Veuillez signaler sans délai toute activité suspecte qui comprend une carte de crédit ou de débit à Services aux commerçants TD, au 1-800-363-1163

Pour de plus amples renseignements, visitez le site à l'adresse www.tdcanadatrust.com/francais/merchant

MD Marque de commerce d'Interac Inc. TD Canada Trust est un utilisateur autorisé de la marque.
MC/MD1 Marque de commerce déposée de MasterCard International Incorporated.

Services aux Commerçants

Sources Mixtes
Groupe de produits issu de forêts bien gérées, de sources contrôlées et de bois ou fibres recyclés.
www.fsc.org Cert no. XX-XXX-XXXX
© 1996 Forest Stewardship Council
FSC
XX%

581615(0810)

Services aux commerçants

Comment mieux protéger votre entreprise

Gare à la fraude liée aux cartes de crédit

Toutes les cartes de crédit émises au Canada sont munies de caractéristiques de sécurité particulières afin de prévenir la contrefaçon et la fraude. Un numéro de compte invalide ou l'utilisation non autorisée d'un numéro de compte valide peuvent donner lieu à une opération frauduleuse par carte de crédit.

L'un des types de perte attribuable à la fraude communs découle de l'utilisation non autorisée d'une carte de crédit perdue ou volée. Les opérations frauduleuses sont généralement effectuées dans les heures qui suivent la perte ou le vol de la carte. Dans la plupart des cas, la victime n'a pas encore signalé la perte ou le vol de sa carte.

Des procédures ont été établies par les diverses sociétés émettrices de cartes afin de vous aider à repérer les cartes falsifiées et à prendre les mesures nécessaires, le cas échéant. En outre, les caractéristiques de sécurité ont été conçues pour vous permettre de reconnaître plus facilement les cartes falsifiées.

Les renseignements contenus dans cette brochure vous aideront à protéger votre entreprise des pertes liées à la fraude.

LES NOUVELLES TECHNOLOGIES VOUS AIDENT À CONTRER LA FRAUDE

Services aux commerçants TD s'emploie à mettre à votre disposition encore plus de techniques de prévention et de sensibilisation à la fraude liée aux cartes de crédit et de débit. L'une d'elles est la technologie des microcircuits, consistant à intégrer une micropuce dans les cartes de crédit et de débit, ce qui permet aux commerçants de traiter les opérations de façon plus sûre et plus commode.

Gare à la fraude liée aux cartes de débit

Bien que les services de paiement direct *Interac*[MD] figurent parmi les plus sûrs dans le monde, la fraude par écrémage de carte de débit demeure une possibilité. L'écrémage est une méthode frauduleuse de capture des renseignements sur un compte à partir de la bande magnétique d'une carte de débit ou de crédit dans le but de falsifier la carte.

En cas d'écrémage de cartes de débit, les numéros d'identification personnels (NIP) peuvent également être volés.

Voici les mesures que vous pouvez prendre pour prévenir l'écrémage :

- Inspectez régulièrement votre équipement de point de vente, notamment les numéros de série, les fils et les câbles. Si un dispositif vous est inconnu, semble avoir été altéré ou a simplement disparu, informez-en immédiatement Services aux commerçants TD.
- Vérifiez les plafonds, les murs et les étagères à proximité des claviers d'identification personnelle, à la recherche d'orifices où l'on pourrait dissimuler une petite caméra.
- Installez votre terminal de débit de façon que les clients aient suffisamment d'espace pour couvrir aisément le clavier lorsqu'ils composent leur NIP. La manière la plus répandue de s'approprier le NIP d'un titulaire de carte consiste en effet à lire par-dessus son épaule.
- Assurez-vous qu'aucune caméra de sécurité dans votre établissement ne filme les clients qui composent un NIP.
- Ne composez jamais un NIP pour un client, même à sa demande.
- Rappelez-vous de remettre au client une copie du relevé d'opération (sa signature n'est pas nécessaire) et de lui rendre sa carte.
- Permettez au client de garder le clavier d'identification personnelle en main jusqu'à ce que l'opération soit terminée.
- Conservez dans vos dossiers tous les relevés d'opération (pour la période indiquée dans votre convention de services de traitement), de même que les horaires des employés et les renseignements sur les fournisseurs.

