

Contact

Idées d'affaires pour les clients des Services aux commerçants TD

NUMÉRO SPÉCIAL SUR LA PRÉVENTION DES FRAUDES

Cinq moyens de protéger votre commerce

En 2003, la fraude par carte de crédit a coûté plus de 138 millions de dollars aux titulaires de carte et aux commerçants canadiens. Que pouvez-vous faire pour combattre ce phénomène? Voici quelques suggestions de pratiques qui vous aideront à protéger vos clients et votre commerce.

1. Vérifiez toutes les cartes

Quand on vous présente une carte *Visa**, assurez-vous qu'elle comporte tous les symboles et marques *Visa* standard (détaillés à la page 2), tels que l'hologramme tridimensionnel d'une colombe, les quatre chiffres imprimés au-dessus ou au-dessous du numéro de carte (qui devraient correspondre aux quatre premiers chiffres imprimés en relief) et la bande de signature où le mot « *Visa* », écrit en bleu et or, est répété. De plus, vérifiez la date d'expiration et assurez-vous que les quatre derniers chiffres du numéro de carte sont imprimés en relief dans l'hologramme.



REQUINQUEZ VOS AFFAIRES

2. Glissez la carte dans le lecteur

La bande magnétique d'une carte de crédit est une caractéristique de sécurité importante; chaque fois que c'est possible, il faut glisser la carte dans un terminal point

de vente. Glissez la carte une fois, dans la direction indiquée par la flèche figurant sur le lecteur, puis vérifiez si le numéro de compte affiché sur l'écran du terminal correspond à celui de la carte.

Si le terminal ne peut lire la carte, prenez une empreinte de la carte et suivez le processus des opérations au clavier.

3. Respectez le processus de traitement

Si une autorisation est nécessaire, demandez un numéro d'autorisation avant de traiter l'opération. Ne remettez pas la carte au client avant d'avoir reçu l'autorisation.

Dans ce numéro

2 / Requinquez vos affaires

- Caractéristiques antifraude

3 / Gérez votre entreprise

- Prévenir la fraude par « écrémage »
- Méfiez-vous des fraudeurs internationaux

4 / Prévention des fraudes

- Douze signaux d'alerte
- Comment se servir du code 10



Suite à la page 2

Cinq moyens de protéger votre commerce

Suite de la page 1

Assurez-vous que la facture est signée (et qu'une empreinte a été prise, s'il s'agit d'une opération manuelle) et que la signature correspond à celle que porte la carte. N'acceptez jamais une carte qui n'est pas signée.

4. Soyez vigilant à l'égard des commandes à distance

Le risque de fraude est encore plus élevé dans le cas de ventes par correspondance, téléphone, télécopieur ou Internet, qui sont conclus sans la carte. Dans ce type d'opération, il est impossible d'identifier le titulaire de la carte de façon certaine; s'il y a fraude, vous vous exposez à un débit compensatoire et à la perte du montant de la vente. (Pour accepter des commandes réglées à l'aide de la carte *Visa* par la poste, par téléphone, par télécopieur ou par Internet, vous devez avoir reçu l'approbation des Services aux commerçants TD.) Pour réduire le risque d'être victime d'une fraude, prenez les précautions suivantes avant de demander une autorisation téléphonique :

- Si l'adresse de livraison diffère de celle de facturation, demandez au client ses numéros de téléphone au travail et à la maison. Vérifiez-les à l'assistance-annuaire ou à www.canada411.ca et rappelez le client pour valider la commande.
- Si le client prendra livraison de la commande, demandez-lui d'apporter sa carte *Visa* et profitez-en pour la glisser dans le lecteur (ou prendre une empreinte) et lui faire signer le reçu.
- Demandez la date d'expiration et la valeur de vérification de la carte 2 (CVV2). Le code CVV2 est un numéro de trois chiffres imprimés après le numéro de compte sur la bande de signature des cartes *Visa*. Ce code permet au commerçant de s'assurer que le client est en possession d'une carte valide au moment où il prend une commande par la poste, par téléphone,

par télécopieur ou par Internet. Le code CVV2 a été mis au point comme moyen de réduire la fraude, mais il ne peut garantir que c'est le titulaire légitime qui passe la commande.

