- Vérifiez si votre entreprise est à l'abri de la fraude en visitant www.visa.ca/securiteavecvisa et faites le questionnaire d'auto-évaluation du marchand.
- Installez des logiciels pour protéger vos systèmes et vos données contre les virus et mettez fréquemment à jour vos logiciels de sécurité.
- Si vous pensez avoir perdu de l'information sur un compte ou une transaction, faites immédiatement enquête et signalez-le sans tarder à votre acquéreur.
- Chiffrez les renseignements de vos bases de données ou de vos fichiers accessibles par Internet ainsi que toutes les données transmises au moyen d'un réseau.
- Détruisez les données de façon sécuritaire lorsqu'elles ne sont plus requises pour des raisons d'affaires.
- Retirez immédiatement l'accès au réseau et aux locaux à tout employé qui quitte votre entreprise.
- Ne fournissez aucune donnée sur un compte à une personne au téléphone – à moins d'avoir initié l'appel.

Pour en savoir plus sur la façon d'identifier, de signaler et d'enrayer la fraude, visitez :

www.visa.ca/securiteavecvisa.

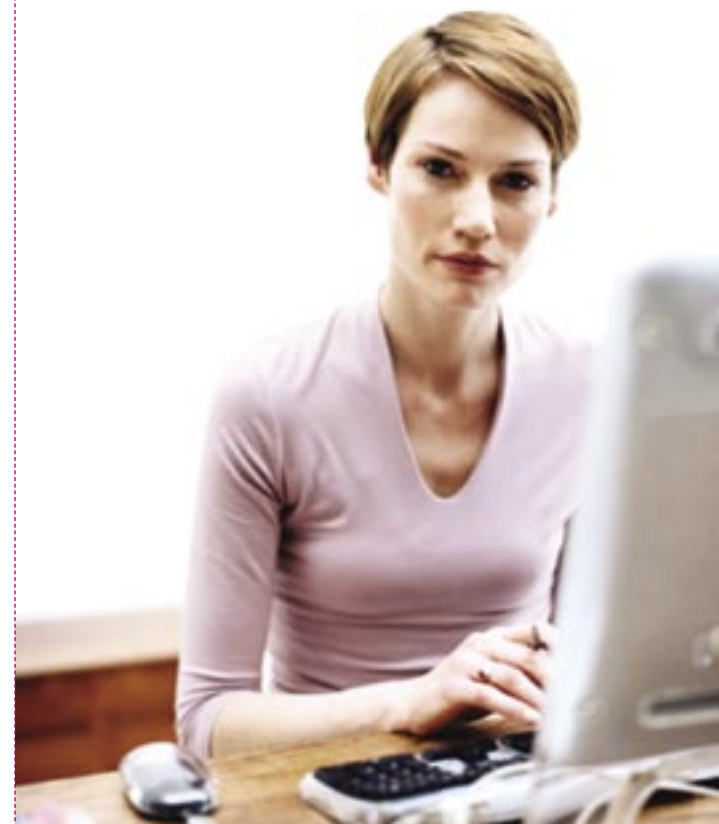


MC Marque de Visa International Service Association;
Visa Canada est un usager licencié.



La fraude par carte de crédit :

Guide pour aider les entreprises à l'identifier, à la signaler et à l'enrayer



Chez Visa, nous nous efforçons de vous offrir l'information la plus récente pour vous aider à établir l'environnement de transaction le plus sécuritaire pour vous et vos clients.

Nous comprenons que vous et vos clients accordez de l'importance à la sécurité et nous travaillons en étroite collaboration avec nos institutions financières membres, les forces de l'ordre et les sociétés de traitement acquéreuses pour assurer un environnement de paiement sécuritaire.

Cependant, il y a des mesures que vous, en tant que marchand, pouvez prendre pour réduire votre risque d'être la cible d'une fraude. Cette brochure fournit de l'information qui vous aidera à identifier la fraude par carte de crédit, à la signaler et à jouer un rôle pour l'enrayer.

LES MULTIPLES FORMES DE LA FRAUDE

Les criminels emploient diverses tactiques pour tenter de frauder des entreprises légitimes. Voici quelques-unes des activités frauduleuses à surveiller.

CARTES FALSIFIÉES

Qu'est-ce que la falsification?

La falsification consiste à faire un double d'une carte de crédit légitime en copiant ou en « écrémant » les données figurant sur sa piste magnétique. Au moyen de cette information « écrémée », des criminels fabriquent de fausses cartes et les utilisent à des fins frauduleuses.