Prévention des fraudes liées aux cartes de crédit – liste de vérification

Vous réduirez les risques d'opérations frauduleuses par carte de crédit en observant scrupuleusement la marche à suivre ci-dessous pour chaque opération de crédit :

1. Assurez-vous que la carte de crédit comporte tous les symboles et marques standards :

☑ Les quatre chiffres imprimés au-dessus ou au-dessous du numéro de compte figurent au recto de la carte.

☑ Le symbole unique est imprimé au recto de la carte. Par exemple :
Visa : V, CV, BV ou PV
MasterCard : M

☑ L'hologramme tridimensionnel de la colombe figure au recto de la carte, ou le mini-hologramme de la colombe ou la bande magnétique holographique apparaît au verso de la carte.

2. Assurez-vous que l'empreinte est claire et lisible sur toutes les copies de factures :

☑ Si vous utilisez un terminal électronique et que vous n'arrivez pas à y glisser la carte, entrez l'opération manuellement. Prenez bien soin d'examiner les caractéristiques de sécurité des cartes que vous ne parvenez pas à lire électroniquement.

☑ De plus, prenez manuellement l'empreinte de la carte de crédit afin de pouvoir prouver que l'opération a été réglée au moyen de cette carte. Assurez-vous que votre plaque de commerçant est fixée sur l'imprimante à carte. Inscrivez la date, le numéro d'autorisation et le montant sur la facture et assurez-vous que le client l'a signée. Si vous éprouvez constamment des difficultés à glisser les cartes des clients dans votre terminal, veuillez communiquer avec Services aux commerçants TD.

3. Téléphonez pour obtenir une autorisation dans les cas suivants :

☑ Votre terminal électronique affiche le message « Appel autorisation ».

☑ Le numéro de compte qui apparaît à l'écran de votre terminal diffère du numéro figurant au recto de la carte.

☑ Vous avez des doutes sur le titulaire de la carte, sur la carte de crédit ou sur la signature.

Sachez que le fait d'obtenir un numéro d'autorisation ne sert qu'à confirmer la disponibilité des fonds sur la carte. Ce numéro ne confirme pas que le titulaire de carte a autorisé l'opération et ne prévient pas la rétrofacturation.

REMARQUE : Si vous utilisez un terminal électronique, la limite d'opération vous sera fournie par Services aux commerçants TD. Si votre terminal est hors service en raison d'une panne de courant ou de difficultés techniques, suivez la procédure d'exécution manuelle : téléphonez afin d'obtenir une autorisation, inscrivez le numéro d'autorisation sur la facture et prenez manuellement l'empreinte de la carte de crédit pour toute opération dont le montant est égal ou supérieur à votre limite d'opération manuelle.

4. Assurez-vous que la signature du titulaire de la carte sur la facture correspond bien à celle qui apparaît sur la bande de signature, au verso de la carte de crédit. Au besoin, n'hésitez pas à demander des pièces d'identité.

CODE 10 – Autorisation

Dès que vous avez des doutes sur une opération de crédit ou sur un titulaire de carte, téléphonez sans tarder au centre d'autorisation de Services aux commerçants TD au **1-800-363-1163** en précisant qu'il s'agit d'une autorisation CODE 10.

À la simple mention du CODE 10, vous informez l'agent qu'il pourrait s'agir d'une opération douteuse ou frauduleuse, sans toutefois alerter la personne qui présente la carte. Vous devrez ensuite répondre par « oui » ou par « non » à une série de questions afin de vérifier l'authenticité de la carte. L'agent vous communiquera alors un code d'autorisation ou vous demandera de conserver la carte de crédit. C'est d'ailleurs pour cette raison que vous devriez avoir la carte en main tout au long du processus d'autorisation.

Ne tentez pas d'arrêter ou de retenir la personne qui utilise la carte de crédit. Prêtez attention à son apparence physique et à tout autre détail pertinent dans l'éventualité où elle sortirait de votre établissement.

Une carte perdue, volée ou falsifiée pourrait faire l'objet d'une récompense.

Caractéristiques de sécurité de tous les types de cartes de crédit

Reconnaître les cartes suspectes est une première démarche tout indiquée pour vous protéger contre la fraude par carte de crédit. Vous devez connaître les caractéristiques de sécurité de chaque type de carte et vous devriez pouvoir reconnaître les signes communs de falsification afin de déceler les cartes pouvant être frauduleuses ou contrefaites.