- Quant aux commandes par Internet, protégez-vous en utilisant *Vérifié par Visa**, un outil de paiement en ligne qui permet d'authentifier l'identité du titulaire par la saisie d'un mot de passe. Pour en savoir plus sur ce programme, consultez le site www.visa.ca/verifie
- Laissez-vous guider par le bon sens. La commande paraît-elle anormale étant donné votre type d'entreprise? Est-ce que le profit en vaut le risque?

5. Prenez le temps de former le personnel

Il est important d'informer vos employés de première ligne de la marche à suivre pour la vérification des cartes et les autorisations « code 10 ». Expliquez dans quelles situations la méfiance s'impose (voir l'article en page 4). Les Services aux commerçants TD vous offrent de la documentation qui vous aidera à sensibiliser votre personnel au sujet de la prévention des fraudes.

Pour plus d'information sur la façon de vous protéger contre la fraude, communiquez avec le bureau d'aide des Services aux commerçants TD au 1 800 363-1163, et commandez un exemplaire de notre brochure sur la prévention des fraudes par carte de crédit. ■

Caractéristiques antifraude

La carte *Visa* comporte des caractéristiques de sécurité intégrées, conçues pour vous aider à différencier une carte véritable d'une carte falsifiée. Voici les caractéristiques auxquelles vous devez vous attarder :

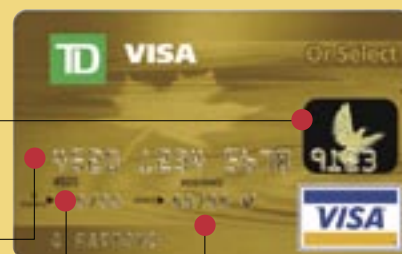
Hologramme de la colombe : La colombe a-t-elle l'air tridimensionnelle et semble-t-elle voler lorsque vous inclinez la carte d'avant en arrière? Les quatre derniers chiffres du compte sont-ils imprimés en relief dans l'hologramme?

Impression en relief : L'impression est-elle claire et droite? Le numéro de compte à 16 chiffres commence-t-il par le chiffre 4?

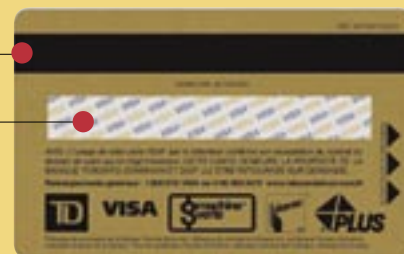
Quatre chiffres imprimés : Correspondent-ils aux quatre premiers chiffres imprimés en relief?

Bande magnétique : Elle contient le numéro de compte codé et d'autres données. Vérifiez que la bande magnétique fait partie intégrante de la carte et qu'elle ne montre aucun signe d'altération.

Bande de signature : Le mot « *Visa* » écrit en bleu et or est-il répété et en angle? Comparez la signature au verso de la carte avec la signature qui apparaît sur le reçu pour vérifier que l'orthographe et l'écriture sont les mêmes. Si les signatures diffèrent, demandez une pièce d'identité. N'acceptez pas une carte *Visa* qui n'est pas signée.



Date d'expiration : N'acceptez ni les cartes utilisées avant la date d'entrée en vigueur, ni les cartes expirées.



Si vous avez des doutes sur une carte, faites un appel « code 10 » (voir page 4).

Prévenir la fraude par « écrémage »

L'écrémage est l'enregistrement des données de compte stockées sur la bande magnétique d'une carte de crédit ou de débit pour en fabriquer une copie falsifiée.

À cause du raffinement de la technologie, les criminels peuvent aujourd'hui copier avec une facilité sans précédent les données des bandes magnétiques, au moyen d'un terminal factice ou trafiqué. Voici quelques conseils pour mettre fin à cette pratique.

Connaissez votre matériel

Inspectez régulièrement les terminaux point de vente et les claviers NIP, et vérifiez-en le numéro de série. Si le nombre ou l'apparence des appareils change, signalez-le aux Services aux commerçants TD.