La falsification représente une grande partie de la fraude reliée aux cartes de crédit émises au Canada.

Que fait Visa pour prévenir la fraude par carte falsifiée?

La carte à puce VISA®

Visa offrira bientôt des cartes à puce Visa à ses titulaires des cartes. Une carte à puce est une carte de crédit dotée d'une puce intégrée renfermant un micro-ordinateur. Au Canada, Visa fait figure de chef de file dans l'intégration des micropuces aux cartes de crédit. La micropuce des cartes Visa emmagasine et traite les données. Il est pratiquement impossible de falsifier l'information d'une carte à puce. Les pays qui ont adopté la carte à puce ont constaté une réduction de la fraude par falsification de l'ordre de 80 %. Pour en savoir plus sur la carte à puce Visa, visitez www.visa.ca/puce.

Caractéristiques de sécurité des cartes Visa®

L'une des façons les plus faciles d'éviter la fraude par carte falsifiée consiste à repérer ce type de carte avant le traitement de la transaction. La carte Visa comporte des caractéristiques de sécurité conçues pour aider les marchands à faire la différence entre une carte véritable et une carte falsifiée.

Au moment de traiter une transaction, prenez le temps de vous assurer que la carte présentée pour paiement comporte les caractéristiques de sécurité suivantes.



Impression en relief : Est-elle claire et droite?

Les quatre chiffres imprimés : Correspondent-ils aux quatre premiers chiffres imprimés en relief?

Bande de signature : Le mot VISA écrit en bleu et en or est-il répété et en angle?

Que pouvez-vous faire pour enrayer la fraude par carte falsifiée?

- Vérifiez toujours si la carte comporte des caractéristiques de sécurité, telles que l'impression en relief et la répétition des quatre premiers chiffres imprimés sur la carte.

- Comparez les signatures. La signature qui figure sur le reçu devrait correspondre à celle qui se trouve au verso de la carte de crédit.
- Si vous avez des doutes sur une carte, appelez votre centre d'autorisation et demandez une autorisation « code 10 ». La personne qui vous répondra vous donnera des instructions. Toutefois, ne le faites jamais au risque de votre sécurité personnelle.
- Assurez-vous que tous vos employés connaissent les procédures d'acceptation appropriées.
- Il importe de connaître ses employés. Vérifiez les références ou les antécédents de comportement de tous vos employés.

FRAUDE SANS PRÉSENCE DE LA CARTE

Qu'est-ce qu'une fraude sans présence de la carte?

Ce type de fraude est commis sans l'utilisation réelle d'une carte—par exemple en ligne, par téléphone ou par la poste—et connaît la plus forte croissance au Canada. Les fraudeurs aiment tout particulièrement ce type de fraude, parce qu'ils n'ont pas à présenter physiquement une carte pour commettre ce crime.

Que fait Visa pour prévenir la fraude sans présence de la carte?

Programme Vérifié par Visa®

Le service *Vérifié par Visa* est un programme mondial qui procure un nouveau niveau de sécurité pour les transactions en ligne. *Vérifié par Visa* aide à protéger les marchands contre les transactions frauduleuses par l'utilisation d'un mot de passe par le titulaire de carte, ce qui aide à s'assurer que ce dernier est bel et bien la personne qui effectue la transaction. Puisque le service *Vérifié par Visa* répond à une préoccupation clé des consommateurs en matière de protection en ligne, il peut améliorer votre réputation en tant que site sécuritaire et vous assurer la fidélité de votre acheteur en ligne.

Les commerces de détail en ligne qui participent au programme *Vérifié par Visa* peuvent être protégés contre les débits compensatoires imputables à la fraude, dans une proportion pouvant atteindre 70 %.

Valeur de vérification de la carte 2 (CVV2)

Le code CVV2 est un numéro de trois chiffres imprimés sur la bande de signature des cartes Visa. Ce dernier permet au marchand de s'assurer que le client est en possession d'une carte valide au moment où il effectue une transaction par Internet, par téléphone ou par la poste.

Lorsqu'il accepte une commande sans présence de la carte, le marchand peut demander au client de lui fournir ce numéro afin de vérifier s'il est bel et bien en possession de la carte. Visa et les émetteurs fournissent une vérification du code en temps réel afin d'aider les marchands à s'assurer que la personne qui effectue l'achat est en possession de la carte. Si un acheteur ne peut fournir que le numéro de 16 chiffres de la carte de crédit et la date d'expiration, il se peut qu'il ne soit pas en possession de la carte, ce qui pourrait indiquer une transaction frauduleuse.