Avant d'accepter une carte, assurez-vous qu'il n'y a pas eu de modification ou d'ajout d'inscriptions en relief au numéro de compte. Vérifiez que les dates de validité, qui figurent en relief sous le numéro de compte, n'ont pas été modifiées.

N'acceptez pas une carte qui est utilisée avant la date qui est indiquée à droite des mots « VALABLE DU » ou après la date qui figure à droite des mots « JUSQU'AU ».

Toutes les cartes sont dotées d'une bande de signature au verso. Comparez l'orthographe et l'écriture de la signature sur la bande de signature à celles sur la facture. S'il y a divergence, n'hésitez pas à demander des pièces d'identité. N'acceptez jamais une carte de crédit qui n'est pas signée.

Sur la bande de signature, vous devriez vérifier qu'il n'y a pas de traces de falsification évidentes telles que des rayures, la présence de ruban blanc ou de liquide correcteur blanc ou une signature superposée à une autre au moyen d'un stylo-feutre. Si le mot « void » apparaît de façon répétitive sur la bande de signature, son contenu a été effacé ou abîmé d'une quelconque façon, et vous ne devriez pas accepter la carte.

Toutes les cartes ont une bande magnétique au verso qui renferme le numéro de compte. Cette bande devrait être lisse et droite et ne devrait pas comporter de traces de falsification.

Chaque fois que vous glissez la carte dans votre terminal électronique, la bande magnétique est lue, et le numéro de compte s'affiche à l'écran du terminal. Assurez-vous que le numéro qui apparaît à l'écran correspond au numéro de compte qui figure au recto de la carte. Lorsque le reçu est imprimé, vous devriez également comparer le numéro de compte sur le reçu à celui sur la carte. S'il y a divergence, téléphonez pour obtenir une autorisation CODE 10.

Aux pages suivantes, vous verrez des images du recto et du verso de trois types de cartes *Visa* et *MasterCard* différents, ainsi qu'un guide de leurs caractéristiques de sécurité particulières. Familiarisez-vous avec ces caractéristiques de sorte que vous puissiez reconnaître les cartes suspectes et vous protéger contre la fraude.

Éléments de sécurité d'une carte *Visa** et d'une carte *MasterCard*MD1

Carte *Visa*

1 Numéro de compte

Tous les numéros de compte *Visa* ont 16 chiffres et commencent par 4. Vous devez vérifier que les chiffres sont clairs et nets, qu'ils ont la même taille et qu'ils sont répartis également. Si les chiffres semblent flous, il y a peut-être eu ajout d'inscriptions en relief sur la carte.

2 Numéro d'identification de la banque

Les quatre premiers chiffres du numéro de compte constituent le numéro d'identification de la banque (NIB) et apparaissent de façon répétée en plus petits caractères sous les numéros embossés. Vous devriez vérifier que les quatre chiffres sous le numéro de compte correspondent aux quatre premiers chiffres embossés. Si ces deux séries de chiffres ne concordent pas, la carte a été altérée ou falsifiée.

3 Marque *Visa*

La marque *Visa* doit figurer dans le coin inférieur droit, supérieur gauche ou supérieur droit de la carte. La plupart des cartes ont une orientation horizontale. Les cartes à puce peuvent avoir une orientation verticale.

Un « V » est visible sur la marque *Visa* lorsqu'on place la carte sous une lumière ultraviolette.

4 Puce

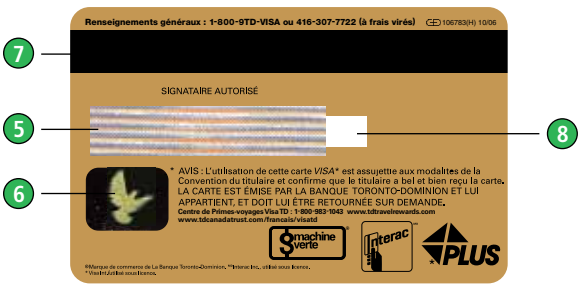
Une micropuce intégrée stocke des renseignements dans un format encodé sécuritaire, ce qui rend la tâche plus difficile aux utilisateurs non autorisés qui tentent de copier les renseignements de la carte ou d'y accéder.

5 Bande de signature

La bande de signature, qui peut avoir cette allure ou être personnalisée, doit figurer au verso de la carte. Le mot *VISA* se répète et est visible sur la bande lorsqu'on la place sous une lumière ultraviolette.