Regardez aussi autour des terminaux et sous les comptoirs s'il y a du matériel, des fils ou des câbles qui ne devraient pas y être. Méfiez-vous des appareils que vous ne connaissez pas, aussi petits soient-ils. Les « glaneuses » dernier cri, de la taille d'un téléavertisseur, peuvent être portées à la ceinture ou glissées dans une poche.

Examinez les endroits surplombant les claviers NIP où une minicamera peut être dissimulée pour saisir le NIP des clients, par exemple sur une tablette au-dessus d'un comptoir, et vérifiez s'il y a des trous suspects au plafond ou dans les murs.

Connaissez votre entreprise

Les entreprises dont les employés sont appelés à travailler seuls durant de longues périodes, la nuit ou la fin de semaine, sont particulièrement vulnérables aux tentatives d'écrémage. Songez à faire des contrôles inopinés en vous rendant à votre établissement pendant ces périodes.

Vous avez également intérêt à tenir des registres précis. Conservez les horaires du personnel dans vos dossiers durant 12 mois; ainsi, vous pourrez facilement trouver qui avait accès à tel terminal et à quelle date.

Tenez un registre des équipes de nettoyeurs, d'électriciens ou de peintres qui font des travaux pour vous, surtout hors des heures d'ouverture. Vérifiez si leurs employeurs consignent sur papier leurs noms et coordonnées.

Connaissez votre personnel

Il faut bien contrôler l'embauche et la supervision des employés.

- Avant d'embaucher, vérifiez les références du candidat et demandez à voir une carte d'identité gouvernementale avec photo.
- Consignez les nom, adresse, numéro de téléphone, date de naissance et numéro d'assurance sociale des nouveaux employés.
- Exigez que les employés signent chaque



facture ou y inscrivent leur numéro d'employé, et vérifiez de temps à autre que tous observent la consigne.

- Promettez une récompense à qui signalera une tentative d'écrémage ou de corruption de la part de spécialistes de la technique. ■



Méfiez-vous des fraudeurs internationaux

Depuis quelques mois, on a constaté une hausse spectaculaire du nombre de commandes frauduleuses passées par des étrangers à des commerçants canadiens.

Un commerçant reçoit par téléphone ou courriel une modeste première commande d'un client d'outre-mer; la relation est établie. Une deuxième commande est bientôt reçue, cette fois pour une grande quantité de produits à expédier à l'étranger.

Soyez prudent si cela vous arrive ou si une commande de l'étranger comporte l'un ou l'autre des traits suivants :

- On demande d'expédier à une seule adresse une commande passée avec plusieurs cartes de crédit.
- L'adresse et le pays de livraison diffèrent de ceux du titulaire (par exemple, une commande portée à une carte émise en Australie est à expédier en Bulgarie).
- On vous commande de très grandes quantités, des articles de grande valeur ou un grand nombre d'articles identiques – à livrer d'urgence ou le lendemain.
- Des produits que vous n'avez pas en stock sont demandés.

Si une commande de l'étranger éveille vos soupçons, suivez les recommandations quant au traitement des opérations sans présentation de carte (voir le point 4 à la page 2) – y compris la vérification du code de sécurité CVV2 – et respectez à la lettre le processus d'autorisation.

Sachez toutefois que l'obtention d'un numéro d'autorisation ne fait que confirmer que des fonds sont disponibles. Cela ne signifie pas que le titulaire légitime a autorisé l'opération et n'élimine pas la possibilité d'un débit compensatoire.

Douze signaux d'alerte

Savoir déceler les premiers signes d'une opération potentiellement frauduleuse peut vous épargner du temps et de l'argent. Tant le client que la carte de crédit qu'il présente peuvent vous paraître suspects et vous alerter.

Examinez attentivement la carte afin de détecter des signes de trafiquage ou de contre-façon et surveillez de près le comportement d'individus que vous ne connaissez pas.