Carte *Visa* TD Or Élite sans puce

Carte *Visa* TD Or Élite à puce



6 Mini-hologramme de la colombe

Le mini-hologramme de la colombe figure au verso de la carte, soit en dessous, à la gauche ou à la droite de la bande de signature sur les cartes qui ne sont pas des cartes à puce et sous la bande de signature sur les cartes à puce.

7 Bande magnétique

Assurez-vous que la bande magnétique est lisse et droite et qu'elle ne comporte pas de signes d'altération.

8 Code de valeur de vérification de la carte 2 (CVV2)

Le code à trois chiffres (CVV2), qui sera imprimé en creux au verso de la carte, doit figurer dans la case blanche à droite de la bande de signature ou sur la bande de signature.

Carte *MasterCard*

1 Numéro de compte – quatre premiers chiffres

Les quatre premiers chiffres du numéro de compte doivent être identiques à ceux préimprimés en dessous (numéro identificateur de banque, ou BIN). Tous les numéros de carte *MasterCard* commencent par un 5.

2 Numéro de compte – quatre derniers chiffres

Les quatre derniers chiffres du numéro de compte doivent correspondre aux quatre chiffres imprimés sur le reçu remis au titulaire de carte.

3 Hologramme de la mappemonde

L'hologramme de la mappemonde est tridimensionnel, avec plusieurs fois le mot « *MasterCard* » imprimé en arrière-plan. Lorsque la carte est tournée, l'hologramme réfléchit la lumière et donne l'impression d'être animé.

4 Lettres stylisées

Les lettres stylisées MC ont été supprimées, mais peuvent tout de même apparaître sur des cartes jusqu'au 1er juin 2010.

5 Bande de signature

La bande de signature est conçue pour laisser des traces évidentes si l'on tente de la falsifier. Le mot « *MasterCard* » y est imprimé plusieurs fois en diverses couleurs, dans un angle de 45 degrés. Comparez toujours la signature au verso de la carte avec celle du titulaire sur le reçu lors d'opérations réalisées au moyen de la bande magnétique.

6 Numéro CVC2

Les quatre chiffres imprimés sur la bande de signature doivent être identiques aux quatre derniers chiffres du numéro de compte. Ils sont suivis par le numéro CVC2 (trois chiffres).

7 Puce

Une micropuce intégrée stocke des renseignements dans un format encodé sécuritaire, ce qui rend la tâche plus difficile aux utilisateurs non autorisés qui tentent de copier les renseignements de la carte ou d'y accéder. Après avoir inséré la carte dans un terminal de lecture de cartes à puce, le titulaire est invité à entrer son numéro d'identification personnel unique ou NIP.

8 *PayPass*MC

(Facultatif) La carte peut comporter la technologie de paiement sans contact *PayPass*. La signature n'est pas requise dans le cas d'une opération *PayPass* en deçà d'un certain montant.

Surveillez tout comportement douteux…

Même si les situations suivantes sont susceptibles de se produire lors d'une opération tout à fait légitime, certaines ou l'ensemble de celles-ci risquent de survenir plus fréquemment dans le cas d'une opération frauduleuse. Surveillez le client qui :

- fait des achats à l'aveuglette sans trop s'attarder au prix, à la grandeur, à la couleur ou au style;
- achète des articles coûteux en quantité inhabituelle;
- règle de gros achats avec une carte de crédit ou de débit nouvellement valide;
- achète de gros appareils tels qu'un téléviseur ou une chaîne stéréo et insiste pour emporter la marchandise immédiatement, même si la livraison est comprise dans le prix;
- effectue plusieurs petits achats afin de vérifier si la carte est acceptée;
- tire la carte de crédit ou de débit de sa poche plutôt que de son portefeuille;
- signe la facture de manière lente ou laborieuse;
- n'est pas en mesure de fournir sur demande une pièce d'identité avec photo;
- presse le commis pour un service rapide ou parle sans arrêt parce qu'il est nerveux ou pour détourner l'attention du commis.

Fraude sans présence de la carte

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

Une fraude sans présence de la carte est une opération frauduleuse effectuée sans l'utilisation d'une carte. Généralement, cette fraude se produit lorsque les clients ne fournissent qu'un numéro de carte de crédit pour passer une commande par Internet, par téléphone ou par la poste. Étant donné que vous ne voyez jamais la carte, vous n'avez aucun moyen de vérifier sa validité à l'aide des caractéristiques de sécurité mentionnées aux pages 7 à 10.