Signes de contrefaçon

- La surface de la carte n'est pas uniforme, est égratignée ou écaillée, et les bords sont pliés.
- Il n'y a pas d'hologramme tridimensionnel.
- On voit des retouches de peinture métallique sur l'hologramme, après réembossage du numéro de compte.
- Les quatre chiffres imprimés ne correspondent pas aux quatre premiers chiffres imprimés en relief.
- L'espacement est irrégulier, des caractères sont de style différent.
- Il y a de la peinture ou du ruban adhésif sur la bande de signature, ou celle-ci est endommagée ou effacée, révélant le mot « VOID ».

- On détecte les traces d'un nom, d'un numéro ou d'une date effacés.

Comportements suspects

- Avec une carte qui vient d'être validée, un client achète de grandes quantités d'articles coûteux sans se préoccuper de la taille, de la couleur, du style ou du prix.
- Une femme présente une carte où est inscrit un nom d'homme ou vice versa.
- Un client achète des appareils électroniques coûteux (téléviseurs, chaînes stéréo) sans s'informer des caractéristiques ou de la garantie, ou tient à prendre la marchandise immédiatement, même si le prix comprend la livraison.
- Des clients sortent une carte de leur poche plutôt que de leur portefeuille, signent la facture gauchement ou très lentement, ou regardent le nom inscrit sur la carte avant de signer.
- Un client paraît très nerveux ou presse un commis peu avant la fermeture.

De tels comportements peuvent être légitimes, mais mieux vaut jouer de prudence. Si vous avez le moindre soupçon, demandez une autorisation « code 10 » par téléphone. ■

Comment se servir du code 10

Si votre expérience, votre instinct ou les conseils donnés dans ce bulletin vous portent à croire qu'une carte de crédit est falsifiée, appelez sans attendre le Centre d'autorisation Visa des Services aux commerçants TD, au

1 800 363-1163. Précisez qu'il s'agit d'une autorisation « code 10 » et observez cette marche à suivre :

- Restez calme et courtois, et gardez la carte tant que vous n'avez pas obtenu l'autorisation.
- Aux questions du préposé, répondez par oui ou par non.
- Il vous enjoindra soit de conclure l'opération (sans oublier d'inscrire le numéro d'autorisation), soit de retenir la carte.
- N'essayez pas d'arrêter le client ou de l'empêcher de partir.

Bien qu'il soit important de signaler les fraudes potentielles, ne mettez pas en danger votre propre sécurité par une demande d'autorisation « code 10 ».

Il vous faut du papier?

Les sociétés qui suivent sont des fournisseurs de papier privilégiés des Services aux commerçants TD pour les terminaux point

de vente. Pour vous assurer que vous faites affaire avec un fournisseur digne de confiance, appelez l'un d'entre eux quand vous aurez besoin de papier.

- J.L. Inc., 1 800 363-4873

- Main-Tech Industries, 1 800 268-5120
- Maxwell Media Products, 1 800 561-6406
- Wedge Paper Products, 1 888 933-4337 (service en français)

Le bulletin *Contact* est publié périodiquement par les Services aux commerçants TD. Pour plus d'information, vous pouvez nous écrire à : Bulletin Contact, Service du marketing des Services aux commerçants TD, 15th floor, Royal Trust Tower, Toronto (Ontario) M5K 1A2; ou téléphonez-nous au numéro sans frais 1 800 363-1163.

♻️ Imprimé sur du papier recyclé

Les Services aux commerçants TD ne font aucune recommandation et ne donnent aucun conseil en ce qui a trait à la nature, à la pertinence ou à la valeur potentielle d'un produit ou d'un service en particulier.

Tous les efforts ont été faits pour que l'information contenue dans le présent bulletin soit exacte. Cependant, Les Services aux commerçants TD et La Banque Toronto-Dominion n'assument aucune responsabilité en ce qui concerne d'éventuelles erreurs ou omissions que comporterait cette information ou des pertes subies par les titulaires et découlant de ces erreurs ou omissions.

* Visa International Service Association/TD Canada Trust est un utilisateur licencié de la marque.

© 2005 La Banque Toronto-Dominion, tous droits réservés.

 **Services aux Commerçants**