La fraude sans présence de la carte est le type de fraude qui croît le plus rapidement au Canada. Il est populaire auprès des criminels parce qu'il leur permet de commettre une fraude sans encourir les risques qui se présentent lorsqu'ils tentent d'effectuer un achat au magasin avec une carte contrefaite ou altérée.

Que font *Visa* et *MasterCard* pour aider à prévenir la fraude sans présence de la carte?

Pour vous aider à vous protéger contre la fraude sans présence de la carte, *Visa* a élaboré le programme *Vérifié par Visa**, le Service de vérification d'adresse (SVA) et a ajouté le code de valeur de vérification de la carte 2 (CVV2) à toutes nos cartes. *MasterCard* a élaboré le programme SecureCode et le Système de vérification d'adresse (SVA) en plus d'ajouter le numéro CVC2 à toutes les cartes.

En quoi consistent les programmes *Vérifié par Visa* et SecureCode?

Vérifié par Visa et *MasterCard* SecureCode[MD1] utilisent un système de mot de passe pour intégrer un nouveau niveau de sécurité aux opérations en ligne effectuées par carte *Visa* ou par carte *MasterCard*. Le titulaire de carte crée un mot de passe qu'il doit entrer lorsqu'il effectue un achat à partir du site Web d'un marchand qui participe au programme *Vérifié par Visa* et SecureCode. On s'assure ainsi que la personne qui effectue l'achat est le titulaire de carte réel et non quelqu'un qui a le numéro de compte de la carte.

Vos clients savent que la fraude par carte de crédit en ligne est de plus en plus présente, et, lorsqu'ils voient que votre site Web fait partie de *Vérifié par Visa* et SecureCode, ils savent que leurs achats sont sécuritaires à partir de votre site. Aussi, si vous participez au programme *Vérifié par Visa* ou SecureCode, vous pouvez obtenir une meilleure protection contre les débits compensatoires liés à la fraude.

Que sont le code de valeur de vérification de la carte 2 (CVV2) et le numéro CVC2?

Le code à trois chiffres CVV2 et le numéro CVC2 sont d'autres caractéristiques de sécurité des cartes de crédit qui vous aident à vous assurer que la personne qui effectue un achat par Internet, par téléphone ou par la poste est un titulaire de carte légitime. Le CVV2 et le CVC2 sont des codes de sécurité à trois chiffres qui figurent sur la bande de signature ou à la droite de celle-ci, au verso des cartes *Visa* et *MasterCard*. (Voyez les images de carte aux pages 8 et 10 pour obtenir des exemples du code à trois chiffres CVV2 et du CVC2.)

Comment le code à trois chiffres CVV2 et le CVC2 vous protègent-ils contre la fraude?

Lorsque vous prenez une commande sans présence de la carte, par Internet, par téléphone ou par la poste, n'oubliez pas de demander ce numéro à trois chiffres. Le système *Visa* et *MasterCard* vérifie en temps réel que le code à trois chiffres CVV2 ou CVC2 que vous avez fourni correspond au numéro de compte mentionné par le client.

En fournissant le code à trois chiffres CVV2 ou CVC2, le client indique qu'il est réellement en possession de la carte. Si le client ne détient que le numéro de compte ou le numéro de compte et la date d'expiration, cela peut indiquer qu'il s'agit d'une opération frauduleuse.

En quoi consiste le Service de vérification d'adresse (SVA)?

Ce service assure la vérification des renseignements sur l'adresse de facturation du titulaire de carte et fournit au marchand un code de résultat distinct du code d'autorisation. En tant que marchand, vous pouvez décider de poursuivre l'opération en fonction du code de résultat. Les émetteurs ne sont plus autorisés à réclamer des débits compensatoires liés à la fraude en raison du code 83 (pas en possession de la carte), sauf s'ils participent au programme SVA et ont répondu à la demande de vérification d'un marchand.

Piratage

Étant donné que les entreprises dépendent de plus en plus de la technologie, les criminels recherchent de nouvelles façons d'exploiter la technologie à leurs propres fins. Les criminels avisés de nos jours peuvent pirater votre ordinateur pour avoir accès à des renseignements de nature délicate sur vous, votre entreprise et vos clients.

Que font *Visa* et *MasterCard* pour protéger votre entreprise contre les pirates?

Le programme Sécurité de l'information concernant les comptes (SIC) de *Visa* et le programme de protection des données de *MasterCard* sont des programmes qui aident à sécuriser l'environnement physique et virtuel de votre entreprise. Le programme SIC et celui de protection des données vous fournissent des outils faciles à utiliser conçus pour vous aider à protéger les comptes des titulaires de carte et les données des opérations contre les pirates informatiques. Ces programmes comportent un questionnaire d'autoévaluation qui vous permet d'évaluer à quel point votre entreprise est protégée.

Quelle autre mesure prennent-elles?

Visa et *MasterCard* ont aligné leurs programmes sur un programme de normes de sécurité des données offert par d'autres organisations de paiement dans le but de créer la Norme de sécurité des données de l'industrie des cartes de paiement. Ce regroupement de normes est conçu pour accroître la sécurité des renseignements sur les cartes et pour mieux protéger les titulaires de carte et les marchands contre la fraude. Il simplifie la vie aux marchands comme vous en établissant des normes de sécurité que vous pouvez mettre en place.

Comment peuvent-elles vous aider à assurer la sécurité de votre entreprise?

Pour évaluer le niveau de sécurité de votre entreprise contre la fraude, vous pouvez visiter le site de *Visa* à l'adresse **www.visa.ca/securiteavecvisa**. Vous pouvez également visiter les sites **www.visa.ca/fr/merchant** et **www.mastercard.com/ca/gateway/fr** afin de vous assurer que votre entreprise respecte la Norme en matière de sécurité des données de l'industrie des cartes de paiements. Pour en apprendre davantage sur le PCI Council, visitez le **www.pcisecuritystandards.org**

Quelles étapes pouvez-vous suivre pour protéger votre entreprise?

Il y a un certain nombre de procédures que vous pouvez suivre pour protéger votre entreprise contre les pirates. Protégez vos systèmes et données contre les virus au moyen d'un logiciel de sécurité et assurez-vous de le mettre à jour. Toutes les données qui sont envoyées par l'intermédiaire de réseaux ou qui sont conservées dans des bases de données ou des fichiers accessibles par Internet doivent être encodées, et vous ne devriez jamais conserver des données qui ne sont plus nécessaires à votre entreprise. Lorsque les données ne sont plus requises, détruisez-les de façon sécuritaire de sorte qu'elles ne soient plus accessibles à quiconque accède à votre système sans autorisation. En tout temps, si vous croyez que des renseignements sur un compte ou une opération ont été volés, signalez la situation sans délai à Services aux commerçants TD.

Prenez note que les criminels se servent souvent des appels téléphoniques pour obtenir de façon frauduleuse des renseignements sur les entreprises. Le fait de ne

jamais donner de renseignements sur un compte par téléphone à moins que vous n'ayez initié l'appel vous-même doit faire partie de vos politiques.

Comment pouvez-vous sauvegarder les renseignements de vos clients?

Tous les documents qui contiennent les numéros de compte de cartes de crédit doivent être conservés et détruits de façon sécuritaire pour sauvegarder les renseignements des clients.

Devez-vous prendre des mesures particulières à l'égard de vos employés?

La sécurité de votre entreprise dépend de vos employés. Pour vous aider à protéger les données relatives aux comptes, limitez l'accès à vos employés sauf en cas de nécessité absolue. Lorsqu'un employé n'est plus à votre service, révoquez son accès à votre réseau et à vos locaux.

Pour aider vos employés à protéger votre entreprise contre la fraude, donnez-leur une formation sur la façon de reconnaître les pratiques suspectes et établissez un système qui leur permet de vous signaler ces situations.

Grâce aux normes et aux pratiques en place, votre entreprise et vos clients devraient être mieux protégés contre la fraude.

Pour votre protection

Prenez garde au blanchiment des factures de carte de crédit. Par ce procédé, un tiers vous demande de traiter ses factures dans votre compte de commerçant, moyennant une commission généreuse. Cette pratique enfreint la Convention de services avec les commerçants qui vous lie à Services aux commerçants TD et peut se traduire par des débits rejetés ainsi qu'à la résiliation immédiate de votre Convention de services avec les commerçants. Si les factures se révèlent frauduleuses, des accusations criminelles pourraient être portées contre vous. Ne succombez pas à la tentation de traiter les factures d'une autre entreprise ou d'un tiers. Le risque n'en vaut pas la peine!